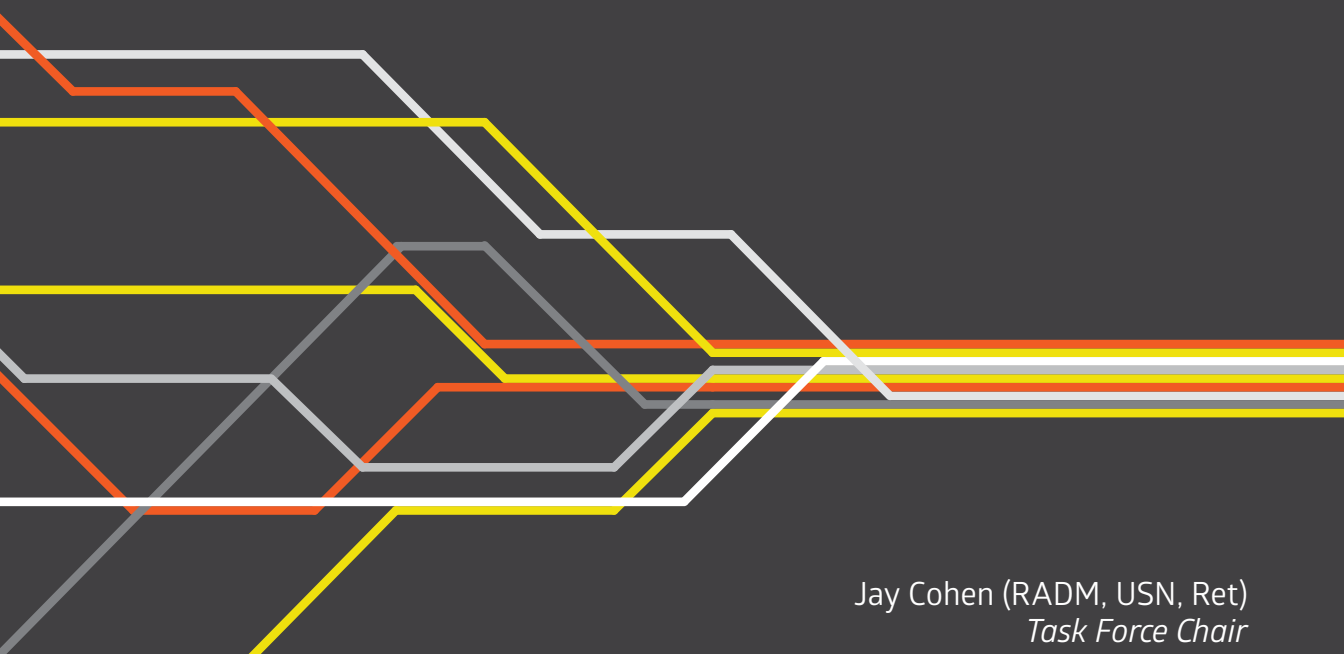


STIMSON

Partners in Prevention

Making Public-Private Security Cooperation More
Efficient, Effective and Sustainable
Recommendations of the Task Force



Jay Cohen (RADM, USN, Ret)
Task Force Chair

Barry Blechman
Task Force Vice Chair

Partners in Prevention

Making Public-Private Security Cooperation More Efficient, Effective and Sustainable

Recommendations of the Task Force

Jay Cohen (RADM, USN, Ret)
Task Force Chair

Barry Blechman
Task Force Vice Chair

Photo Credits

Page 8: US Department of Agriculture/USDAgov

Page 12: Kristin Resurreccion/kisrex

Page 16: ByeAngel/byeangel

Page 20: US Customs and Border Protection/cbpphotos

Page 24: Jacksonville Port Authority/jaxport

Page 42: Dorothy Gambrell/catandgirl

All photos via flickr.com and used under Creative Commons Licence.

© 2014 The Stimson Center

All rights reserved. No part of this publication
may be reproduced or transmitted in any
form or by any means without prior written
consent from the Stimson Center.

STIMSON

1111 19th Street, NW, 12th Floor

Washington, DC 20036

Tel: 202.223.5956 | Fax: 202.238.9604


www.stimson.org



Jay Cohen (RADM, USN, Ret)
Principal, Chertoff Group
Task Force Chair



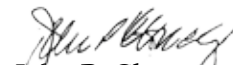
Barry Blechman
Former CEO, DFI International
Task Force Vice Chair



Amb. Kenneth C. Brill
Former Director,
National Counterproliferation Center



Gary Gregg
Former President and CEO,
Liberty Mutual Agency Corporation



John P. Clancey
Chairman, Livingston Intl.;
Director, Maersk Line



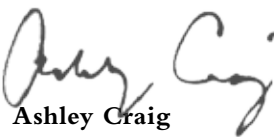
Dr. Rupert Herbert-Burns
Former Director of Intelligence,
Lloyd's Marine Intelligence Unit;
Non-Resident Research Fellow,
Stimson Center



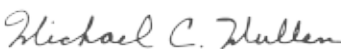
John Cogliano
Former Massachusetts Secretary
of Transportation



Peter Lichtenbaum
Partner and Co-Chair,
Intl. Trade & Finance Group,
Covington & Burling



Ashley Craig
Partner and Co-Chair,
Intl. Trade Group, Venable LLP



Michael C. Mullen
Executive Director,
Express Association of America



W. Bradford Gary
Former VP, Allergan



David Oliver (RADM, USN, Ret)
Former COO,
EADS North America



(Ms.) Ronnie L. Goldberg
Senior Counsel,
US Council for Intl. Business



Rob Rosenberg
CFO, NTELX

Disclaimer

The findings and recommendations contained in this report are those of the Task Force members as interpreted by the Stimson research team. Nothing in this report is intended to make any representations on behalf of the organizations with which Task Force members are affiliated. Any mistakes or inaccurate interpretations of meaning or intent are the sole responsibility of Stimson.

CONTENTS

Foreword.....	9
Executive Summary.....	13
The Challenge and the Imperative for Change.....	17
The Blended Threats of Illicit Trafficking.....	17
Our Solutions: Three Prerequisites for Modernizing Public-Private Security Cooperation	18
Task Force Findings.....	21
Recommendations.....	25
Reward “Trusted Exporters” of Sensitive Goods and Technologies.....	25
Empower Logistics Service Providers to Increase “Return on Investment” for Both Government and Industry.....	28
Modernize the Information-Sharing Toolkit for Trade Transparency and Risk Management.....	31
Promote Layered Port Security through the SAFETY Act and Resilience STAR Program.....	34
Develop a Public-Private “Playbook” for Resilient Trade Flows.....	36
Extend the Terrorism Risk Insurance Act and Consider Future Changes.....	38
Fully Implement The International Trade Data System.....	39
Conclusion.....	40
Endnotes.....	44
Acknowledgements.....	49



SECURITY AND ECONOMIC
COMPETITIVENESS GO HAND IN
HAND AND ARE INCREASINGLY
GLOBAL IN SCOPE.

FOREWORD

In September 2012, the Partners in Prevention Task Force was convened at the Stimson Center for its first plenary meeting. To capture the impetus for the project and the big-picture ideas that would guide our work, we developed and unanimously adopted a “Statement of Principles,” reproduced here in full:

Partners in Prevention Task Force: Statement of Principles September 2012

A growing number of transnational threats to our physical and economic security — from nuclear proliferation to arms and narcotics trafficking — overwhelm the know-how, capacity, and jurisdiction of any single government. In particular, global supply chains have become key enablers for a range of illicit activities. By undermining security and legitimate business, these illicit activities harm both the public and private sectors. More effectively mitigating these threats while opening new economic opportunities requires a multilayered approach that better integrates the expertise and decentralized market-driven mechanisms of the private sector, and that fully leverages non-regulatory tools as first recourse. This approach should be guided by the following principles:

Public-private collaborations must be responsive to market characteristics and security gaps. Even when modeled on past successes, static, formulaic approaches will not keep pace with today’s economic and security dynamics. The key to mutually beneficial collaboration is a flexible process and incentive structure that satisfies the economic concerns of industry and the regulatory concerns of government. Market forces, in themselves, are not a panacea. Respect for proprietary business operations and the profit motive must be balanced with sufficient transparency for oversight in service of security challenges.

Information sharing must be an ongoing priority. Properly calibrating the roles and responsibilities of government and private sector actors depends on an institutionalized information-sharing framework that benefits both constituencies. Moreover, when effective public-private collaborations already exist, new initiatives should strengthen and complement them rather than duplicating effort.

Security and profitability can be mutually reinforcing goals. Companies can maintain existing market advantages and unlock new opportunities by improving security within their organizations and respective industries, and by contributing to the security and resilience of the wider global trading and financial systems.

The path from those principles to the findings and recommendations that we present in this report was instructive and rewarding. Task Force members and staff from the Center’s Managing Across Boundaries Initiative collaborated over 18 months with hundreds of industry partners. Most of this outreach was concentrated among high-tech manufacturers and service providers, transport and logistics firms, and insurance providers. The two-part goal of these dialogues was to turn our founding principles into concrete recommendations that individually were *actionable* and that collectively were *diverse*.

The goal to offer *actionable* ideas led us to approach key issues largely, though not exclusively, through the lens of US exports. Particularly since the September 11, 2001, terrorist attacks, the US government has devoted significant attention and resources to regimes for screening and safeguarding imports, and to the protection of infrastructure that is critical for the nation’s trade. Those goals remain priorities. But we must realize that rising interdependence between the US and global economies means that what happens at our borders, and within them, is only part of the story. Security and economic competitiveness go hand in hand and are increasingly global in scope. Public-private partnerships therefore must align security imperatives with market dynamics more innovatively to be sustainable. The greatest opportunity to advance this mutually beneficial approach today lies at the intersection of traditional security concerns and the interests of the US exporting community — what we call the “export nexus.”

The goal to offer *diverse* ideas, in part, reflected a necessary humility. There is no silver bullet that can protect the nation against the full range of cross-border illicit trafficking threats or thwart all proliferation efforts. To the contrary, just as we must broaden our perspective on how market dynamics figure in achieving genuine security, we must dramatically expand the set of public-private tools we are willing and able to use. We had no illusions that we could construct this full “portfolio.” Rather, our aim was to demonstrate more succinctly the need for, and the potential of, modernized partnerships across several key variables:

- **Relevant national security mission areas.** Mission areas that our recommendations address include combating terrorism and the proliferation of weapons of mass destruction, protection of intellectual property and other sensitive private sector information, border management, counter-intelligence, port security, and the resilience of critical infrastructure.
- **Operating context and functional requirements.** Our recommendations highlight public-private dynamics in both steady-state environments and contingency scenarios. A related but distinct consideration is the precise capabilities required in any given context.
- **Nature of public-private interactions.** The solutions we advocate reflect varied degrees of regular, direct engagement between government and industry. Some call for frequent and close collaboration on

a very particular problem of common interest. Some call for cooperative mechanisms that can be employed as needed. And some call for non-regulatory frameworks that enable coordination of a more decentralized nature or a largely industry-led effort.

Given this goal, the variety among Task Force members was a great asset. Although they served, of course, in their individual capacities, they represented an impressively wide range of specialties, outlooks and professional backgrounds. Some have spent their entire careers in the private sector, while others have held senior positions in government. It has been a pleasure working with each of them, and we are grateful for their time and valuable insights.

While traditional government countermeasures will remain crucial for US security, they no longer suffice. Complementary mechanisms that leverage the resources, agility and expertise of the private sector are essential — and not just for “security,” narrowly understood. They also will go far in shaping the future of US global influence and leadership. We urge stakeholders in both industry and government to take these ideas, work with Stimson and the other organizations willing to confront the challenges of implementation head-on, and act.



Jay Cohen (RADM, USN, Ret)
Task Force Chair



Barry Blechman
Task Force Vice Chair

ILLICIT TRAFFICKING... HAS LAID BARE THE WEAKNESSES OF TOP- DOWN GOVERNMENT CONTROLS.

EXECUTIVE SUMMARY

A global economy has empowered criminals and terrorists on a global scale. Embedded across worldwide production, trade and investment networks, illicit trafficking in high-tech data and equipment, narcotics, arms and counterfeit goods has laid bare the weaknesses of top-down government controls. Without bold changes, both public and private interests are likely to suffer a growing toll from this insidious and intermingling array of threats, including the especially grave threat of nuclear proliferation.

We must meet today's rapidly evolving security challenges with a more integrated, proactive, network-like response. In particular, we must better leverage the agility, resources and expertise of the private sector. Diminishing government resources add even greater urgency to this imperative.

This is an opportune moment for action, particularly where security issues intersect with US exports. President Obama's February 2014 executive order on streamlining export/import processes has added momentum to a range of trade-facilitation efforts, such as the impressive work by industry participants in US Customs and Border Protection's Advisory Committee on Commercial Operations. Recent international developments are poised to serve as "force multipliers" as these efforts advance further down the path to implementation.

Traditional law and regulation will remain the pillars for security. But those pillars must now be reinforced with more agile, non-regulatory approaches to counteract cross-border illicit networks more systemically. Market-based incentives will be key to ensuring that this "new normal" in public-private partnerships is genuinely sustainable.

By appealing to three interrelated prerequisites for enhanced partnerships — enabling stakeholder engagement, modernizing risk management and leveraging value-added information — we offer a range of pragmatic action items for advancing security and economic competitiveness. Some are directed at government, some are directed at industry and some call for a collaborative approach. We recommend:

- Rewarding "trusted exporters" of sensitive goods and technologies
- Empowering logistics service providers to increase "return on investment" for both government and industry

- Modernizing the information-sharing toolkit for trade transparency and risk management
- Promoting layered port security through the SAFETY Act and Resilience STAR Program
- Developing a public-private “playbook” for resilient trade flows
- Extending the Terrorism Risk Insurance Act and considering future changes
- Fully implementing the International Trade Data System

Each of these ideas, if implemented, would bring meaningful change. Together, they would go far in building the broader portfolio of tools we urgently need for modernized public-private security cooperation.

WE SHOULD NOT WAIT
FOR A NEAR-TRAGEDY
BEFORE WE ACT.



THE CHALLENGE AND THE IMPERATIVE FOR CHANGE

“... the inclination to equate control with safety gives a false sense of security.”

Beyond “Fortress America”: National Security Controls on Science and Technology in a Globalized World
National Research Council Committee on Science, Security and Prosperity

The Blended Threats of Illicit Trafficking

When Al-Qaeda in the Arabian Peninsula (AQAP) successfully conveyed printer cartridges laced with explosives onto two express delivery aircraft in October 2010 — only to be stymied at the eleventh hour thanks to an intelligence tip — there was good reason for a frenzied response. But in a break with usual practice, government agencies chose to collaborate with industry to bridge the information gaps that the incident had exposed. Through a process of “co-creation,” regulators and representatives of the major integrated express delivery companies developed the concept for what became the Air Cargo Advance Screening Program.

Under the new program, express delivery companies are required to transmit only the most crucial shipment information on an expedited timeline, with less stringent parameters. As a result, companies are able to transmit the information to US security officials much earlier than under the old rules. The companies even have provided government with access to their proprietary systems in order to improve the targeting process. In short, the program advances the public interest through more timely and effective security targeting of cargo, and the private interest through a reduced regulatory burden.

In many other cases, the US government has not modernized its approach. We should not wait for a near-tragedy before we act.

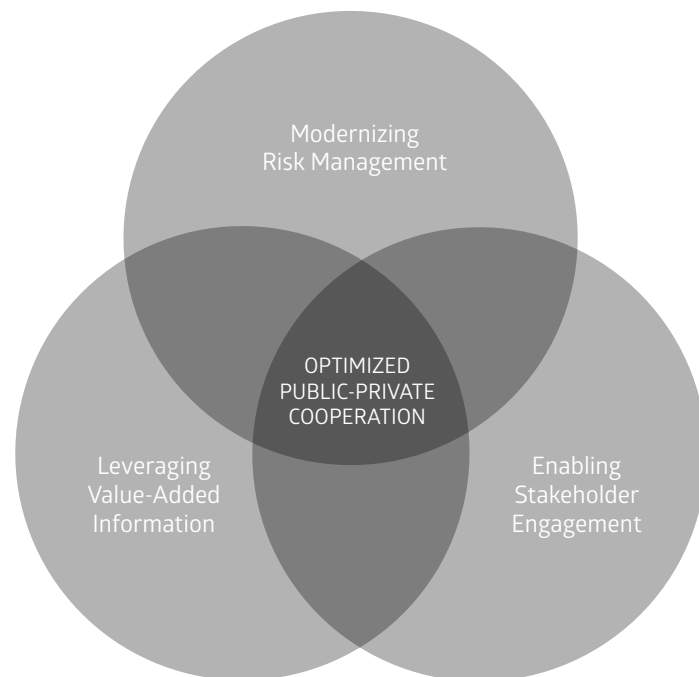
Illicit trade in weapons, narcotics, counterfeit goods and much more has found many seams where even the most well-resourced law enforcement and intelligence efforts do not suffice. These threats are thriving on contemporary availability of sophisticated technologies and know-how, as well as a lack of transparency in some aspects of the international shipping system. They are taking root in, and spreading through, the same global physical and informational infra-

structure that powers legitimate trade and communication. We are especially concerned by trafficking in dual-use goods and technologies, such as those that could support a nuclear weapons capability.

Traditional law and regulation are, and will remain, the pillars for security. But globalization mandates that those pillars now be reinforced with more agile, non-regulatory approaches to counteract cross-border illicit networks more systematically. The precise circumstances and objectives will often differ, so we need to develop a portfolio of tools. Market-based incentives will be key to ensuring that this “new normal” in public-private partnerships is genuinely sustainable.

Our Solutions: Three Prerequisites for Modernizing Public-Private Security Cooperation

Dialogue with hundreds of industry partners over 18 months has left us confident that both government and industry have within their reach pragmatic, actionable steps that can make a meaningful difference. At a broad level, three interrelated themes emerged from these discussions, representing three strategic prerequisites for building out the public-private toolkit for addressing 21st-century proliferation and illicit trafficking challenges. In developing our ideas with industry partners, one of the principal criteria we followed was ensuring that each recommendation significantly addressed at least one of these prerequisites.



Leveraging “Market Power” in Public-Private Partnerships

Modernizing Risk Management

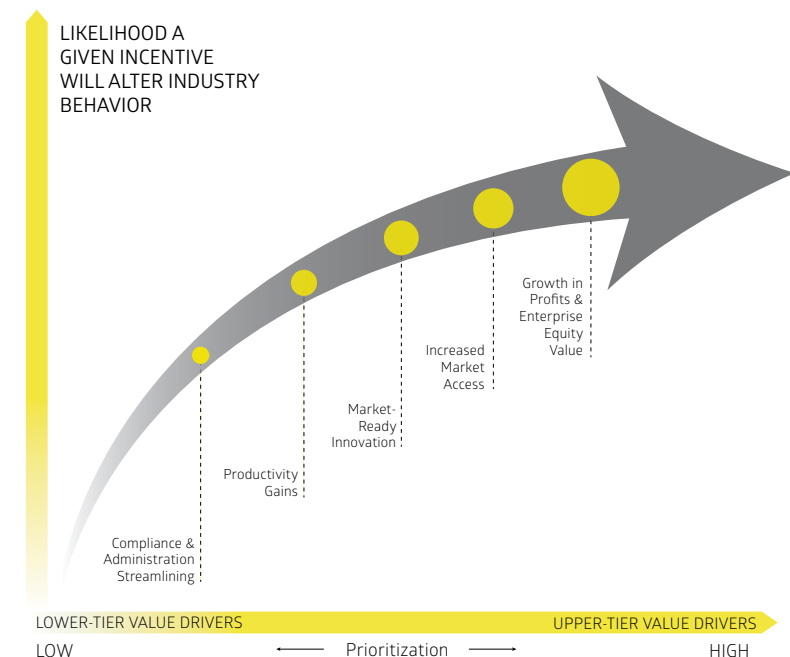
- Realigning government and industry assumptions of risk to better reflect their respective capabilities, resources and interests — and thereby enhancing efficiency and effectiveness
- Forging more integrated decision-making and operational capacities among government and industry actors
- Identifying market-based incentives that can change industry behavior meaningfully and sustainably

Leveraging Value-Added Information

- Achieving greater clarity on regulatory regimes and enforcement practices
- Establishing information-sharing mechanisms that enable richer analytics

Enabling Stakeholder Engagement

- Involving a broader set of private sector stakeholders for a more informed view of how security imperatives interact with market dynamics, both across and within industry sectors
- Creating a regulatory environment that promotes innovation in the service of both security and economic competitiveness



The Full Spectrum of Industry Value Drivers: A Simplified View

GLOBAL ECONOMIC INTEGRATION HAS OPENED OPPORTUNITIES FOR BILLIONS OF PEOPLE, BUT IT HAS ALSO EMPOWERED CRIMINALS AND TERRORISTS ON A GLOBAL SCALE.



TASK FORCE FINDINGS

- **Global commerce is stretching traditional tools of governance to their limits — and beyond.** Global economic integration has opened opportunities for billions of people, but it has also empowered criminals and terrorists on a global scale. Embedded across worldwide production, trade and investment networks, illicit trafficking in high-tech data and equipment, narcotics, arms and counterfeit goods has laid bare the weaknesses of top-down regulatory, intelligence and enforcement tools. Without bold changes, both public and private interests are likely to suffer a growing toll from this insidious and intermingling array of threats, including the especially grave threat of nuclear proliferation.
- **A fluid and complex threat environment demands a diverse “portfolio” of public-private solutions.** We must meet today’s rapidly evolving security challenges with a more integrated, proactive, network-like response. In particular, we must leverage the agility, resources and expertise of the private sector. While government will never act at the speed of 21st-century innovation and commerce, it must be prepared to employ a broader array of legal, policy and institutional tools to enable this approach.
- **A modernized approach to public-private engagements can — and must — advance *both* public security and economic competitiveness.** Public-private partnerships are much more likely to be sustainable and effective when they meet three interrelated prerequisites.
 - *Modernizing Risk Management.* Beneath widespread support for the general idea of public-private partnerships is a distressingly poor understanding of how different approaches are needed for different objectives and different circumstances. Government must more aggressively explore the potential of market-based incentives to change industry behavior meaningfully and sustainably. That does not mean handouts to industry. To the contrary, it means aligning security strategies with industry value drivers in sustainable fashion, allowing a greater “return on investment” for all.
 - *Leveraging Value-Added Information.* Industry and government both could derive substantial value beyond the status quo by sharing data and other information related to the security and regulatory environ-

ments. The challenge is to precisely identify the informational needs of both parties and the proper modalities to meet those needs.

- *Enabling Stakeholder Engagement.* Public-private mechanisms such as the Critical Infrastructure Partnership Advisory Council must better reflect the complexities of the modern economy — both in the issues they address and in the stakeholders they include. Government must find the institutional means to engage more effectively with stakeholders beyond the 16 identified “critical infrastructure” sectors, including small businesses, third-party logistics providers (particularly those active in US export transactions), and those individuals whose lobbying status currently precludes them from sharing their expertise in relatively transparent fora. Public-private cooperation also should better promote industry innovation in the service of security priorities. Under current approaches, process often weighs down genuine problem solving.
- **Look to the “export nexus.”** Senior US government leaders recognize that more innovative approaches are crucial for addressing cross-border security challenges and the equally urgent task of adapting to a restrictive budgetary environment. But this is an especially opportune moment to act, in particular where security issues intersect with US exports.
 - President Obama’s February 2014 executive order on streamlining export/import processes¹ has added momentum to a range of trade-facilitation efforts, such as the impressive work by industry participants in US Customs and Border Protection’s (CBP) Advisory Committee on Commercial Operations (COAC).²
 - Recent international developments can serve as “force multipliers” as these efforts advance further down the path to implementation. Examples include the Trade Facilitation Agreement that was part of the World Trade Organization’s December 2013 “Bali Package,” as well as the Mutual Recognition Arrangements that harmonize the US Customs-Trade Partnership Against Terrorism with the comparable regimes of foreign trading partners.
 - The National Export Initiative (NEI) has entered a new phase with “NEI/NEXT,” and a determined leadership at the Commerce Department is adding new ideas and new energy to the government-industry conversation.
 - A major initiative to reform export controls is pivoting to a special focus on dual-use goods and technologies — those that have both commercial and military (or proliferation) applications. Here again, the Commerce Department is playing a central role.

Many important steps to promote synergies between security and competitiveness do not require major new authorities — especially if senior executive branch offi-

cials leverage relevant interagency tools. Close coordination between the Departments of Commerce and Homeland Security will be especially important.

- **Modest institutional innovations can enable government-industry security cooperation to flourish where historically it has faltered or never been attempted.** In particular, third-party vehicles developed and operated by industry or public-interest organizations, in coordination with government as appropriate, have strong potential. In many cases, trade associations and private standards-development organizations can play a crucial facilitation role. In some cases, other organizations are needed to dedicate time and resources, provide subject matter expertise, or convene disparate stakeholder groups.



THE US EXPORTING COMMUNITY REMAINS SUBJECT TO A COMPLEX MAZE OF LEGAL AND REGULATORY REQUIREMENTS.

RECOMMENDATIONS

Reward “Trusted Exporters” of Sensitive Goods and Technologies

The US exporting community remains subject to a complex maze of legal and regulatory requirements. But to address threats such as illicit transshipment in an increasingly global marketplace, government must find ways to complement traditional oversight and enforcement mechanisms with decentralized, market-embedded incentives for enhanced diligence. This layered approach would more systemically discourage and impede illicit, careless, and otherwise problematic industry activities in global value chains.

One important example can be seen in the regimes affecting US exporters of goods and technologies controlled under the Export Administration Regulations. When contemplating enforcement actions against one of these exporters, the US government expressly takes into account the strength of the company’s internal compliance program. A similar approach in assessing company applications for export licenses could unlock substantial dual benefits. A properly crafted incentives regime for “compliance-plus” company programs would enable government to target oversight resources more efficiently and identify problematic transactions more consistently. At the same time, it would raise the general level of diligence throughout the exporting community by rewarding those companies that voluntarily adopted more rigorous processes in key functional areas, such as end-user evaluation (sometimes called “know your customer” due diligence).

The Export Administration Regulations and “Dual-Use” Items

The Export Administration Regulations (EAR) (15 CFR 730-799) often are characterized as regulating exports and reexports of US-origin dual-use items — goods and technologies that have both civilian and military (or proliferation) applications. In fact, items subject to the EAR also include some purely civilian items and some items that are used exclusively for military applications but that do not warrant control under the International Traffic in Arms Regulations. Of these, the Task Force is concerned principally with the challenges posed by trade in dual-use items, which generally is more susceptible to the smuggling and misinformation tactics of illicit traffickers.

The administration's Export Control Reform Initiative will soon turn its focus from military items to dual-use goods and technologies. The Commerce Department and other administration officials already have indicated plans for a comprehensive review of the Export Administration Regulations. The time to act on common-sense solutions that advance both public and private interests has arrived.

Findings

- The White House and the Departments of Commerce, Defense and State have demonstrated laudable collaboration and persistence in the first phase of the Export Control Reform Initiative. The next phase of the initiative is a critical opportunity to move beyond list reform and more fundamentally modernize risk management of sensitive goods and technologies, particularly to better address the growing risks of illicit transshipment and unauthorized end-use. Leveraging industry expertise and resources must be a central part of any such effort.

Recommendations for Government and Industry

- As a priority, the Department of Commerce, in consultation with the Departments of Defense, Homeland Security and State, should work with industry to develop and pilot a “trusted exporter” regime (“the regime”). Under the regime, US exporters of dual-use items could voluntarily opt to qualify for broader licenses/authorizations upon adequately demonstrating adherence to a government-recognized set of best practices, developed by industry, for enhanced diligence in compliance and licensing. Exporter procedures for end-user evaluation should be a core part of the regime.
 - Participating companies should be subject to external procedural audits on a periodic basis to verify compliance. The regime should stipulate assessment of specific remediation measures if such audits identify a major infraction for which insufficient implementation of the agreed practices is shown to be the primary cause.
 - The pilot test of the regime should include select exporters of at least three significantly different categories of controlled items. It also should avoid arbitrary timelines in order to ensure the regime can be properly tested and modified as needed.
 - The Commerce Department should consider how coordinating the proposed regime with existing regimes could improve efficiency and effectiveness for all stakeholders. Existing regimes worth consideration in this regard include License Exception Strategic Trade Authorization, Authorization Validated End-User and the Special Comprehensive License.
- The Commerce Department and CBP should facilitate further cooperation on relevant issues among three of the advisory committees under their sponsorship: from the Commerce Department, the President's Export Council Subcommittee on Export Administration (PECSEA) and the

Regulations and Procedures Technical Advisory Committee (RPTAC); and from CBP, the COAC.

Recommendations for Industry

- Industry specialists in export controls, from a diverse set of companies, should endorse a set of cross-sector best practices for end-user evaluation. Best-practice guidance in other key functional areas, such as training and the administration of “deemed exports,” also would be valuable.

Participating industry specialists should communicate closely with the Commerce Department to ensure the industry-developed guidance can gain appropriate government recognition to serve as the regime's underlying benchmarks. They likewise should consult with CBP to ensure alignment with CBP's Trusted Trader Program.

- The exporting community should support a formal standards development process in partnership with an organization accredited by the American National Standards Institute. Including the National Institute of Standards and Technology or another US government entity in the process should be strongly considered. While such a process would be time-consuming, it could promote broader and more consistent adoption of the voluntary best practices.

Empower Logistics Service Providers to Increase “Return on Investment” for Both Government and Industry

Logistics service providers (LSPs) play a critical role in contemporary global trade. They serve as the connective tissue among disparate legal jurisdictions, geographic locales and client business models. But this wide reach, along with the diverse services LSPs provide, means many regulatory regimes and trade-facilitation initiatives do not reflect LSP business models in their full complexity. The Customs–Trade Partnership Against Terrorism, for instance, has yet to include the full range of LSPs that operate in US foreign commerce.

“Logistics Service Provider”

For purposes of this report, logistics service provider is a generic term the Task Force has stipulated to encompass all variants of non-asset-based and limited-asset-based transport providers. In US foreign and domestic commerce, such entities include: Indirect Air Carriers (IACs), also known as air freight forwarders; Non-Vessel-Operating Common Carriers (NVOCCs); ocean freight forwarders; surface forwarders; and property brokers. These references are not meant to be exclusive or exhaustive. While the Task Force sought to be inclusive, the third-party logistics sector is highly diverse and often varies from country to country.

This has security implications on two levels. First, LSPs sometimes can evade scrutiny in facilitating illicit trade, knowingly or otherwise. Second, government and industry alike are missing an opportunity to leverage, through positive incentives, the unique position and expertise of LSPs for a greater “return on investment” — that is, for better security outcomes and more profitable trade.

But both government and industry have expressed interest in finding a way to seize that opportunity. Among a set of seven best practices it has published for exporters/reexporters, the Department of Commerce recommends using LSPs that adhere to similar compliance and due diligence practices.³ Industry feedback on an earlier draft of that document reflected a strong preference for a “trusted network” or certification program for LSPs.⁴

Findings

- LSPs must figure prominently in efforts to develop a set of next-generation “trusted trader” regimes, particularly for US exports. To leverage market-based incentives effectively, it is vital that such regimes remain voluntary and reflect input from both the exporting community and LSPs as to what specific benefits could elicit their participation on a sustainable basis.
- With properly recalibrated compliance and liability burdens, a number of US businesses — especially small and medium sized enterprises — could

“Small and medium sized enterprises in particular need assistance with application procedures and development of robust compliance programs.”

Coalition for Security and Competitiveness

Recommendations for a 21st Century Technology Control Regime, January 2010

In a 2013 survey, 77% of LSPs cited risks connected to US export regulations as a reason for losing business.

Source: Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), *2013 Export Survey*, November 2013

benefit substantially from the risk management expertise and cost advantages that highly reputable LSPs provide. Top-tier LSPs could likewise benefit from a regime that recognizes the security and efficiency gains they bring to international trade.

- In establishing its new Trusted Trader Program, CBP took a laudable first step by aiming to streamline the requirements and associated benefits for the Importer Self-Assessment and the Customs–Trade Partnership Against Terrorism — and thus building a stronger link between compliance and supply chain security. Collaboration with LSPs would offer many opportunities to strengthen that link further.

Recommendations for Government and Industry

- CBP and LSPs should begin a collaboration to develop a voluntary “trusted trader” regime for LSPs (“the regime”).
- The regime should align with and leverage relevant international instruments, including but not limited to:
 - the World Customs Organization (WCO) SAFE Framework
 - Mutual Recognition Arrangements that harmonize the US Customs–Trade Partnership Against Terrorism with comparable regimes of foreign trading partners
 - the Trade Facilitation Agreement included in the World Trade Organization’s December 2013 “Bali Package”
 - the April 2013 *ICC Guidelines for Cross-Border Traders in Goods* issued by the International Chamber of Commerce Commission on Customs and Trade Facilitation
 - the anticipated WCO international guidelines on customs-trade partnerships
- Stakeholders should build on the lessons developed in relevant government–industry dialogues previously, including but not limited to the *BIS*

*'Best Practices' for Industry to Guard Against Unlawful Diversion through Transshipment Trade*⁵ and the *Freight Forwarder Guidance* published by the Department of Commerce.⁶

Recommendations for Government

- The Border Interagency Executive Council (BIEC), newly codified and empowered by a recent executive order, should ensure that all agencies with significant roles in US exports actively participate in the collaboration.⁷ Since many export-related regulatory and enforcement authorities reside outside CBP, this broader set of government participants is crucial to identifying sufficient benefits for LSPs to view the regime as viable.
- In parallel with the government-industry collaboration for LSPs, the Commerce Department's Bureau of Industry and Security should update its guidance on routed export transactions, beyond the February 2014 Proposed Rule that focuses largely on definitional issues.⁸ Further guidance is needed to address the major differences in LSP operational practices, as well as how those practices sometimes differ across modes for a given LSP.

Recommendations for Industry

- LSPs should actively share their views on private sector benefits they would like to see emerge as part of the government-industry collaboration.
- To enhance understanding of the varied roles played by LSPs, firms and trade associations should continue to support the current Department of Commerce training for export-focused CBP officers on issues related to the Export Control Reform Initiative.

Modernize the Information-Sharing Toolkit for Trade Transparency and Risk Management

As government and the expert community confront the challenge of adapting security strategies for an era of global proliferation and criminal networks, industry confronts its own challenges — many of them competitive, but many others regulatory. Multiple layers of export controls and sanctions often leave even the best-intentioned, law-abiding company wondering whether its internal compliance measures are sufficient. In many cases, such ambivalence leads companies to forego business opportunities they would have acted on in a less ambiguous regulatory environment.

For the law-abiding company, in other words, enforcement of export controls and sanctions affects not only compliance practices, but also its more fundamental assessments of risk and return. The clarity and consistency with which government regulators articulate and apply enforcement policies have an indirect but substantial impact on economic competitiveness. Recent efforts by some of the relevant agencies to revise their respective enforcement guidelines, and to better coordinate those guidelines with one another, are important but insufficient steps.

Similar dynamics undermine communication and information sharing on a host of other related topics. One example arises when a US exporter receives a suspect inquiry from an unknown foreign company seeking to procure proliferation-sensitive items. Government has various tip lines, outreach programs and other mechanisms to communicate with industry on such matters.⁹ But US exporters often are not aware of these mechanisms, or elect not to use them.

Findings

- There is substantial potential for both government and industry to benefit from a diverse set of new or enhanced information-sharing tools. Whether the context is public-private, public-public or private-private interaction, such tools can advance government and industry interests through improved

"In the absence of support and clarity in how the lines are drawn, [small and medium sized enterprises] are reluctant to export and assume an inordinate amount of risk and liability. All exporters periodically receive information from prospective buyers that could be of importance to U.S. enforcement and intelligence authorities. The adversarial nature of our system makes sharing that information difficult."

Coalition for Security and Competitiveness
Recommendations for a 21st Century Technology Control Regime, January 2010

clarity on regulatory regimes and enforcement practices, richer analytics to support risk management in both government and industry, and enhancements to trade transparency more generally.

- Many agencies have established mechanisms for communicating with the private sector, but government officials tend to overestimate the breadth of industry feedback they receive. Industry reluctance to use these mechanisms owes principally to liability concerns, confusion regarding sometimes duplicative or vaguely defined tools, and the absence of a clear business case for such engagement.

Recommendations for Government and Industry

- The Department of Commerce and major trade associations should jointly develop a framework of technical and procedural options for two-way information sharing on issues related to trade, innovation and technology transfer.¹⁰ The framework could begin simply, with publication of a consolidated “menu” of such options available under the existing authorities of interested agencies. In time, it might also serve as a vehicle to create new mechanisms better suited for specific unmet needs. Recommended applications include:
 - Government feedback on industry inquiries related to compliance and enforcement¹¹
 - Industry provision to government of information on foreign entities making suspect purchase inquiries or engaging in other anomalous behaviors, and government dissemination of relevant analysis
 - Exchange of best practices between industry and the Export Enforcement Coordination Center (E2C2) for developing trendline data on illicit transshipment, along with shared access to associated data repositories
 - Government provision of properly sanitized intelligence to industry stakeholders that support interdictions of suspected contraband
 - Identifying how the Open Data Policy¹² and the Open Data Cross-Agency Priority Goal¹³ can better harness government-wide data assets to support trade transparency and improve supply chain performance, much like a recent executive order aims to do with respect to climate change¹⁴
 - Industry provision of subject matter expertise and analytics capabilities in developing updates to the Intelligence Community Assessment of Threats to the Global Supply Chain System, first completed in 2012
 - Industry support to the Program Manager for the Information Sharing Environment (PM-ISE) for relevant milestones under the PM-ISE’s December 2013 implementation plan¹⁵

Recommendations for Industry

- Industry should establish benchmarking mechanisms for peers to share best practices in protecting against illicit transshipment and other misappropriations of sensitive technologies.

Should informal benchmarking exercises show particular value, industry should consider extending this work to establish a codified set of best practices. Industry also should consider pursuing collaboration with various third parties, including external security experts, civil society stakeholders and standards development organizations.

- Industry should support research on how best to manage legal risks associated with the options included in the proposed framework of information-sharing mechanisms, as well as development of practical guidance on issues such as constructing nondisclosure agreements. Industry also should support further research on how technological and regulatory trends might demand further institutional innovations over the longer term.¹⁶
- Exporters, supply chain and transport firms and insurance providers should assess the potential of third-party information-sharing vehicles to mitigate compliance risk and more generally promote secure, transparent and efficient operations. Stakeholders in the cybersecurity domain have begun to explore this institutional option; it should be examined for possible use in other domains. Such a capability could take many forms, and participating firms could elect to use it in tandem with or in lieu of a related public-private mechanism. As one example, the third-party entity could securely receive information from participating firms related to sensitive transactions; analyze the information in aggregate; and share with participating firms value-added insights that could be adapted for their individual risk management processes.¹⁷

Technology providers should work with participating companies to fashion a technology platform with the capabilities desired for sanitizing the information submitted, performing analytics and providing related decision support.

Promote Layered Port Security through the SAFETY Act and Resilience STAR Program

Seaports worldwide are in the midst of change. Expansion of the Panama Canal and other developments in maritime commerce are prompting many ports to make major investments in their basic infrastructure, information technology systems and intermodal facilities. These widespread construction and modernization efforts are an opportunity to promote existing best practices for security, and perhaps to incentivize new ones, while also promoting gains in efficiency.

US seaports are in the midst of at least \$46 billion in infrastructure upgrades planned over the 2012-2016 period.

Source: American Association of Port Authorities
US Port Infrastructure Investment Survey, 2012-2016, May 2012

The SAFETY Act, administered by the Department of Homeland Security (DHS), is intended to foster investment in anti-terrorism technology and enhance critical infrastructure security. The Act provides specific liability protections to qualifying technology innovators and standards developers. The Resilience STAR Program, modeled on the widely known ENERGY STAR certification system, aims to promote critical infrastructure resilience by recognizing owners and operators that have met specific, industry-defined performance targets. Also administered by DHS, Resilience STAR was first introduced in the home construction sector, but the White House has publicly stated a goal of expanding it into the transportation sector.¹⁸

Findings

A surge in construction and related modernization efforts at US ports presents an opportunity for broad adoption of enhanced security practices and new operational efficiencies. It is a good opportunity particularly to achieve the White House goal of expanding the Resilience STAR Program into the transportation sector.

Recommendations for Government

- To reinforce its efforts to establish layered port security standards, DHS should consider Block Designation of SAFETY Act protections for private sector leaders in standards development for security at multimodal ports.
- DHS also should consider expanding the Resilience STAR Program to include transportation stakeholders with adequately demonstrated competencies in port security and business continuity.

- In developing the National Freight Strategic Plan, the Department of Transportation should give appropriate weight to security considerations, particularly in outlining strategies to improve freight intermodal connectivity.¹⁹

Recommendations for Industry

- Industry should prepare standards and methodologies to optimize both the security and efficiency of global trade practices related to port operations.
- Risk management experts and standards development bodies should support the current effort sponsored by the Department of Transportation's Maritime Administration to develop a Port Investment Toolkit.

Develop a Public-Private “Playbook” for Resilient Trade Flows

Whether natural or man-made, catastrophic events have serious security and economic consequences. When ports and intermodal facilities suffer major damage, the direct costs borne by exporters/importers soon cascade throughout supply chains, and the effects reach well beyond bottom-line accounting. Compromises to the physical infrastructure supporting trade flows — as well as disruptions in their oversight mechanisms — increase risk in other areas, including smuggling of proliferation-sensitive items.

To date, government and industry have had limited success in developing business resumption plans that identify clear, detailed roles and responsibilities.²⁰ Among the challenges are the number of stakeholders involved throughout both government and industry, the sheer volume and speed of cargo throughput, and the many port-to-port variations in governance and other local variables.

Credibly signaling to industry that there would be a serious attempt to bring greater clarity to post-disruption planning could well have the reinforcing effect of prompting greater industry engagement in the process, and thus better results. While the ability to recover more quickly from a major disruption would not reflect a “positive” incentive, it would indeed reflect legitimate value. It also would highlight the advantages of those ports having established and stress-tested detailed business resumption plans.

Findings

- The challenges of coordinating the many public and private stakeholders make emergency restoration of trade flows a critical area to innovate in public-private governance mechanisms in general, and market-based incentives in particular. Effective business resumption planning requires the complete participation of the individual port authorities, whose unique relationships with local port stakeholders are key to securing buy-in from shipping companies, masters and unions.
- Insurers have an important and often overlooked role in assessing the impact of an incident, limiting additional harm and providing immediate financial support to those affected.

Recommendations for Government

- In preparing incident-specific annexes to the National Response Framework, the Federal Emergency Management Agency (FEMA) should include clear guidance on roles and responsibilities for trade flow restoration in different emergency scenarios, both natural and man-made.²¹ As the coordinating agency for the Economic Recovery Support Function, the Department of Commerce should help formulate this guidance by soliciting input from relevant industry stakeholders. FEMA and the Commerce Department should examine how the work on business resumption planning by the COAC and select industry partners could inform the incident annexes.

- FEMA’s National Business Emergency Operations Center should make government-industry coordination in emergency trade resumption a leading priority. To this end, the Center should leverage the relevant COAC-industry efforts to the extent possible.
- The Department of Transportation’s Maritime Administration should work with industry to update the Port Risk Management and Insurance Guidebook and include a new section outlining best practices for trade resumption after natural and man-made disruptions.

Recommendations for Industry

Insurance providers, other maritime industry stakeholders and standards development organizations should explore the viability of insurance and risk management products benchmarked against certified competency in business continuity planning and operations.

Extend the Terrorism Risk Insurance Act and Consider Future Changes

Because terrorism risk cannot be modeled reliably, insurers and reinsurers would not provide the industry-desired level of coverage without government backstopping. Congress passed the Terrorism Risk Insurance Act (TRIA) to provide that backstop, but its authorization expires at the end of 2014.²² Overall, insurers can be efficient “financial first responders” to natural or man-made disasters. While they cannot quantify the threat of terrorism, they can provide policyholders guidance and incentives to reduce other elements of risk before an event.

“[M]arket-based incentives can promote significant changes in business practices and encourage the development of markets such as insurance for cyber, chemical, biological, or radiological risks.”

Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, December 2013

Findings

The Terrorism Risk Insurance Program is a well-conceived effort to realign government and industry incentives so as to enhance both national security and economic competitiveness. However, the program does not specifically address coverage for catastrophic cyber events, as well as nuclear, chemical, biological and radiological (NCBR) events. Similar programs overseas mandate broader coverage.

Recommendations for Government

- Congress should extend TRIA for five years and direct the Treasury Department’s Federal Insurance Office to immediately stand up a multi-stakeholder task force to study possible TRIA program changes and report its findings, including recommended congressional action, within 18 months.

Topics of the study should include: the potential expansion of offered or mandated coverage to include NCBR events and catastrophic cyber events, along with any additional risks that task force members deem worthy of inquiry; specific policy incentives that might be offered to TRIA policyholders that adopt specific security and resilience practices, with a comparative evaluation of both incentives and policyholder practices; and potential increases in the loss threshold above the current level of \$100 million.

Recommendations for Industry

The private sector and broader public should participate in the proposed task force, identifying how other market-based incentives might be introduced into the TRIA regime to enhance national security and promote development of the private market.

Fully Implement The International Trade Data System

Across the US government, 47 agencies have some role in imports or exports.²³ The varied technology platforms, data requirements and associated processes seen across these agencies have caused major inefficiencies for both government and industry. The International Trade Data System (ITDS), under development for years, is intended to remedy these issues by providing a “single window” — a federated clearinghouse through which trade entities can submit, and government agencies can collect, required data. ITDS would enhance export enforcement by providing greater visibility on export transaction data and brokering information to the appropriate agencies for more efficient, effective and domain-specific risk assessment processes and analyses. It therefore would be an asset in preventing proliferation and mitigating other transnational crimes.

In February 2014, President Obama signed an executive order mandating full implementation of ITDS by December 2016 and codifying the role of the BIEC.²⁴ The BIEC brings together senior officials from relevant agencies to oversee ITDS implementation and help advance related border-management and trade-facilitation initiatives — those affecting US imports and US exports alike. The February 2014 directive also mandates the BIEC to engage with industry and other non-governmental entities on ideas that can “improve supply chain management processes, with the goal of promoting economic competitiveness through enhanced trade facilitation and enforcement.” To that end, the BIEC has established an External Engagement Committee as a dedicated mechanism for stakeholder dialogues.

Findings

Full and effective implementation of ITDS would significantly increase efficiency and effectiveness, without affecting existing agency systems for trade data. ITDS would enable both government and industry to leverage a more comprehensive set of trade data to improve supply chain performance, reduce costs and harmonize risk assessment processes. The president’s February 2014 executive order presents an important opportunity for mutually beneficial public-private cooperation toward those objectives.

Recommendations for Government

- The White House should closely monitor implementation of the February 2014 executive order — not only to ensure deployment of full and effective ITDS functionality on schedule, but also to drive progress on the broader mandates of the BIEC to engage industry and other stakeholders for modernized trade and enforcement processes. Leveraging the BIEC for a more integrated government approach to “trusted trader” regimes is one of the primary ways agencies can satisfy the executive order’s requirements in this regard.
- Before mandating that industry submit additional data elements in export/import processes, CBP and other affected agencies should ensure such action

would not undermine the executive order’s goal of “a reduction of unnecessary procedural requirements that add costs to both agencies and industry.”

Recommendations for Industry

Industry should continue its active participation in ITDS pilots and provide ongoing feedback to ensure ITDS remains a technology-neutral, interoperable and efficient platform for trade facilitation as well as data integration and sharing.



ACHIEVING GENUINE SECURITY AMID
A RANGE OF COMPLEX CROSS-BORDER THREATS
REQUIRES NEW PARTNERS
AND NEW MODELS FOR
ENGAGING THOSE PARTNERS.

CONCLUSION

Globalization of trade and commerce has changed the nature of governance itself. Top-down regulatory and enforcement tools cannot keep pace with contemporary technological change or with the speed and volume of global freight movement. Achieving genuine security amid a range of complex cross-border threats requires new partners and new models for engaging those partners. Perhaps most important, it requires a deep and diverse set of industry partnerships.

Our recommendations highlight a range of pragmatic, actionable steps toward this end. They would better align industry profitability and public security as mutually reinforcing goals in global business operations, principally through non-regulatory means. We do not presume that this approach offers a panacea. But it will be an essential part of any successful security strategy in the 21st century.

Now is the time for decisive steps toward a new paradigm in public-private partnerships.

Endnotes

¹ Executive Order 13659. “Streamlining the Export/Import Process for America’s Businesses.” *Federal Register* 79, no. 37 (February 19, 2014). Accessed February 25, 2014. <http://www.gpo.gov/fdsys/pkg/FR-2014-02-25/pdf/2014-04254.pdf>.

² For instance, industry members of the COAC recently developed a set of principles for improving interagency and public-private coordination on export regimes, including “the strategies associated with the National Export Initiative (NEI) and Export Control Reform (ECR).” See: COAC. Sub-committee on Exports. *Master Principles for a One U.S. Government at the Border Cooperation for Exports*. February 2014. Accessed February 27, 2014. http://www.cbp.gov/sites/default/files/documents/export_master_principles.pdf.

³ US Department of Commerce (DOC), Bureau of Industry and Security. *BIS ‘Best Practices’ for Industry to Guard Against Unlawful Diversion through Transshipment Trade*. August 2011. Accessed October 11, 2013. http://www.bis.doc.gov/index.php/forms-documents/doc_view/625-best-practices.

⁴ Ibid., 13.

⁵ Ibid.

⁶ US DOC. Bureau of Industry and Security. *Freight Forwarder Guidance*. February 2012. Accessed October 14, 2013. https://www.bis.doc.gov/index.php/forms-documents/doc_view/620-new-freight-forwarder-guidance.

⁷ Executive Order 13659, “Streamlining the Export/Import Process.”

⁸ In February 2014, the Commerce Department’s Bureau of Industry and Security (BIS) issued a Proposed Rule that would add the term “Foreign Principal Party Controlled Export Transaction” to describe the transactions currently permitted under section 758.3(b) of the Export Administration Regulations (EAR) and described as “routed export transactions.” BIS proposed this change to remedy confusion owing to the Census Bureau’s distinct definition of “routed export transactions” in the Foreign Trade Regulations (FTR) when specifying who must file the required information in the Automated Export System for a given transaction. If the proposed rule were implemented, the term “routed export transaction” would remain in use only in the FTR, and all appearances of the term in the EAR would be replaced with “Foreign Principal Party Controlled Export Transaction.” See: US DOC. Bureau of Industry and Security. “Delegation of License Requirements Determination and Licensing Responsibility to a Foreign Principal Party.” *Federal Register* 79, no. 25 (February 6, 2014). Accessed February 25, 2014. <http://www.gpo.gov/fdsys/pkg/FR-2014-02-06/pdf/2014-01176.pdf>.

⁸ Examples include Project Guardian, an initiative of the Commerce Department, and Project Shield America, an initiative of the Department of Homeland Security.

¹⁰ Such a framework would build on guidance for developing industry partnerships that the National Security Council issued last year. The guidance encouraged agencies to clearly convey what authorities they possess, and what constraints they must respect, to private sector interlocutors. It also encouraged process-related steps, such as agency development of pre-cleared Memoranda of Understanding that can be used in support of industry partnerships. See: The White House. *Building Partnerships: A Best Practices Guide*. April 2013. Accessed January 13, 2014. http://www.colorado.feb.gov/useruploads/files/white_house_-_building_partnerships_best_practices.pdf.

¹¹ Government could provide such feedback in various ways and with various levels of specificity. One recent example that is relatively formal and specific is a statement the Department of Justice (DOJ) and Federal Trade Commission (FTC) issued jointly to underscore that they “do not believe

that antitrust is — or should be — a roadblock to legitimate cybersecurity information sharing” among private sector entities. The statement built on a previous, more general set of guidelines the agencies issued to address when antitrust concerns arise in private sector collaborations. See: US DOJ and US FTC. *Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information*. April 2014. Accessed April 12, 2014. <http://www.justice.gov/atr/public/guidelines/305027.pdf>; US FTC and US DOJ. *Antitrust Guidelines for Collaborations Among Competitors*. April 2000. Accessed April 12, 2014. <http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>.

¹² US Office of Management and Budget. *Memorandum M-13-13: Open Data Policy – Managing Information as an Asset*. By Burwell, Sylvia, Steven VanRoekel, Todd Park, and Dominic Mancini. May 2013. Accessed November 28, 2013. <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>.

¹³ As required by the Government Performance and Results Modernization Act of 2010 (Public Law 111-352), the Executive Office of the President periodically sets, and then tracks progress on, Cross-Agency Priority (CAP) Goals in a limited number of crosscutting policy and management areas. First mandated by Executive Order 13642 (“Making Open and Machine Readable the New Default for Government Information,” May 2013), the CAP Goal on “Open Data” was explained further in the administration’s Fiscal Year 2015 budget documents.

¹⁴ Executive Order 13653. “Preparing the US for the Impacts of Climate Change.” *Federal Register* 78, no. 215 (November 1, 2013). Accessed December 18, 2013. <http://www.gpo.gov/fdsys/pkg/FR-2013-11-06/pdf/2013-26785.pdf>.

¹⁵ Office of the Director of National Intelligence. Program Manager for the Information Sharing Environment. *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding*. By Paul, Kshemendra. December 2013. Accessed February 3, 2014. https://mise.mda.gov/drupal/sites/default/files/20140103%20Final%20NSISS%20Strategic%20Implementation%20Plan_0.pdf.

¹⁶ This research would serve as a useful complement to current industry, government and public-private efforts, such as the work of the Emerging Technology and Research Advisory Committee at the Commerce Department.

¹⁷ Particularly in cases when this third-party option is employed entirely independent of government, participating industry stakeholders should take all necessary steps to ensure that the types of information they exchange do not raise concerns regarding antitrust or related issues. See: FTC-DOJ, *Antitrust Guidelines for Collaborations Among Competitors*; DOJ-FTC, *Antitrust Policy Statement on Sharing of Cybersecurity Information*.

¹⁸ The White House. *National Strategy for Global Supply Chain Security – Implementation Update*. January 2013. Accessed September 24, 2013. http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf.

¹⁹ Section 1115 of the Moving Ahead for Progress in the 21st Century Act (MAP-21; Public Law 112-141) mandates the Department of Transportation to produce a National Freight Strategic Plan by July 2015. The plan is required to include “strategies to improve freight intermodal connectivity.”

²⁰ Area Maritime Security Committees (AMSCs), for example, have been one of several venues where government and industry have engaged in recent years on business resumption issues. Pursuant to section 102 of the Maritime Transportation Security Act of 2002 (Public Law 107-295), the US Coast Guard has established 43 AMSCs, covering all 361 US seaports. AMSCs bring together disparate port stakeholders, including law enforcement officials and industry representatives, to share information, assess risks and conduct exercises in support of their respective Area Maritime Security Plans. As codified at 46 USC 70103(b)(2), Area Maritime Security Plans must include “response and

recovery protocols to prepare for, respond to, mitigate against, and recover from [an incident]... as efficiently and effectively as possible.”

²¹ According to the Government Accountability Office (GAO), FEMA officials plan to complete these annexes by Fiscal Year 2017. See: US GAO. *National Preparedness: Actions Taken by FEMA to Implement Select Provisions of the Post-Katrina Emergency Management Reform Act of 2008*. Report no. GAO-14-99R. Washington, DC: GAO, November 2013: 10. Accessed February 4, 2014. <http://www.gao.gov/assets/660/659242.pdf>.

²² The original TRIA (Public Law 107-297) was enacted in November 2002. The law also is referred to sometimes as TRIPRA, for the Terrorism Risk Insurance Program Reauthorization Act of 2007 (Public Law 110-160), which authorized the program through December 2014.

²³ *Participating Government Agencies in ITDS*. International Trade Data System Board of Directors, May 2012. Accessed December 10, 2013. http://www.itds.gov/linkhandler/itds/toolbox/organization/pgas/pgs_roster.ctt/pgs_roster.pdf.

²⁴ Executive Order 13659, “Streamlining the Export/Import Process.”

Project Staff

Brian Finlay

Nate Olson

Debra Decker

Gerson Sher

ACKNOWLEDGEMENTS

This compact document runs dense with the valuable ideas — some featured explicitly, but most reflected implicitly — of far too many participants from industry and government for the space here to accommodate. Suffice it to say that we at Stimson are excited to continue our work with many of them, as well as new partners, in the months and years ahead.

For the financial support that made this work possible, our deepest thanks go to Emma Belcher and the John D. and Catherine T. MacArthur Foundation; Carl Robichaud and the Carnegie Corporation of New York; and the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC), Center on Contemporary Conflict, Naval Postgraduate School.

The distinguished members of the Task Force that guided this project gave selflessly of their time and insights, and showed a striking enthusiasm for tackling tough issues. I wish particularly to thank Jay Cohen (RADM, USN, Ret) and Stimson Center co-founder Barry Blechman, respectively Task Force Chair and Vice Chair. They each brought a lifetime of expertise and practical know-how, along with patience and good humor, to this effort. It was a privilege to work with them.

For that privilege — and the many others that came with this work — I am indebted especially to Brian Finlay, managing director of the Stimson Center and director of the Center's Managing Across Boundaries Initiative. By entrusting me with a role in making his vision for Partners in Prevention a reality, he gave me an opportunity for which I remain most grateful.

Finally, a wonderful team at Stimson was instrumental to the success of this project. Debra Decker, Gerson Sher, Shannon Dick and Alex Georgieff each invested countless hours on all fronts — from helping shape some of the major ideas submitted to the Task Force, to assisting with background research, to meticulously reviewing and editing drafts. Sincere thanks also to Lita Ledesma for the superlative visual design of this report.

Nate Olson
Project Manager

Making Public-Private Security Cooperation More Efficient, Effective and Sustainable

A global economy has empowered criminals and terrorists on a global scale. Embedded across far-flung production, trade and investment networks, illicit trafficking in high-tech data and equipment, narcotics, arms and counterfeit goods has laid bare the weaknesses of top-down government controls. The challenges of preventing illicit transshipment and other misappropriations of sensitive technologies have never been more urgent.

In this report, Stimson's Partners in Prevention Task Force presents its final recommendations to US government and industry stakeholders for combating these threats through public-private partnerships that more effectively harness the power of decentralized, market-based incentives. Individually actionable but collectively diverse, these seven targeted proposals follow an 18-month Stimson collaboration with hundreds of industry partners spanning high-tech manufacturers and service providers, transport and logistics firms, and insurance providers.

With the rise of a global marketplace, finding more innovative ways to leverage the resources, agility and expertise of the private sector is essential – and not just for “security,” narrowly understood. It will also go far in shaping the future of US global influence and leadership. The Task Force proposals connect that strategic imperative with pragmatic steps forward.