PREPAREDNESS, RESPONSE, AND RESILIENCE TASK FORCE

Operationalizing Resilience:

A Systems-based Approach Emphasizing Risk Management is Required

Task Force Co-Chairs
Michael Balboni
Daniel Kaniewski
R. David Paulison

THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY POLICY INSTITUTE

October 13, 2011

Founded in 2003, ***the George Washington University Homeland Security Policy Institute*** *(HSPI) is a nonpartisan "think and do" tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation.*

HSPI's ***Preparedness, Response, and Resilience Task Force*** *brings together experts from government, academia, and the private and non-profit sectors to consider contemporary policy issues facing the homeland security, first responder, and emergency management communities. To this end, the Task Force convenes sessions with policymakers and publishes policy papers and reports with actionable policy recommendations for the future. The Task Force is predicated on the idea that a more nuanced approach to these policy issues can contribute to a greater level of resiliency for all levels of government, the private sector, and the public writ large.*

Recent considerations of the Task Force include the meaning of resiliency; the critical junctures that exist between policy and implementation; the nexus between preparedness, response, and resilience; and the future of resiliency as it relates to a diverse and changing operational environment.

While consensus positions were sought and often achieved, the Task Force Co-Chairs take full responsibility for the opinions and recommendations herein.

Comments should be directed to hspi@gwu.edu. For more information on HSPI and its programs, please visit http://homelandsecurity.gwu.edu.

ISBN: 978-0-9839904-1-3

Support provided by

ICF INTERNATIONAL

Preparedness, Response, and Resilience Task Force

Co-Chairs

Michael Balboni*
Former Deputy Secretary for Public Safety, State of New York;
Former New York State Senator

Daniel Kaniewski
Deputy Director, Homeland Security Policy Institute;
Assistant Vice President for Homeland Security, The George Washington University;
Former Special Assistant to the President for Homeland Security, The White House

R. David Paulison**
Former Administrator, Federal Emergency Management Agency;
Former Administrator, U.S. Fire Administration;
Former Fire Chief, Miami-Dade County (Florida) Fire Rescue Department

Members

Raphael Barishansky*
Chief of Public Health Emergency Preparedness, Prince George's County (MD) Health Department

Chris Battle*
Partner, Adfero Group;
Former Chief of Staff, U.S. Immigration and Customs Enforcement

Michael Bopp
Partner, Gibson, Dunn & Crutcher LLP;
Former Associate Director, Office of Management and Budget;
Former Staff Director, Senate Homeland Security and Governmental Affairs Committee

Marko Bourne
Principal, Booz Allen Hamilton;
Former Director of Policy and Program Analysis, Federal Emergency Management Agency

Carlos Castillo
Senior Advisor, PricewaterhouseCoopers, Washington Federal Practice;
Former Assistant Administrator, Federal Emergency Management Agency; Former Director, Miami-Dade County Office of Emergency Management

Sharon Caudle*
Younger-Carter Distinguished Policymaker in Residence, Texas A&M University; Former Assistant Director, Homeland Security, Government Accountability Office

Rich Cooper*
Vice President, Research & Emerging Issues, U.S. Chamber of Commerce National Chamber Foundation;
Principal, Catalyst Partners, LLC

Darrell Darnell*
Senior Associate Vice President for Safety and Security, The George Washington University;
Former Director of Resilience Policy, National Security Staff, The White House;
Former Director, DC Homeland Security and Emergency Management Agency

Harvey Johnson
Vice President, BAE Systems;
Former Deputy Administrator, Federal Emergency Management Agency;
Vice Admiral, U.S. Coast Guard (Ret.)

Mick Kicklighter
Director, Center for Infrastructure Protection and Homeland Security, School of Law, George Mason University; Former Inspector General, Department of Defense; Lieutenant General, U.S. Army (Ret.)

Alan McCurry**
Former Chief Operating Officer, The American Red Cross

Kirstjen Nielsen*
Managing Director and General Counsel, Civitas Group; Former Special Assistant to the President for Homeland Security, The White House

John Paczkowski*
Vice President, ICF International;
Former Director, Emergency Management and Security at Port Authority of New York and New Jersey

Kenneth Rapuano
Director of Advanced Systems & Policy, MITRE;
Former Deputy Assistant to the President, The White House

Peter Roman
President, WIT Consulting, LLC

Scott Somers
Vice Mayor, City of Mesa, Arizona;
Member, Urban Search and Rescue Arizona Task Force #1

Adam Thiel**
Fire Chief, City of Alexandria, Virginia

Tevi Troy*
Senior Fellow, Hudson Institute; Former Deputy Secretary, Department of Health and Human Services

David Trulio*
Director, Federal / Civil Programs, Raytheon Company; Former Special Assistant to the President and Executive Secretary, Homeland Security Council, The White House

Bert Tussing*
Director, Homeland Defense and Security Issues, Center for Strategic Leadership, U.S. Army War College

Task Force Staff

Keith Stefanelli
HSPI/ICF Resilience Scholar

**Denotes HSPI Senior Fellow*
***Denotes HSPI Steering Committee Member*

Executive Summary

In our May 2011 Interim Report on Resilience, the HSPI Preparedness, Response, and Resilience Task Force called on national policymakers and homeland security practitioners to move beyond the conceptual discussion of resilience and advance practical and tangible means to realize resilience aims. The development of the National Preparedness System, as called for by Presidential Policy Directive-8 (PPD-8), National Preparedness, represents an opportunity to achieve these goals. In this paper the Task Force argues that to achieve the aims of PPD-8, policymakers must:

- **Harmonize and integrate the planning frameworks** in the National Preparedness System called for by PPD-8 at both the Federal interagency and State and local levels of government **using a systems-based approach.** A systems-based approach is essential to avoiding the creation of new independent silos of activity that will only make whole-of-government and whole community preparedness and resilience all that more difficult to attain.

- **Collaboratively develop and incentivize the use of risk management practices** for preparedness and resilience. These practices should guide integrated Federal, State, and local government and private sector planning and decision-making across the PPD-8 frameworks; be adaptable to suit unique circumstances; and allow for the strategic comparison of risks among a range of threats and hazards.

- **Enhance risk communication** across the entire homeland security enterprise, and especially with State and local governments, the private sector, non-profit and community groups, and the public at large. This should be accomplished by engaging in candid and transparent conversations regarding significant risks and associated consequences.

Introduction

In our Interim Report on Resilience, the HSPI Preparedness, Response, and Resilience Task Force cited the need for national policymakers and homeland security practitioners to move beyond the conceptual discussion of resilience and advance practical and tangible means to realize its intended aims.[1] The Task Force believes that resilience can indeed be operationalized and that the means to do so are already in existence. In point of fact, many communities already have built resiliency into their operations.[2] However, existing processes and practices are not sufficiently robust, nor are they harmonized and integrated to the degree necessary to achieve unity of effort across the homeland security enterprise or provide the "all-of-nation" unity of purpose called for by Presidential Policy Directive-8 (PPD-8), National Preparedness, issued March 30, 2011.[3]

It is the position of the Task Force that resilience will be best achieved by 1) harmonizing and integrating the planning frameworks called for in PPD-8, using a systems-based approach, 2) collaboratively developing and incentivizing the use of risk management practices for preparedness and resilience that guides integrated Federal, State, and local government and private sector planning and decision-making, and 3) enhancing risk communication by engaging in candid conversation about risk with all affected stakeholders, particularly non-government partners.

Integrating Elements of the National Preparedness System through a Systems-Based Approach

The successful application of a systems-based approach to problem-solving takes a holistic view of the problem space and recognizes the interdependencies between and among the various components of the system. Addressing any one aspect of the system in isolation can have unintended consequences on the others, at best resulting in suboptimal solutions and at worst creating the potential that a significant interdependency will go unaddressed. In homeland security, that could mean lives lost and vital infrastructure destroyed or damaged and out-of-commission for an extended period of time.

---

[1] HSPI Preparedness, Response, and Resilience Task Force, *Interim Task Force Report on Resilience* (Washington: HSPI, May 2011), available at http://www.gwumc.edu/hspi/policy/report_Resilience1.pdf.
[2] See, for example, the research of the Community and Regional Resilience Institute, available at http://www.resilientus.org/divisions/community-resilience-research.html.
[3] *Presidential Policy Directive-8, National Preparedness* (Washington: The White House, March 30, 2011), available at http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm. PPD-8 was released at a Homeland Security Policy Institute event; see http://www.gwumc.edu/hspi/events/PPD8_national_preparedness302.cfm.

The relationship between infrastructure (i.e., "hard") resilience, and societal (i.e., "soft") resilience is an apt example of the notion applied to the homeland security domain. The expectations of the public regarding the availability and functioning of lifeline infrastructure during or immediately following an event will vary significantly based upon the levels of preparedness and resilience in communities. The better the understanding of the practical limits on governments and the private sector to maintain or rapidly replace lifelines during or after disasters, the more likely communities and families are to develop the means to minimize and absorb loss of critical services and other stresses. On the other hand, an integrated approach to risk assessment and planning across the infrastructure protection and emergency management communities would optimize the perspectives and capabilities of both, resulting in more coordinated efforts toward risk mitigation and the building of preparedness capabilities.

Among the major challenges of the Department of Homeland Security (DHS) are its sheer size and the autonomous nature of its components that at times tend to fragment what should otherwise be synchronous and coordinated effort. In fairness, DHS and the homeland security enterprise writ large are still in a relatively early phase of development, and many DHS components are still highly focused on – and accountable for – addressing the specific mission functions for which they are directly responsible, rather than the system as a whole. Not unlike their Defense counterparts before the Goldwater-Nichols Department of Defense Reorganization Act of 1986, at this early stage of maturity, DHS components tend to operate under the notion that individual agencies' "ownership" of a homeland security mission or activity is exclusive, and they therefore do not see the functions they perform as part of an overall large system for national preparedness and resilience. In the absence of a systems-based approach, the instincts to preserve operational "turf" and protect budget funding create poor collaborative behaviors and less than a total whole-of-government result.

PPD-8, issued just over seven months ago, offers a unique but limited window of opportunity to re-engineer our approach to homeland security in a way that addresses these challenges. The first iteration of a new National Preparedness Goal has already been published under the auspices of PPD-8.[4] The real work – and the real opportunity – comes in the form of the development and integration of a new National Preparedness System, a description of which is due to the White House in late November, and the development of which will take place in the months that follow. The National Preparedness System will include a series of five national planning

[4] *National Preparedness Goal, First Edition* (Washington: The Department of Homeland Security, September 2011), available at http://www.fema.gov/pdf/prepared/npg.pdf.

frameworks associated with the five homeland security mission areas defined in PPD-8.[5]

The development and integration of the frameworks requires a systems-based approach. In order to strengthen the security and resilience of the United States as directed by PPD-8, decision-makers responsible for particular mission areas and functions must understand the relationships, interdependencies, and possible cascading effects across the homeland security enterprise writ large. Today, too many efforts in these different areas are conducted independent of one another, and therefore are often insensitive to downstream implications that impact other preparedness functions. The amount of investment in the protection or redundancy of lifeline infrastructure such as water or power, for example, can have significant implications for the prioritization of response capabilities to augment or reconstitute these functions.

The benefits of a systems-based approach are further underscored during times of fiscal austerity. When vast resources can be allocated across the array of functions that comprise the five homeland security mission areas, progress can be achieved, albeit inefficiently, without the full integration of efforts. This is essentially what occurred in the years immediately following 2001. Ten years later, however, as all homeland security stakeholders are increasingly faced with tighter budgets, the optimization of resource allocation across homeland security mission areas becomes vital. Decision-makers must better understand the relative return on investments for preparedness efforts – both within individual missions and as compared to other homeland security functions – in order to make informed decisions that drive toward true efficiency.

A systems-based approach will allow the frameworks to account for the interdependencies among the homeland security mission areas, recognize the relationships between "hard" and "soft" resilience, and drive preparedness investments towards better optimization. The National Disaster Recovery Framework (NDRF), already well underway prior to the release of PPD-8, was published in September.[6] Policymakers now have the challenge of ensuring the remaining frameworks, including a revision of the National Response Framework, are integrated with each other. A systems-based approach will aid this effort.

[5] PPD-8 indicates that the integrated national planning frameworks are to cover prevention, protection, mitigation, response, and recovery.
[6] *National Disaster Recovery Framework* (Washington: The Department of Homeland Security, September 2011), available at http://www.fema.gov/recoveryframework.

Risk Management: The Underlying Business Case

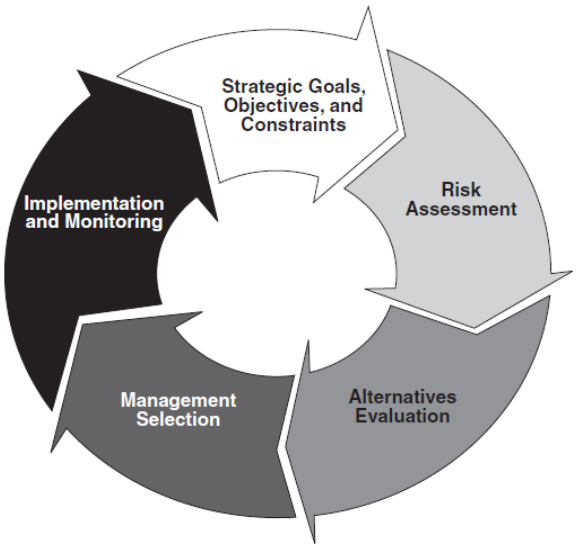
It is important to draw a clear distinction between risk assessments and risk management.

Risk assessments are based upon inputs and analytics, and they should be adaptable to account for different contexts and associated functional requirements for interpreting risk. Different homeland security contexts will require different approaches and even different time horizons for assessing risk. For example, risk assessments of airline passengers will, by their nature, be different from risk assessments for maritime cargo. Cyber security risks will be different from those associated with assessing public health or bio-terrorism threats.

While the homeland security domain is diverse and will therefore require a diverse set of approaches to risk assessment, the fundamental framework underlying risk management is universal. Any robust risk management framework involves a number of steps beginning with an assessment of risk spanning a range of threats and/or hazards, planning to formulate strategy in response to those risks, analysis of gaps in capabilities or needed threat mitigation measures, the risk-informed application of limited resources to address those gaps, and the measurement of performance as the basis for managing continuous improvement. The process is iterative, and the ultimate measures of risk management performance are the development of needed capabilities and the mitigation of priority hazards in ways that achieve measurable reduction in relative risk over time with each round of the cycle. The Government Accountability Office (GAO)[7] and others[8] have, several times over the last decade, called for a consistent risk management process to be employed across the homeland security enterprise, and the GAO's simple model ably represents the concept.

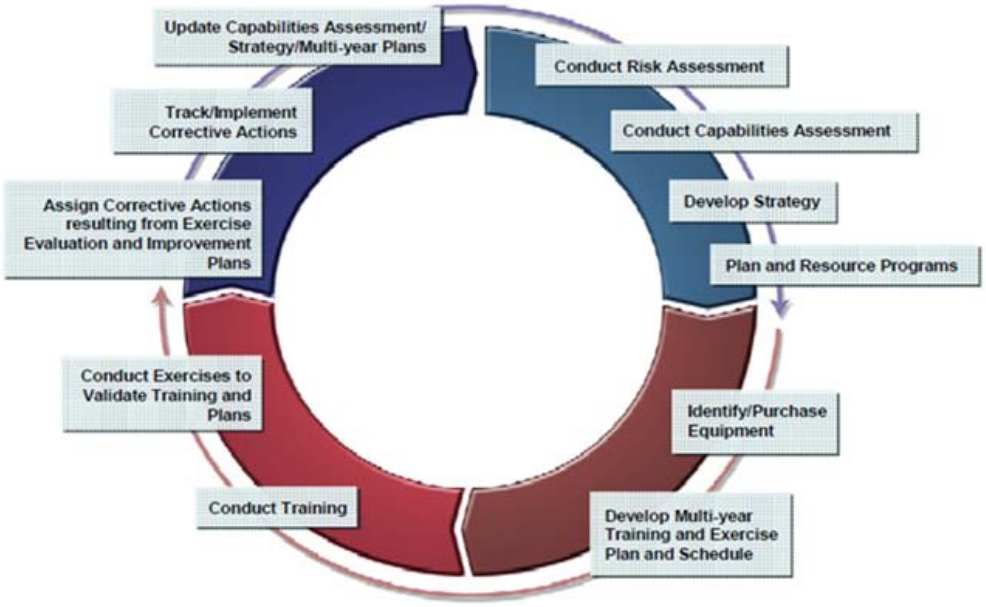
[7] U.S. Government Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington: GAO, December 2005), available at http://www.gao.gov/new.items/d0691.pdf; *Highlights of a Forum: Strengthening the Use of Risk Management in Homeland Security* (Washington: GAO, April 2008), available at http://www.gao.gov/new.items/d08627sp.pdf; *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security* (Washington: GAO, June 2008), available at http://www.gao.gov/new.items/d08904t.pdf; *Quadrennial Homeland Security Review: Enhanced Stakeholder Consultation and Use of Risk Information Could Strengthen Future Reviews* (Washington: GAO, September 2011), available at http://www.gao.gov/new.items/d11873.pdf.

[8] As an example, see Homeland Security Studies and Analysis Institute, *Risk and Resilience: Exploring the Relationship* (Arlington, VA: HSI, November 22, 2010), available at http://www.homelandsecurity.org/hsireports/Risk-Resilience_Report_Final_public%20release%20version%20_Task_10-17_29-Nov-2010.pdf.



The GAO Risk Management Framework[9]

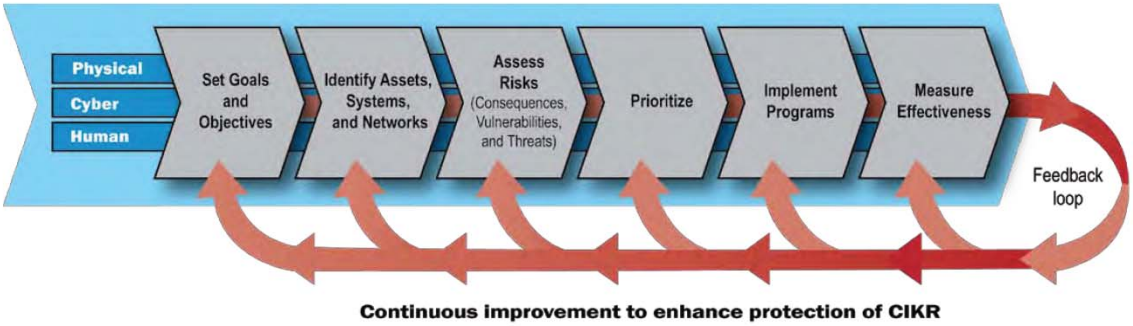
Indeed, a similar construct was found in previous iterations of the Target Capabilities List, the companion document to the National Preparedness Guidelines which was issued under the auspices of Homeland Security Presidential Directive-8 and most recently updated in September 2007. [10]



The Preparedness Cycle found in the original Target Capabilities List

[9] U.S. Government Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington: GAO, December 2005), available at http://www.gao.gov/new.items/d0691.pdf.
[10] *National Preparedness Guidelines* (Washington: The Department of Homeland Security, September 2007), available at http://www.fema.gov/pdf/government/npg.pdf.

Meanwhile, the risk management framework outlined in the 2009 National Infrastructure Protection Plan (NIPP) is likewise a similar-looking process for continuous assessment and improvement specific to physical facilities and assets. The NIPP identifies risk as "an important means of prioritizing mitigation efforts for partners ranging from facility owners and operators to Federal agencies."[11] The risk management framework promoted by the NIPP is aimed at enabling "risk-informed decision-making" related to the nation's critical infrastructure and key resources.



The NIPP Risk Management Framework[12]

Both the preparedness cycle used by the emergency management community and the risk management framework in the NIPP are intended to be risk-based, span the spectrum of all-hazards, and are designed to identify and mitigate gaps across the homeland security mission areas. Despite their similar intent and construct, they have evolved largely independently of one another, and their application tends to be biased in the direction of the community owning and applying them. As a result, core homeland security risk management efforts in infrastructure protection and disaster response and recovery are not synchronized.

A consistent risk management framework applied at the State and local levels across the PPD-8 frameworks can provide the common ground for unity of effort, which is essential to the "whole community" and "all-of-nation" approach to resilience that is now the central theme of national homeland security policy. The preparedness cycle and NIPP risk management framework are compatible ideas and simply require the institutional will needed to harmonize them.

Planning under the auspices of the Federal Emergency Management Agency's Comprehensive Planning Guidance 101 is already underway at the State and local

[11] *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington: The Department of Homeland Security, 2009), 27, available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
[12] *NIPP*, 4.

level, but is largely response-focused.[13] To achieve targeted improvements in preparedness and resilience, it must be modified to account for regional interdependencies and to support risk-based decision-making and resource allocation across all of the PPD-8 frameworks.

The DHS Office of Risk Management and Analysis has offered yet another new though similar construct in its release of risk management doctrine earlier in 2011. This framework may provide the universal basis for harmonizing and integrating risk management practices.

The RMA Risk Management Process[14]

A consistent risk management process must be at the heart of the systems-based approach to the integrated frameworks called for by PPD-8. Use of risk management will enhance decision-making at all levels by prioritizing threats based upon their levels of risk, identifying the capabilities needed to address those risks, and ultimately providing a method for tangibly measuring the relative reduction in risk over time. Furthermore, applying risk management provides jurisdictions a practical method for prioritizing those capabilities that provide the best return on investment in aligning risk to a level acceptable to the jurisdiction. Doing so in the context of the application of a systems-based approach ensures recognition of the effect that an investment will have on the system as a whole and not on one mission area or one geographic area alone. A jurisdiction may invest in a specific capability independently, identify relevant capabilities in nearby jurisdictions, or work with the private sector, non-profit

[13] Federal Emergency Management Agency, *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101 Version 2.0* (Washington: The Department of Homeland Security, November 2010), available at: http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf.
[14] The Office of Risk Management and Analysis, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington: The Department of Homeland Security, April 2011), 16, available at http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

sector, or Federal partners to ensure the delivery of that capability. Finally, and importantly, employing risk management helps to identify those capabilities that either do not exist or are not realistically attainable in the needed timeframe. Disaster response decision-makers must recognize these gaps in capabilities as "deltas" to be managed in coordinating an all-of-nation response.

Lastly, it is important to recognize that wide variances in both perceptions and tolerance of risk by the public are a challenge to employing risk management, as is complacency. Risk is experientially based. The longer it has been since the last consequential hurricane and the more "false alarms" since, the less likely it is that the public will follow preparedness and emergency guidance. Furthermore, from a political standpoint, elected officials tend not to emphasize the communication of lower probability, higher consequence risks, and will often focus on hazards that the public incorrectly perceives to be the riskiest. As we pointed out in our Interim Report, elected officials and the public they represent are highly reluctant to define acceptable thresholds of risk or consequence.[15] Overall, decision-makers in elected and appointed positions and other leaders in localities, States, and the Federal government need a better understanding of how to communicate relative risk and prudent preparedness actions to inform candid conversations with the public about acceptable levels of risk.

Recommendations

The Task Force puts forth the following three recommendations for policymakers to consider during the implementation of PPD-8 and beyond.

Recommendation 1: *Harmonize and integrate the planning frameworks in the National Preparedness System called for by PPD-8 at both the Federal interagency and State and local levels of government using a systems-based approach. A systems-based approach is essential to avoiding the creation of new independent silos of activity that will only make whole-of-government and whole community preparedness and resilience all that more difficult to attain.*

PPD-8 implementation offers a rare opportunity for DHS to further integrate its mission areas in such a way that allows for decision-makers at all levels of government to realize the fullest return on their preparedness investments. The frameworks must be developed with the recognition that each one has an effect on all the others.

[15] *Interim Report,* 16.

Recommendation 2: *Collaboratively develop and incentivize the use of risk management practices for preparedness and resilience. These practices should guide integrated Federal, State, and local government and private sector planning and decision-making across the PPD-8 frameworks; be adaptable to suit unique circumstances; and allow for the strategic comparison of risks among a range of threats and hazards.*

Risk management must be a cornerstone of homeland security, and PPD-8 offers the opportunity to further promulgate its application throughout all levels of government. In coordination with risk managers across all sectors and at all levels, the homeland security enterprise should collaboratively implement a consistent risk management process that supports priorities of importance to individual communities and promote it as an underlying business process for decision-makers.

Recommendation 3: *Enhance risk communication across the entire homeland security enterprise, and especially with State and local governments, the private sector, non-profit and community groups, and the public at large. This should be accomplished by engaging in candid and transparent conversations regarding significant risks and associated consequences.*

Risk is not a well-understood concept, but it can become better understood within the homeland security enterprise and with the public writ large by engaging in frank and direct conversations about risks and tradeoffs, and encouraging the collaborative identification of acceptable risk thresholds. PPD-8 calls for a "comprehensive campaign to build and sustain national preparedness, including public outreach and community-based and private-sector programs to enhance national resilience." DHS should use the campaign to further promulgate the concept of risk within the homeland security enterprise and to further educate security stakeholders, including the public as a whole, on the concept of risk. Significantly, DHS need not, and should not, be the exclusive face of this effort – for example, when addressing certain sensitive issues susceptible to mischaracterization or distortion, there is an important role to play in this campaign for prominent former government officials and other non-governmental voices.

Conclusion

We have made much progress as an enterprise since 2001. By advancing the homeland security missions with a systems-based approach, employing consistent risk management practices across the homeland security enterprise, and enhancing risk communication efforts, we can better achieve resilience. Given PPD-8 implementation, now is an appropriate time to make these advancements.

THE GEORGE WASHINGTON UNIVERSITY

HOMELAND SECURITY POLICY INSTITUTE