Enhancing the Organization of the United States Department of Homeland Security to Account for National Risk

By Michael H. Brody
Enhancing the Organization of the United States Department of Homeland Security to Account for National Risk

By Michael H. Brody

Suggested Citation

Abstract

The Department of Homeland Security (DHS) must enhance its organization to more fully account for, align resources against, and act on the prioritized risks of the homeland security enterprise. This will require: (1) enhanced regionalization of DHS, achieved through the networking of stakeholders within and between DHS operational regions; (2) creation of trans-regional, multi-functional, priority-risk-based authorities for the Secretary of DHS; and (3) establishment of statutorily defined, joint operational authorities for the Department. To substantiate this argument, this article: first, reviews a set of factors which define why DHS faces this problem, and how there are growing, serious demands to solve this problem; second, presents a case-study of the United Kingdom’s method for establishing national risk priorities; third, identifies the characteristics of an enhanced organizational model for DHS; and, fourth, delivers a set of recommendations for the enhancement of the Department’s organization to account for national risk.

Introduction

The Department of Homeland Security (DHS) must fully account for, align resources against, and act on the prioritized risks of the homeland security enterprise. This article argues that DHS must enhance its organizational structure to establish a common method to assess and prioritize risk across the Department’s mission areas, which incorporates all DHS stakeholders in the process.

This will require three major reforms. First, the department must be regionalized effectively through the networking of stakeholders within and between DHS operational regions. Second, the department must create trans-regional, multi-functional, priority-risk-based (TMP) authorities for the Secretary of DHS, empowering the Secretary to allocate/reallocate select assets, personnel and resources, nationwide, on a fixed-term basis, to align effectively the Department’s authorities and resources within and between operational regions to best support the risk mitigation networks established under this new form of network-federalist national security strategy. Legislation would likely be required to empower the Secretary, and perhaps the Deputy’s Management Action Group (DMAG) with the authority to resolve differences and establish priorities for missions that cut across different DHS components, missions, and regions. This course of action would place the Secretary and, by extension the DMAG, in a more direct, joint leadership role in ongoing DHS operations. Such authority would serve to accelerate DHS decision-making and response times, precluding or truncating prolonged DHS headquarters vs components conflicts in Washington, DC, as well as fights between components’ headquarters and their own regional offices. It would
allow for the clear definition and enforcement of priorities across the Department. The third needed reform is the establishment of statutorily defined, joint operational authorities for the Department. While DHS operational components certainly possess the ability, will, and authority to partner with one another on, for example, the current Joint Task Forces in operation nationwide focused on border security and immigration enforcement, they lack strong, permanent authorities to fund and fully enable such joint operations and make them truly “joint.” Stated differently, DHS joint operations are rooted in good will and the strength of direction from a given DHS Secretary and DHS Component leaders.

Organization of Analysis

First, this article reviews a set of factors and trends which collectively establish why we have the problems outlined above, demonstrates why there are growing, serious demands to solve this problem, and provides a rationale for enhancing the organization of DHS to account for, prioritize, and act on national risk through the use of networks, regions, and new authorities. Second, the article will present a case-study of the United Kingdom’s method and organization for establishing national risk priorities as a useful way to identify potential U.S. organizational enhancements. Third, it recommends additional concepts for the enhancement of the Department’s organization to account for national risk, including new authorities and organizational models.

The Problem

The Department’s inability to address the problems of coordinating and establishing risk-based priorities across the Department, and more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions, stems from four main factors, including: (1) U.S. constitutional federalism and the dynamic nature of that system; (2) a lack of a standard methodology to prescribe absolute risk values applicable across issue areas; (3) unclear purpose and objectives for the application of risk in homeland security; and (4) a lack of political will. We will analyze these four factors in order to briefly outline the tenets of a more effective homeland security risk assessment process.

Factor 1 – Federalism, and the Limitations of the Use of Risk at the Department of Homeland Security

A paradox of American federalism creates the first hurdle for the application of risk in homeland security. The United States constitution is rooted in federalism. A central, federal authority is established to address issues of a truly national nature, such as national defense, while States retain all rights and powers not explicitly provided to the Federal government, including the power to make laws to protect the public health, safety, and welfare of State citizens. While interpretations of constitutional law have shifted since 1787, State governments possess a relatively high degree of autonomy under the U.S. constitutional order making American
democracy very much a dynamic, adaptive system. That system often creates an unfortunate paradox – the Federal government is the single largest and most powerful governing authority in the nation while State and local governments have considerable autonomy but are limited in resources, creating a situation in which all State and local authorities want guidance and resources from the Federal government, but want to be left to their own discretion when applying such guidance and resources. It is this paradox that lays the basis for the first hurdle to the application of risk in homeland security policy.

**Factor 2 – No Standard Risk Methodology**

No single method of assessing the risk of natural and manmade hazards can be appropriately and uniformly applied across, or even within all issue areas and across all levels of government in the United States. Across DHS, the common reference for risk assessment methodology has for many years been: Risk = A Function of Threat, Vulnerability, and Consequences (Risk = f(T,V,C)). This method is suitable for natural hazards, rooted in probability derived from historical experience and has been in use for many years. However, it has been shown to be unsuitable for man-made disasters, like terrorism, where probability and consequence are far more complex and not so easily distilled to the “TVC model.” Indeed, for the past decade there has been growing recognition that, as Ezell et al. point out,

\[\text{[m]ultiple approaches, perhaps in combination are needed to address the complex issue of terrorism, including event trees, decision trees, fault trees, Bayesian belief networks, game theory, and agent-based models, among others, [and that such diversified methods] have been shown to be useful approaches for assessing terrorism risks, especially for creating a baseline comparison of these risks. But decision trees, like PRA and all approaches, have limitations and are not on their own a complete solution.}\]

Further complicating risk assessment at DHS is the fact that in practice, DHS Policy, the Coast Guard, CBP, CISA, FEMA and other elements of the Department use varying methods to gauge risk, based on their particular mandates and mission needs. At the State level, all-hazards risk assessment predominates given the variety of threats at this level of government as well as limited resources which must be made to account for a variety of risks. The Threat and Hazard Identification and Risk Assessment (THIRA) is typically used to build a State’s hazard or risk profile. Major urban areas themselves use a variety of methods to gauge their own risks, including scenario modeling to better account for terrorism risk, or the risks posed by industrial disasters, excessive heat, or urbanization itself. Private industry utilizes an array of advanced historical, statistical modeling techniques to account for issues such as logistics, supply, and inventory requirements. The reality is that each of these entities has developed a risk-assessment methodology appropriate to their own needs and understanding of the threats and vulnerabilities they face.

Despite this multifaceted reality, there are many who still proceed on the assumption that all levels of government should apply a common risk methodology when making homeland security policy decisions despite the reality of differing issues, missions, and hazards facing different types of jurisdictions and economic sectors. This often creates contradictory situations.
in which the risk and threats that, for example, a State identifies as most relevant for its preparedness are different from those which the Federal government uses to prescribe policy or resource allocations. If the nation is to effectively utilize risk assessment to ensure homeland security, it must identify and support those risk assessment methods that are most appropriate and valuable for particular jurisdictions and define how they can work in harmony.

Factor 3 - Competing Purposes and Lack of Objectives for the Application of Risk Assessment

Bureaucratic competition, rooted in different legal authorities and the persistent scramble to justify funding, both federally and nationwide, persists with respect to who is responsible for conducting and reporting on risk assessments, and to what end. Indeed, at DHS, Congress has yet to unify, or consolidate the myriad statutes which collectively enable the Department, nor has it narrowed Congressional oversight to one or a few committees. These inadequacies continue despite the fact that two 9/11 Commission Report recommendations explicitly call for the comprehensive and effective use of risk assessment in homeland security decision making. Indeed, the report called for the setting of risk-based priorities for the protection of critical infrastructure, the assignment of roles and missions, the measurement of the effectiveness of preparedness efforts, and ultimately, the allocation of limited resources and homeland security assistance.

Indeed, as early as 2010, a National Academies Review of the Department of Homeland Security’s Approach to Risk Analysis determined that the Department’s ability to operationalize and integrate risk-based decision making into actual Department policy development, and adequately evaluate and communicate its underlying assumptions and analytical uncertainties, were deficient. Further defining the problem, former U.S. Department of Homeland Security Secretary Chertoff in his book, Assessing the First Five Years, concluded that U.S. all-hazards risk assessment methodology does not adequately account for medium and long-term planning, suffers from the negative side effects of actions taken for short-term gain, and lacks overall transparency.

For an even more contemporary examination of such issues, a 2018 RAND study established that DHS required: (1) a transparent and repeatable process for assessing and comparing strategically-significant threats and hazards from which DHS is responsible for protecting the nation; (2) risk assessments which can serve as a common reference point for discussions about how threats and hazards affect the nation; and (3) a common understanding of the impacts of threats and hazards on the nation. RAND argued that achieving such requirements would allow DHS leadership to develop and implement strategic plans that direct the department’s resources to protect the nation from threats, respond effectively to disasters, and promote economic resilience. In concluding its study, RAND found that its recommendations on improving the methodologies used to characterize national risk would still not provide all information required to complete a DHS strategic planning process. RAND found that additional perspectives would be required to allow DHS to evolve from risk assessment to risk...
management, including: 1) understanding which threats and hazards pose the greatest risk to the nation; 2) identifying threats and hazards for which current efforts are disproportionate to risk; 3) providing additional recommendations on how to further reduce risk; and 4) determining how to place DHS’ role and responsibilities within the larger context of whole-of-government responsibilities for managing the risks from the identified threats and hazards.\(^{16}\)

As a result, we can discern that much work remains in terms of both methodology and organization for DHS to achieve an effective and impactful characterization of national risk. In homeland security, there are only nebulous references to “risk-based” methodologies such as allocating grants on a risk-based basis.\(^{17}\) No clear statement exists for the nation on how and why we should use risk-based priorities and planning in homeland security.\(^{18}\) Should risk be used to determine how the Federal government prioritizes its preparedness for certain types of incidents? Should risk be used to prioritize the pre-distribution of essential commodities and response assets before hurricane season? If so, how, by whom, through what process, at what level of security classification? In short, while much language has been committed to the use of risk in homeland security, no clear strategy statement for its application in the complex system which is American government has yet to be developed.

**Factor 4 – The Absence of Political Will**

The fourth impediment to the use of risk in homeland security is the absence of political will to enforce the use of risk assessment for all-hazards preparedness. Congress and past administrations have offered much language on the need for risk-based policy in homeland security\(^{19}\) and major sources of homeland security policy and doctrine such as the Quadrennial Homeland Security Review\(^{20}\) have offered much language on the need for risk-based policy in homeland security, but in reality, few political representatives are willing to return home to declare that they supported reducing homeland security resources for their constituency so that another one, facing greater risks, could be better prepared. Nor has any leader been willing to declare and commit to what their jurisdiction must be prepared for and to what degree, based on risk assessment. The reasons why, including severe political liability if a risk assessment is ultimately perceived as wrong, are understandable. For example, a 2008 GAO report found that political factors pose challenges to allocating homeland security resources based on risk\(^{21}\), because of a reluctance by politicians and others to make risk-based funding decisions.\(^{22}\) In short, all appearances seem to confirm a lack of political will within the Federal government to effectively articulate to itself or the public what its risk assessment methodology is and which threats and hazards are most pressing and deserving of attention. Elected officials and political appointees instead make investment decisions based on the public’s beliefs about which risks should be given the highest priority, beliefs that are often based on incomplete information. Consequently, there is less incentive for officials to invest in long-term opportunities to reduce risk.\(^{23}\) Yet, the consequences of proceeding as the nation has, are equally severe – the inefficient use of limited resources and the injection of purely political considerations where lives are at stake.
Trends

In addition to the factors outlined above, a set of increasingly pressing trends further establish why it is both logical and urgent for DHS to enhance its organization to coordinate and establish risk-based priorities across the Department, while more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions.

Trend - Natural Disasters Are Getting Worse and Occurring More Frequently

First, the U.S. faces considerable diversity and increasing severity of threats and risks. Since 2006, China, the United States, India, Indonesia and the Philippines are the top five nations for occurrence of natural disasters. Globally, the total number of natural disasters reported each year has been steadily increasing from 78 in 1970 to 348 in 2004. In the United States, the rate of disasters reported has gone from approximately 50 in 1960, to over 400 by the mid-1990s. No doubt, up to 1/3 of these increases have resulted from better reporting and statistics collection, but 2/3 of these increases have been due to a rise in hydro-meteorological disasters, including droughts, tsunamis, hurricanes, typhoons and floods. Natural geologic disasters, such as volcanic eruptions, earthquakes, landslides and avalanches have remained steady to date.

Two trends contribute to this high rate for the United States. First, shifts in climate are impacting the severity of weather. Heavy rainfall is increasing in intensity and frequency across the United States particularly in the U.S. Northeast. Heatwaves are now more frequent since the 1960s, while at the same time, extreme cold temperatures are less frequent. Recent record-setting hot years are projected to become common in the near future for the United States. Concurrently, the incidence of large forest fires in the western United States and Alaska is also up since the early 1980s. Annual U.S. trends toward earlier spring melt and reduced snowpack are already affecting water resources in the western United States, and these trends are expected to continue.

The second contributing factor to the increasing rate of natural disasters in the U.S. derives from trends in urban development. Rapid and unplanned urbanization into flood-prone regions increases the likelihood of flash and coastal flood damage. Large areas covered with cement mean the flow of water becomes very strong with runoff not being absorbed naturally by soil, causing collection and then rushing downstream to become heavier and faster floods. As more and more people are effectively placed in the way of harm, the damaging impact of natural events is amplified. Thus, the World Bank has determined that the United States is at relatively high economic risk from multiple hazards, with 9.3% of its population, 67.5% of its total area, and 68.7% of its GDP in areas at such risk from multiple hazards.

A striking example of the impact of such development occurred in 2017 when the dollar value of natural and man-made disasters rose to $306 billion worldwide, in large part due to damage caused by Hurricanes Harvey, Irma, and Maria, as well as a series of earthquakes and...
major forest fires around the world. The U.S. was the hardest hit region in 2017, with three hurricanes causing $93 billion in insured losses – but the most important source of these losses was a surge of residents and new homes in coastal communities in the U.S. Southeast since earlier destruction caused by Hurricanes Katrina, Rita and Wilma caused devastation in 2005 creating much greater loss potential than ten years ago. Indeed, FEMA estimates that approximately 13 million Americans are now exposed to threat of a “100-year-flood,” or an extreme flood with a 1 percent annual chance of occurring per year. However, researchers from the University of Bristol and The Nature Conservancy argue that 41 million Americans are at risk of 100-year floods — suggesting a major underestimation of risk by government. The EPA has also acknowledged that flooding is now much more frequent on the United States coastline – as much as 10 times more likely since the 1950s in Mid-Atlantic States due to subsiding land and increases in relative sea level. Hurricane Harvey’s impact was made more severe by human-induced climate change, and is indicative of a tripling of the chances of further extreme rainfall along the Gulf Coast, according to American Geophysical Union.

Trend – Man-Made Disasters – Less Probable, Perhaps More Consequential

Terrorism and other human-made disasters pose a unique challenge to the coordination of national risk assessment and management. They are less probable, but carry significant social and political consequences such as fear and the potentially disproportionate, if not irrational allocation of limited resources against threats which simply do not carry as great a risk. For example, according to a September 2016 study by the Cato Institute, some 3,024 Americans died from 1975 through 2015 due to foreign-born terrorism. That number includes the 9/11 terrorist attacks (2,983 people) and averages nearly 74 Americans per year. Since 9/11, however, foreign-born terrorists have killed roughly one American per year. Six Americans have died per year at the hands, guns, and bombs of Islamic terrorists (foreign and domestic). Globally, the number of terrorism-related incidents has gone from 651 in 1970, to a peak of 16,860 in 2014, with significantly varying rates of incidents per year, and even more significantly varying rates of incidents and concentrations of deaths by region and country. The social, political and economic consequences of terrorism in the United States are great, but the rate of terror incidents in the U.S. is low compared to the rest of the world, and overall, when compared to other forms of crime in the U.S. Yet, the Federal government still spends many billions of dollars each year in an effort to defeat terrorist organizations and to protect from, and be prepared to respond to terrorist attacks. As this examination will discuss below, addressing the problems of coordinating and establishing risk-based priorities across the Department, while more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions, might allow for greater transparency, clearer communication, and ultimately more balanced and reasonable allocation of resources in the face of threats like terrorism.
Trend – We Are More Interconnected and Interdependent Than Ever Before

Our economy and society have become exceptionally interconnected and networked. Global commerce and communications have driven our economy and way of life to become on-demand and interdependent. The systems which allow this way of life to operate are designed for maximum efficiency and operate nation-wide, if not globally. This means that the consequences of risks in one jurisdiction, or region, can have a major, if not cascading effect across many others and that the impact of an incident can be significantly magnified. Thus, in such a networked and interdependent economy, risk cannot be effectively managed, or responded to, by any one jurisdiction, company, or partner.

In a recent study, researchers measuring the economic interdependence of 364 U.S. metropolitan areas examined how those cities fared during the 2008 financial crisis – they found that the most interdependent and integrated urban areas (often the largest cities) suffered greater relative losses in economic performance and took longer to recover than their less-integrated and smaller urban areas. The implications of these findings are that integration and interdependence, while creating greater efficiencies and margins of performance and profit, also decrease the number of points of failure in a system, and increase the likelihood that as one member of a complex system fails, others fail as well. In practical terms, if one major bank in an urban area loses its cash reserves, so will others in the same area; if one construction business loses its development business in a big city, others are likely to see a loss of business as well.

Modern disasters have a significant capacity to result in unanticipated and cascading impacts. Indeed, system-wide failures result from chain reactions across different systems and are triggered by high rates of interconnectivity. As a result, risk spreads across communities, regions, industries and traditional lines of political authority. Whole groups of people share the same risks, often without knowing it, and certainly not being prepared to address them. For those responsible for managing risk, like government and industry leaders, risk assessments are sometimes not seen in their common, overlapping contexts, which can lead to conflicts over resources, liability, and/or responsibility. For instance, corruption, or simply self-interest, can reduce the impact of risk assessments when a local government self-interestedly allows construction of new building in flood prone areas against recommendations emerging from risk assessments. In relation, a local government, when balancing risks with development goals, may consciously prioritize privately funded property investments with no bad intentions whatsoever, so as to increase a tax-base and local population.

In our networked world with interdependent economies, infrastructures, and people, the risks faced by any one agent depend on the choices of all others. Thus, whether an individual chooses to invest in risk mitigation depends in large part on how she expects others to deal with risk. If a property or business owner thinks that others will not invest in risk management, then this reduces the incentive for her to do so. On the other hand, should she believe that others
will invest in risk reduction, it may be best for her to do so also for a variety of reasons, including profitability, legal-liability protection, and good corporate citizenship. As we will argue below, government, particularly the Federal government, can do much to influence, regulate, and incentivize such risk management behavior in the increasingly complex and interdependent systems which make up our economy and democracy.

Trend – The Advent of Resilience

As our economy and society have become more interdependent and reliant on networks of trade, finance, logistics, supplies, and energy there is a growing recognition of and investment in resilience. More than one-third of the U.S. population lives in hazard-prone areas. The National Oceanic and Atmospheric Administration (NOAA) reported in 2017 that the number of $1 billion dollar damage incidents is increasing per year, since 1980, with 16 in 2011, 15 in 2015, and 16 in 2017 alone. Indeed, 2017 was the costliest year on record for natural disasters in the United States, with a price tag of at least $306 billion. The list of such incidents, in 2017 alone, is remarkable: California had its wettest winter on record, ending years of drought; California faced its most destructive and largest wildfire season ever, killing 22 people and damaging 5,600 structures; Hurricane Harvey set a rainfall record for a tropical storm with over 4 feet; Puerto Rico faced what was the longest blackout in U.S. history after Hurricane Maria, with over 1,000 estimated to have died; San Francisco reported its highest temperature ever, while other parts of the country set records for high-temperature streaks; 14 locations in Oklahoma, Missouri, and Arkansas reported record-high water during floods in April and May; and requests for federal disaster aid jumped tenfold compared to 2016, with 4.7 million people registering with the Federal Emergency Management Agency.

The U.S. has built a highly efficient society rooted in cheap and quick replacement of losses. Such a model is expensive and inefficient in the face of more intense weather, the cascading effects of an interdependent society and economy, and a public sector with ever increasing demands and fewer available resources. Resources for critical infrastructure investments are more limited and stretched further than ever before, and the importance of data and transport networks is greater to the operation and survival of our society than ever before. In a recent example, since Hurricane Harvey, an entire real estate industry has developed in Houston, Texas, focused on the buying and selling of flooded homes for redevelopment, in zones which will almost certainly flood once again. Rooted in relatively cheap development prices, welcoming, scenic communities, and relatively high profit margins, this market in Houston has essentially created the basis for recurring disasters as developers only provide as much information as required to consumers, and develop just outside of formally designated FEMA floodplains. Building resilient infrastructure thus requires strong political leadership and even stronger market and regulatory incentives to be achieved.

There is growing recognition of the need for more and higher-quality data and information on threats and disasters at both national and international levels. Within the United States, several Federal reports have highlighted the importance of both historical and current data on hazard events and their associated impacts. Yet, increased knowledge does not, in and of itself, necessarily result in improved disaster risk management. Resilience requires the transparent,
Enhancing the Organization of the United States Department of Homeland Security to Account for National Risk

By Michael H. Brody

public dissemination of risk-related information, for such information sharing to be networked and viral rather than being delivered through top-down processes, and for government to partner with all necessary stakeholders to ensure that comprehensive risk assessments capture the full risk context of a community and region. Further, both government and industry have increasingly recognized resilience as a means by which to achieve both risk management and profitability, and that resilience, must in turn, become more standardized and incentivized across industrial sectors as well as public jurisdictions rooted in a common understanding of risk and an agenda for risk mitigation.

Trend – Government Is Losing Credibility, While Being Asked to Deliver More Than Ever Before

Governing in general, is getting harder. Voters increasingly demand that government deliver security and prosperity, and particularly in the face of risks, ensure that vital services and “normal” operations of roads, energy, and general commerce are restored quickly and with minimal disruption. Yet, flat public revenues, distrust, and polarization, hamper government performance. According to a Gallup Poll survey released in September 2016, only 42 percent of Americans have a “great deal” or “fair amount” of trust in the country’s political leaders—a drop of about 20 points since 2004 and a new low for Gallup trends. In addition, technology has expanded the range of players who can block or circumvent political action and have increasingly helped to make NGOs, corporations, and empowered individuals “public actors.” The diffusion of power through technological, economic, and social change also is making it more difficult for governments to implement effective policies by creating more potential veto players on issues, reinforcing a gap in expectations. Governments must now actively deal and coordinate with an increasing number of actors—NGOs, corporations, social-media driven groups, and other entities, as they attempt to fulfill their legal and electoral mandates. Ironically, for homeland security disciplines like emergency management, this represents a sort of return to, or evolution of, what has been a reality for local emergency managers for many years, namely, the need to incorporate effectively all elements of a local community into disaster-preparedness planning. The difference today, as we have seen in this examination, is the increased interplay, connectivity, and interdependence of “local” with regional, national and at times, global threats and stakeholders. The Sendai Framework highlights the importance of improved governmental coordination, which could help improve government credibility.

Rationale for Enhancing the Organization of DHS to Better Account For, Prioritize, and Act on National Risks

Taken together, the factors, trends and comparison above can be used to imply a four part rationale for enhancing the organization of DHS to address the problems of coordinating and
establishing risk-based priorities across the Department, while more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions. It is essential to emphasize that the following points are an interpretation and analysis of the trends and factors outlined above. There is room for debate on each of the following assertions, and depending on one’s context in the homeland-security enterprise, some of the following points may seem more or less relevant or accurate. Given these caveats, it is also important to attempt to understand the sources of current limitations when establishing risk-based priorities and strategy for the homeland-security enterprise. First, today, no single jurisdiction or sector of the economy can effectively mitigate risk without the long-term cooperation of diverse partners. Second, our economy and way of life is highly networked. Third, Federal homeland security strategy does not effectively define and prioritize national risks, nor does it meaningfully account for state, local, and private sector risks. Fourth, the legitimacy and effectiveness of government efforts, at all levels, to deliver homeland security suffers in the absence of accountability to prioritized risks and inefficient alignment of resources.

Case Study – Brief Comparison and Lessons from the U.K. Experience with National Risk Assessment

The following analysis identifies policies and practices from the U.K. experience with national risk assessment, providing critical insights and guidance for this article’s analysis.

The United Kingdom is presented with a clear, annual statement of the nation’s priority threats and hazards, and the methods used to arrive at such conclusions. It has also organized itself to coordinate effectively its various local and central governing authorities when applying this common methodology and delivering its ultimate product.

U.K. and U.S. Principles

U.K. resilience strategy operates under four broad principles. First, contemporary risks are complex involving multiple hazards and threats; second, local response is the building block of all resilience efforts; third, multi-agency and jurisdictional inclusiveness is essential to achieving resilience; and fourth, resilience can only be achieved with transparency and openness. These principles establish the notion that U.K. resilience strategy must be focused on the most challenging risks and that determinations of such should be made inclusively and collaboratively.

Like the opposite side of the same coin, the U.S. Department of Homeland Security’s Office of Risk Management and Analysis and its successors focus on establishing a common taxonomy of key terms, while providing specific risk analyses to DHS leadership, and in general, attempting to ensure coordination amongst the different elements of DHS conducting risk assessments through the Integrated Risk Management Framework and its Integrated Risk Management Policy and Directive. However, these policies focus more exclusively on the literal coordination and connection of ongoing, existing risk analyses within the Department and do not establish an
unambiguous, national policy defining how risk must be used to drive U.S. homeland security
decision making and by which parties. In short, unlike the British experience, where risk is an
imbedded principle of resilience, the American experience is still identifying all the different places
where risk analysis may have application in homeland security and is still grappling with how
risk assessment can be more commonly applied in homeland security decision making. It is an
underlying aspiration instead of an underlying principle.

U.K. and U.S. Jurisdictions

Following the principles identified above, under the British Civil Contingencies Act of 2004 (CCA)
and the U.K. National Security Strategy (NSS), British emergency planning and risk assessment
is inherently inclusive and oriented “bottom up.” As the National Risk Register (NRR) describes,
the National Risk Assessment identifies the threats and hazards most pressing to all of Britain, but
accounts for the fact that not all regions of the nation face the same absolute levels of risk and
have in fact their own risk profiles. As a result, local resilience forums also conduct their own risk
assessments which result in a parallel series of Community Risk Registers. In this way, localities
are able to place their risk profiles in context with that of the nation, while still utilizing the same,
basic risk assessment process. This standardization of the broad, generic elements of all-hazards
risk assessment enables the U.K. to be flexible and adaptable to meet the largest range of likely
emergencies, with supplementary national or regional capability for less likely events.

Conversely, there simply is no parallel process in the United States. There is no clearly-defined
process for conducting risk assessment that links State and major urban area risk assessments
to national, or federal, risk assessments. States often rely on their natural-hazard focused
Threat and Hazard Impact and Risk Assessment, while major urban areas facing terror threats
may utilize any number of different sources of intelligence and modeling to define their
threat profile. While instructive as an example, the U.K. does possess different constitutional
traditions, affording the government of the U.K. a different set of customs, norms and
authorities which allow for its National Risk Assessment.

U.K. and U.S. Methods and Process

Under the U.K. NSS, as directed by the CCA, the U.K. Government has a national risk
assessment capability that identifies, assesses, and determines the impact of risks to the
U.K. over a five year period. The U.K. government utilizes a six-step risk identification and
assessment process, which is split into three phases. Phase One involves defining the nature
and scope of a given risk and utilizes three steps including contextualization of a given threat
or hazard, a detailed review and assessment of the dimensions of the hazard, and finally an
analysis of its potential impact. Phase Two includes Step Four and risk evaluation, in which
threats and hazards presenting significant, national risks are identified, and their likelihood and
impact are used to produce actual risk scores - clear values defining the level of risk a threat
or hazard poses, compared to others. Finally, Phase Three, risk treatment, involves Steps Five
and Six, in which decisions are made on which risks are unacceptably high, and plans and
strategies to mitigate those risks are developed, along with associated capability requirements
to meet planning factors. These steps are undertaken by informed subject-matter experts from
multiple government agencies and jurisdictional levels. Their results, while backed by historical statistics and trends, are ultimately rooted in expert, professional human judgment.

Compared to the U.S. experience, the U.K. assessment process is flexible enough to account for a variety of factors that are more difficult to quantify including measures of social disruption and psychological impact.

**U.K. Products, Communication and Transparency**

The U.K. government publishes a National Risk Register (NRR), which sets out the assessment of the likelihood and potential impact of a range of different risks that may directly affect the U.K. The NRR is designed to increase awareness of the kinds of risks faced in the U.K., and provides some detail as to what the government and emergency services are doing to prepare for emergencies. While rooted in the CCA's mandated National Risk Assessment, which is classified, the NRR is designed to facilitate public debate on security, help all elements of society plan and prepare for emergencies, and ultimately present a clear, national statement of which threats and hazards are most pressing for the U.K.

Quite simply, there is no American equivalent to the NRR. As noted above, the Department of Homeland Security is charged with advancing an “Integrated Risk Management Framework” and delivering Department decision makers with risk assessments to inform decision making. In parallel, States routinely conduct Threat and Hazard Impact and Risk Assessments (aka THIRAs) to inform their mitigation planning and resource allocation decisions, but such assessments, typically and understandably, focus on natural hazards most impacting typical mitigation strategies such as levies and retaining walls. States do not publish comprehensive, public statements of all the threats and hazards facing their jurisdiction.

To some degree, there has been recognition in the United States of this deficit. For example, Representative Henry Cuellar, when sponsoring legislation aimed at improving the measurement of federal preparedness grants to states, noted that current grant effectiveness assessment processes and allocation steps do not effectively account for risk and fail to “take the guess work out of the equation.” However, such recognition has yet to materialize into a call for a clear, transparent, national statement on all-hazards risk.

**Lessons from the U.K. Experience**

**Time Horizons**

The U.K. risk assessment process clearly defines both short-term and five-year periods of assessment when defining relative risk values for different threats and hazards. This measure alone, if standardized in U.S. risk assessment efforts, would greatly improve the nation’s capacity for considering longer term planning requirements and avoid the classic pitfalls of seeking immediate gains and benefits while ignoring long term consequences, such as
excessive development in flood prone areas or not adequately providing for the protection of major transportation hubs. In addition, the mere act of producing an annual, national, public statement of the risks facing the nation, would also increase the U.S. ability to reconsider routinely their risk profile and better consider historical-trends analysis to determine future requirements. There is, it is important to note, a basis for such reporting by the Federal government in the National Intelligence Estimates (NIE). NIEs are developed by the U.S. intelligence community on a consensus basis and typically focus on national security issues such as state competitors, terrorist organizations, or international issues. The NIE could serve as a valuable reference for how DHS could develop a similar statement of all-hazards risk(s), reflecting not only DHS or Federal interests, but also those of state, local, and private stakeholders.

Negative Externalities

The U.S., and particularly DHS, could likely benefit from the adoption of many of the U.K.’s methods of assessing risk. In particular, use of a more inclusive, comprehensive risk assessment process would more than likely allow DHS to better account for the long-term impacts of economic-development decisions on overall national preparedness.

Transparency and Resulting Transaction Costs

Finally, by having a clearly defined, regularly delivered statement of the top hazards facing the nation, American emergency planners and policy makers would be able to better coordinate, justify, and target their preparedness efforts, instead of relying on the often confused and conflicting picture of risk that exists today. The effectiveness and efficiency of federal preparedness grant investments would almost certainly improve if based on a nationally recognized, consensus-based profile of national threats and hazards by helping to remove politics, at least in part, from such funding decisions.

Summation of Comparison with U.K. National Risk Assessment

The CCA demonstrates that publication of an annual, public statement of national risk requires a clear legal mandate. As discussed above, at this time in the United States, homeland security authorities have no legal mandate to deliver an “NRR type” annual report to the public. Second, assuming such a clear legal mandate for a “U.S. NRR,” the American homeland security bureaucracy would have to designate one agency or a network of agencies with clear responsibility and resources for delivering such a product. As illustrated earlier, the U.S. Department of Homeland Security is currently organized such that a variety of agencies and offices deliver risk-analysis products, with no clear, central authority on risk assessment. Third, and perhaps ultimately most important, the American homeland security enterprise would have to find the political will to not only reference risk in its decision making, but stand by the results of risk assessments when deciding how to distribute limited resources and prioritize preparedness efforts. To date, such political will has not been demonstrated by U.S. homeland security decision makers or the public.
The Characteristics of the Enhanced Organization of DHS to Better Account For, Prioritize, and Act on National Risks

Having evaluated the factors, trends, comparison and rationale outlined above, we can next identify necessary characteristics of an enhanced organization of the Department which would allow it to address the problems of coordinating and establishing risk-based priorities across the Department, while more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions. First, DHS must establish prioritized risks for incidents facing the nation, at both the national and regional levels. Second, when establishing priority national and regional risks, prioritization must fully account for the diverse interests and risks facing state, local, and territorial jurisdictions and the private sector. Third, the Department of Homeland Security must play a central role to balance Federal priorities and authorities with those of state, local, and private-sector interests. Fourth, DHS must play a central role when aligning resources, regulations, incentives, and standards against priority risks at the national and regional levels. Fifth, DHS must use joint authorities, planning and operations when playing this role, to leverage fully the whole homeland security enterprise.

It is important to note that there is already some organizational basis for achieving these five ends, outlined above, within DHS. As we have seen, recent DHS Secretaries have established new organizational elements such as the Senior Leaders Council (SLC), Deputy’s Management Action Group (DMAG), and Joint Task Forces (JTFs). These entities have increased strategic and operational coordination between and amongst DHS HQ and components. Further, current resource planning and program-planning guidance are now delivered by the Secretary to components, through such groups. However, as noted above, such elements remain largely functions of DHS HQ and do not always reflect the interests and priorities of all homeland security enterprise stakeholders. Further, the priorities established by such organizational elements are often focused on near and mid-term issues and priorities, without clear explanation or rationalization in terms of risk. As noted above, recent GAO examinations have substantiated such limitations.

Iterative Progress to Date and Counterpoints

It is important to emphasize that the factors and issues outlined above have not gone unnoticed or without action at DHS HQ and components. Indeed, the 2010 DHS Bottom Up Review established:

- increasing Accountability as a top priority for future DHS management and operations, so as to, maximize the performance and resource data [DHS] collect[s] to support strategic and risk-informed decision-making... improve the effectiveness of the Department in turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan, [and] Increase [DHS] analytic capability and capacity by enhancing
strategic planning, resource allocation, risk analysis, net assessment, modeling capabilities, statistical analysis, and data collection.88

DHS HQ has established a standardized “Risk Management Plan” for major, new acquisitions to ensure that all major acquisitions at DHS implement a risk management plan identifying, managing and mitigating the risks facing major procurement by the Department.89

In another example of iterative progress made on the factors outlined above, the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) has, since at least 2012, pursued a five (5) year Analytic Agenda employing a comprehensive strategy for identifying, prioritizing, and addressing HITRAC analytic requirements based on rigorous, dynamic analysis of risk-related body of knowledge. That Agenda is turned into an annualized plan that aligns HITRAC resources to immediate analytic requirements. Finally, an Annual Production Schedule is developed to meet partner and stakeholder decision-making needs both for content and for timeliness. HITRAC leads top-down analysis by assessing legislation, Presidential and DHS directives, and plans and guidance, while driving product development based on State, local, tribal, territorial, and private sector bottom-up analytic needs for providing information on the tradeoffs of current and future risk-management decisions.90

A final example of iterative progress by the Department on risk-based management is its Integrated Strategy for High-Risk Management. The Integrated Strategy, and its associated updates have, since 2011:

- outlined the Department’s actions to strengthen management functions while addressing a related High-Risk List designation by the Government Accountability Office (GAO). First issued in 2011, the biannual Integrated Strategy has been commended by GAO as a best practice and is now required by statute.91

The Integrated Strategy focuses on a series of “Integrated Priorities,” the first of which is called “Strengthen Resource Allocation and Reporting Reliability,” which in turn focuses on key objectives including achieving resource allocation by mission areas, common appropriations structures for the whole DHS enterprise, and the modernization of DHS financial systems. There is little doubt that DHS’ demonstrated ability to act on and close out such areas of GAO concern shows significantly improved management of DHS business functions, based on enterprise risk.

Finally, we must recognize that DHS has indeed established a series of Joint Task Forces which remain in operation and do incorporate joint operations between and amongst DHS components and Headquarters. However, they continue to be driven and authorized by existing, component-based authorities, without more permanent and enduring DHS joint authorities defined by statute. Were risk-managed networks supported by clear, strong, joint authorities, they and all their diverse stakeholders would possess a more reliable stream of federal resources and operational justification.

All of the points and examples above represent progress by the Department towards risk-based management and strategic planning. Such progress has been largely focused on DHS
Headquarters-based management functions, comes in response to external audits or compliance functions, and may have been hampered by ongoing reorganization of the Department itself. The issues which the GAO and stakeholders of all kinds have identified remain with respect to the Department’s inability to address the problems of coordinating and establishing risk-based priorities across the Department, while more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions. Therefore, we continue our examination below, assessing a series of concepts for the enhancement of the Department’s organization to account for national risk, including new authorities and organizational models.

Enhancing the Organization of DHS to Account for National Risk

Network-based Governance and Regionalization

As demonstrated above, the ability of DHS to account for national risk, in partnership with the rest of the homeland security enterprise is a complex challenge. It requires: (1) the extensive use of diverse, inclusive, expert analysis; (2) the recognition and potential regulation of interrelationships and dependencies of risks between and amongst various stakeholders, jurisdictions, and industry sectors; and (3) clear, transparent communication of risk and competing priorities, in order to arrive at the effective allocation of limited resources. National risk is diverse, continuously changing, shaped by social and political factors as well as data, and ultimately driven by the need to deliver public value in the form of reduced risk from major incidents. In this dynamic, network-based governance organized around homeland security regions could be a very powerful tool.

In the context described in this article, network-based governance can be defined as: (1) coordinated, interconnected authorities and resources across multiple jurisdictions and economic sectors to address common risks; (2) accomplished through decentralized networks of public and private actors at the regional level; and (3) emphasizing the use of information sharing, consensus-based decision making and prioritization, incentives, and enforcement. The graphic below illustrates the relationship between increasing demands for public-private collaboration, and the need for increased management of networks of stakeholders. When the need for collaboration and networks of stakeholders is low, a classic, vertically integrated government organizational model can be effective. When the demands for collaboration and networks of stakeholders are high, networked governance becomes critical, as the means to ensure cooperation, collaboration and responsiveness to pressing issues or, in this case, risks.
Figure 1 Illustration of the relationship between increasing demands for public-private collaboration, and the need for increased management of networks of stakeholders

A one-size-fits-all, top-down national-risk management organization will not work in the U.S., nor will a completely Federally-driven approach. Instead, DHS could best address national risk through the establishment of regional networks of stakeholders around the management of priority risks within a given region, between regions, and finally, nationally. Stated differently, DHS HQ in partnership with DHS components could take far greater advantage of DHS components’ existing regional constructs, to coordinate and maximize the impact of DHS assets with state, local and private sector partners. This could be done in a way that avoids creating new layers of bureaucracy, but still increases coordination and cooperation between existing regional elements, based on prioritized risks at the regional and local levels. Such regionalization would be vital for DHS to account for the complexity of national risk, and ensure responsiveness and accountability to state, local, private, and non-profit stakeholders, while maintaining cohesive overall national management of such risk. As noted earlier, some elements of DHS are already moving in such a direction. The National Risk Management Center (NRMC), for example, is the

Cybersecurity and Infrastructure Security Agency’s (CISA) planning, analysis, and collaboration center, working to identify and address the most significant risks to the Nation’s critical infrastructure. Through the NRMC’s collaborative efforts with the private sector, government agencies, and other key stakeholders, the CISA works to identify, analyze, prioritize, and manage high-consequence threats to critical infrastructure through a crosscutting risk management paradigm.97

CISA has also recently reorganized itself to place far greater emphasis on its operational regions.98
Such a dichotomy is well illustrated in Stanley McChrystal’s Team of Teams. One could think of our current, vertically-oriented way of governing risks as the “Command and Hierarchy” line in the graphic below, in which each level has its own priority risk(s), stakeholders are neatly broken out by lines of authority and type, and each is solely responsible for their own risks, but has no reason nor incentive to collaborate with any other level of governance. In such a model, authority and “turf” are clear, but collaboration is low and the ability to address risks which cut across levels of authority is equally low. One could next think of the “Command of Teams” line as DHS’ nascent efforts at joint task forces or interagency task forces, intended to bring together interdisciplinary teams which each focus on a particular risk, for example border security, under the command (or joint command) of a Federal agency. In this case, collaboration has increased, as has multi-jurisdictional collaboration on a common risk, but the unit can only focus on its particular priority risk, and can only do so under the hierarchical authority of a “lead agency.” Finally, in the “Team of Teams” line, we can see a notional depiction of network-based governance at the regional level for priority risks, in which multi-stakeholder networks collaborate to address the priority risks in their own region, and, through the coordination of DHS, the nation, from one set of regional networks, to the others. In this way, the strengths and interests of all stakeholders are put to the greatest use against common priority risks, while overall national risk is managed between and amongst regional networks.

Figure 2 Illustration of Potential Evolution of DHS National Risk Management from a Command and Hierarchy Model to a Regionally-Focused Network-based Model of Prioritized Risk Management

To achieve such network-based governance over regional risks, the Department should place greater emphasis on regionalization to address the problems of coordinating and establishing risk-based priorities across the Department, while more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions. The full, functional integration of all DHS component regional offices is not realistic in the short and medium terms, for political and logistical reasons discussed above, most poignantly including competing jurisdictional authorities between and amongst DHS components and Congressional committees and leaders, as well as the often divergent operational cultures and histories of different agencies. Instead, the key to enhanced regionalization is the use of networked relationships and decision making. For DHS to serve as the lead “node” in a series
of networks focused on mitigating priority risks within and between regions, its operational components would have to significantly increase the coordination of their regional operations. Such coordination would be essential when leading networks of state, local, territorial, private and non-private stakeholders, all of whom would consider any element of DHS to be “DHS” and have little patience for parochial, component-based divisions or rivalries. Further, only through such heightened coordination in the regions could DHS effectively marshal the full weight of its existing authorities and resources to have the greatest impact within a network to mitigate risks and enforce priorities with so many diverse partners. There is no doubt that DHS component regional offices are a step towards such enhanced coordination. FEMA Regional offices are often very much at the heart of major incident responses. The newly created DHS Cybersecurity and Infrastructure Security Agency has a plan for “enhanced regionalization.”\textsuperscript{101} However, such offices have varying degrees of coordination between and amongst each other (e.g. different DHS components), and with their DC-based headquarters offices.\textsuperscript{102} Thus, increased regionalization would take the form of heightened coordination between and amongst DHS components within regions; greater operational emphasis on regional operations by DHS components, relative to their headquarters; and the presentation of a unified, DHS “front” when engaging with diverse stakeholders on prioritized risks.

In addition, DHS’s operational regions would engage the Federal interagency, as well as state, local, and major urban area governments, the private sector and non-profit sectors to identify and prioritize risks facing their particular region, and, through the active coordination of DHS headquarters, identify and prioritize those risks cutting across particular regions and nationwide. By combining both “top down” and “bottom up” priorities, DHS would ensure that priority risks were properly contextualized relative to each other at both the national and regional levels, and fully account for the interests and needs of not only Federal authorities, but truly national authorities.

The use of networks and regionalization would result in significant benefits. National homeland security strategy would become rooted in the priorities and partnerships developed at the national and regional levels to address such priority risks. Such networks would ensure the efficient use of limited resources through complementary mitigation efforts; the full exchange of critical data and information necessary to identify, understand and prioritize risks; the understanding of the interactions of risks between and amongst each other, and between and amongst different jurisdictions and stakeholders; the influence of worsening environmental conditions, instead of reliance on past trends; the incorporation of lessons learned from disasters including identification of outdated and ineffective methods of risk mitigation; and the laws, regulations, incentives, penalties, funding, enforcement, and leaders required to ensure the ultimate mitigation of risk. In this way, DHS would remain respectful and cognizant of the interests and authorities of all stakeholders, while ensuring that a national and regional perspective prevailed over parochialism. Each network would develop a strategy properly tailored to the realities of a particular risk and/or region. Where the leadership of a Federal agency was required, on a border security risk, for example, Federal management would be appropriate. Where the leadership of a State or major urban area would prove most effective, on a regional flood mitigation risk, for example, they would lead. Where the management and focus of the private sector proved most essential, on the resilience of the energy grid, for example, the private sector would serve as the hub of the network.
Enhancing the Organization of the United States Department of Homeland Security to Account for National Risk

By Michael H. Brody

Such a networked approach would significantly increase the strength of necessary funding and investment proposals at all levels of government and the private sector. This is so because such proposals would represent the inclusive consensus of a broad cross-section of interagency and intergovernmental stakeholders. This would make it difficult for appropriators to deny the sheer weight of opinion and purpose behind such network-based proposals.

A networked approach could also potentially offer significant political benefits. By focusing on facilitated consensus and regionally-based identification of priority risks, all parties involved, particularly those representing state and local governments, would benefit from clearer and more direct representation of the priorities of divergent jurisdictions and economic sectors. Such representation would provide a degree of “cover” for elected officials, ensuring they had a forum in which to advocate for their particular jurisdiction, constituents, or sector. Such representation would, in turn, result in greater accountability of government and industry to the general public, by more effectively communicating the prioritization of risks and the measures proposed for their mitigation. Enforcement of resulting mitigation strategies would, in theory, be stronger because of the mutually reinforcing oversight of the whole network – transparency and accountability would ensure praise, recognition and market incentives, but also condemnation and enforcement actions, as required. Stronger representation and greater accountability would, in turn, provide much stronger justification for risk mitigation funding requests, particularly at the Federal level but also at the state and major municipal levels, as appropriating legislatures would have no choice but to recognize the sheer force of public and private will embodied by the priorities and proposals of each risk network. Network funding proposals would represent the unified, consensus-based proposal of the whole network. Finally, a networked approach would help to ensure far greater cooperation and coordination on the execution of risk-mitigation activities across the diverse partners composing a regional risk-management network. Such coordination would ensure respect for particular leaders or jurisdictions which sought more direct responsibility for a particular mitigation priority, while also ensuring cooperation between and amongst partners where appropriate and preferred.

In addition to regionalization and the use of network-based governance outlined above, DHS should consider two additional types of enhanced authorities to further advance its organization and ability to account for national risk.

Trans-Regional, Multi-Functional, Priority-Risk-Based Authorities for the Secretary of DHS

Building on a greater emphasis on regionalization, the Secretary of DHS would likely require new authorities to, on a limited basis, allocate/reallocate select assets, personnel and resources, nationwide, and on a fixed-term basis, to align effectively the Department’s authorities and resources within and between operational regions to best support the risk mitigation networks established under this new form of network-federalist national security strategy. Legislation
would likely be required to empower the Secretary, and perhaps the Deputy’s Management Action Group (DMAG) with the authority to resolve differences and establish priorities for missions that cut across different DHS components, missions, and regions. This course of action would place the Secretary and, by extension the DMAG, in a more direct, joint leadership role in ongoing DHS operations. Such authority would serve to accelerate DHS decision-making and response times, precluding or truncating prolonged DHS headquarters versus components conflicts in Washington, DC, as well as fights between components’ headquarters and their own regional offices. It would allow for the clear definition and enforcement of priorities across the Department. Moreover, it would almost surely reduce the development of an “islands unto themselves” identity which lingers in some component regional operations. For the first time, the Secretary would have the kind of authority required to achieve the coordination between and amongst DHS components originally envisioned in the Homeland Security Act.

Joint Authorities

Building on the concepts outlined above, clearer Federal authorities for DHS joint operations, focused on common, national, risk-based priorities would likely be required to enable fully increased regionalization, TMP authorities, and risk management networks. While DHS operational components certainly possess the ability, will, and authority to partner with one another on, for example, the current Joint Task Forces in operation nationwide focused on border security and immigration enforcement, they lack strong, permanent authorities to fund and fully enable such joint operations. Stated differently, DHS joint operations are rooted in good will and the strength of direction from the DHS Secretary. Were risk-managed networks, as proposed in this discussion, supported by clear, strong joint authorities, they and all their diverse stakeholders would possess a more reliable stream of federal resources and operational justification. It would demonstrate a stronger, more lasting commitment to risk mitigation leadership by DHS, to state, local, private and non-profit partners, while further empowering the Secretary to ensure coordination across the Department nationally and in the regions, and with all stakeholders. By focusing on joint-ness, instead of full integration, it would preserve the integrity, identity, and authorities of DHS’ existing operational components.

CONCLUSION

A set of significant and pressing factors and trends creates a strong impetus for the enhancement of the organization of DHS to address the problems of coordinating and establishing risk-based priorities across the Department, while more fully accounting for and acting on the priority risks of all DHS stakeholders within and between DHS operational regions. Through enhanced regionalization and the creation of TMP and Joint authorities, DHS can maintain the strengths of its component-based authorities, resources, expertise and experience, while instituting organizational reforms allowing it to set clearer and stronger Departmental priorities, and more fully accounting for the vital interests of its diverse stakeholders – all rooted in risk.
About the Author

Michael Brody began his career in 2004 in the Office of the Governor of Illinois where he was responsible for developing new homeland security policy for the State. He then served as Director of the Illinois Homeland Security Market Development Bureau which advanced Illinois’ homeland security industry. In 2008, Brody joined FEMA serving as Reporting Section Chief for the National Preparedness Assessments Division, where his team produced the National Preparedness Report. From 2012 to 2014, Brody served as the Policy, Outreach and Communications Manager for the Homeland Security Information Network, where he was responsible for stakeholder management and strategic messaging. Beginning in 2014, Brody worked as the Director for Policy, Architecture and Governance in the Information Sharing Services Office of the DHS Office of the Chief Information Officer (OCIO) where he managed strategy development, program assessment and communications for a portfolio of enterprise IT services. Since May, 2019, Mr. Brody has served as DHS Chair and Visiting Professor at the College of Information and Cyberspace, National Defense University. He holds a BA from the University of Pennsylvania (2000, magna cum laude), a JD from the University Of Illinois College Of Law (2004, cum laude), an MA from the Naval Post-Graduate School’s Center for Homeland Defense and Security (2010), an MA from the National War College (Distinguished Graduate, 2018), and is a DHS Senior Fellow. He may be reached at michael.h.brody.civ@msc.ndu.edu

All the views expressed in this article are those of the author, Michael H. Brody, himself and do not represent those of the United States Department of Homeland Security nor of the National Defense University and its College of Information and Cyberspace.
APPENDIX 1 – Definitions of Key Terms

The DHS Risk Lexicon and associated risk doctrine\textsuperscript{105} have been used to define a set of terms critical to this paper’s analysis.

DHS: It is the role of United States Department of Homeland Security (DHS) and its partners from all levels and types of government, and the private and non-profit sectors, to understand and manage the myriad homeland security risks facing the United States. The U.S. homeland security environment is complex, interconnected, interdependent, and characterized by competing interests. Such interests must be balanced, through the coordination of the whole homeland security enterprise, to ensure the achievement of prioritized national objectives which maximize the value added by limited resources and achieve national risk management.\textsuperscript{106}

Incident: Occurrence, caused by either human action or natural phenomena that may cause harm and that may require action (e.g. DHS plays a role in reducing the risk of an incident in the United States.)

Mitigation: Ongoing and sustained action taken prior to, during or after an incident occurrence, to reduce the probability of, or lessen the impact of, an adverse incident.

National Risk: Derived directly from the language of Presidential Policy Directive-8 (PPD-8) and referencing the DHS Risk Lexicon’s core definition of Risk, National Risk is defined as those threats posing the greatest risk to the security of the whole of the nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters, requiring the achievement of an integrated, layered, and all-of-Nation preparedness approach that optimizes the use of available resources. Therefore, National Risk is rooted in the DHS Lexicon’s core definition of “Risk,” applying that core definition to the whole of Nation (e.g. the potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence of any kind, for the whole of nation).\textsuperscript{107}

Resilience: The ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance.

Risk: The potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence of any kind, natural or human-made (with the exception of threats borne from foreign state actors, which are handled primarily by the U.S. Department of Defense).

Threat: Natural or man-made occurrence(s), individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
Copyright

Copyright © 2020 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).
Endnotes

1. United States Constitution, Article 1, Section 8, and Amendment 10 (1787).

2. National League of Cities v. Usery, 425 U.S. 833 (1976), “The States are integral parts of the constitutional structure and are immune from direct regulation by the federal argument at least with respect to ‘integral’ government functions.”


5. GAO-08-852, “DHS Risk-Based Grant Methodology is Reasonable, But Current Version’s Measure of Vulnerability is Limited,” Figure 2: Evolution of DHS’s Risk-based formula, June, 2008, 8.


10. Ibid., 391 and 396.


15. Ibid.

16. Ibid.

17. GAO-08-852, “DHS Risk-Based Grant Methodology is Reasonable, But Current Version’s Measure of Vulnerability is Limited,” Figure 2: Evolution of DHS’s Risk-based formula, (June 2008), 8.


22. National Commission on Terrorist Attacks upon the United States, 391 and 396.


28. Ibid.


31. Ibid.

32. Ibid.

33. Ibid.


37. Ibid.


41. Ibid.

42. Ibid.

43. Ibid.


45. Ibid.

46. Ibid.

47. Ibid.


51. Shade Shutters and Laurie Mazur, “Human Society is Totally Interdependent - That’s a Huge Advantage, but Also a Huge Survival Risk,”

52. Ibid.


54. Ibid.


56. Ibid.


59. Ibid.

60. Ibid.

62. Ibid.


64. Ibid.

65. Ibid.


69. Ibid.

70. Ibid.

71. Ibid.


95. Ibid.


104. It would, for the first time, create the basis for a true, DHS “joint” operational authority, using prioritized risks and national and regional networks of stakeholders led and coordinated by DHS as the basis of operations.


