

**State/Local Issue Team Problem Analysis  
Structure Working Group  
Project on National Security Reform  
Submitted by  
John F. Morton, Team Lead  
30 OCT 2008**

*“Where the hell is the cavalry on this one?...They keep saying we’re going to get supplies. For God’s sake, where are they?” Kate Hale, Director of Emergency Management, Miami-Dade County FL, Day Three Press Conference, Hurricane Andrew Response, 1992*

*“[A]t some point we saw there was...nothing for the federal government to stick on to.” Scott Wells, FEMA Deputy Federal Coordinating Officer for Hurricane Katrina in Louisiana, quoted in Hurricane Katrina: A Nation Still Unprepared, Special Report of the Committee on Homeland Security and Governmental Affairs, U.S. Senate, May 2006*

*“The preparation and response to Hurricane Katrina show we are still an analog government in a digital age.” A Failure of Initiative, The Final Report of the Select Bipartisan Committee to Investigate the Preparations for and Response to Hurricane Katrina, U.S. House of Representatives, February 15, 2006*

## CONTENTS

PROJECT ON NATIONAL SECURITY REFORM (PNSR) STATE/LOCAL ISSUE TEAM MEMBERS	4
PROBLEM STATEMENT	5
I. INTRODUCTION	6
The Importance of the Topic	6
II. THE CURRENT SYSTEM	6
III. CURRENT HOMELAND SECURITY STRUCTURES	10
Federal Structures	10
Regional Structures	13
State/Local Structures	14
A Primer on the Incident Command System (ICS)	15
IV. UNDERLYING ASSUMPTIONS	18
V. PROBLEM ANALYSIS	19
The Root Cause of Poor Performance	19
Core Problem	19
A. Ineffective and Inefficient Alignment of the Interagency and Intergovernmental Homeland Security Structure	20
Homeland Security Council (HSC)/National Security Council (NSC) Issue Overlaps	20
Executive Office of the President (EOP)/Department of Homeland Security (DHS) Failure to Integrate Strategic-level Guidance	21
The Incomplete Authorities of the Secretary of Homeland Security	22
Vagaries in the Homeland Security Budget Process	23
Uncoordinated Intergovernmental Interfaces	24
B. Ineffective and Inefficient Alignment of Congressional Oversight with Executive Branch Homeland Security Functions	25
C. Lack of Clarity as to the Secretary of Homeland Security's Role in Domestic Incident Management and Improper Alignment of Certain Departmental Functions	27
D. Inadequate Non-Federal Stakeholder Engagement in Policy Development	28
The Intergovernmental Effect of Failed Interagency Leadership	28
The Failure to Engage Proactively Non-federal Stakeholders in Policy Development	29
Failed Private Sector/Non-governmental Organization (NGO) Engagement	29
Federal Advisory Committee Act (FACA) Constraints on Executive Privilege	31

E. Improper Structuring of Homeland Security Resourcing	32
Deficient Risk Analysis Capabilities	32
F. Stovepiped Constraints on Information Sharing	33
Security Classifications and Clearances	33
Failure to Determine Responsibilities for Collection	34
Applying the Positive Example of Joint Terrorism	
Task Forces (JTTFs)	35
Fusion Centers and All-hazards Applications	35
Effect on Unified Command	38
Critical Infrastructure Protection Information Sharing	39
VI. ASSESSMENT OF PERFORMANCE	40
A. Policy and Strategy Development	40
Interagency National Cargo Security Strategy Development	40
B. Planning	42
Uneven Institution of Integrated Planning	42
Relative Success for Prevention and Protection	42
Shortcomings for Response and Recovery	43
Failed Integration with State Planning	44
Ignoring Local Planning Efforts	45
Federal Non-participation in Exercises	45
Inadequate Planning Compromises Effective Resource	
Decision-making	46
C. Resourcing via a Fragmented Grant Structure	48
D. Operational Execution—The Structural Performance of the Katrina Response	52
Degraded Federal Emergency Management Agency (FEMA) Capacity	52
The National Response Plan (NRP)—the New Framework for	
Response	52
NRP Implementation	53
NRP Design	54
NRP Execution	56
VII. CONSEQUENCES	59
VIII. CONVENTIONAL WISDOM	59
IX. CONCLUSIONS/FINDINGS	59
FINDING 1: The NRF is still in need of Federal-level structural and process	
improvement.	59
FINDING 2: The expectation is almost a given that the Federal government will	
provide and manage primary support.	60
FINDING 3: The assumption that Hurricane Katrina was America’s worst natural	
disaster reinforces that expectation.	61
FINDING 4: Primary responsibility and authority for homeland security <i>may</i>	
have to devolve from the Federal to the state level.	61

**PNSR Structure WG State/Local Issue Team Members (by primary focus area)\***

- Team Lead—John F. Morton, DomesticPreparedness.com
- Constitutional Issues—The Hon. John O. Marsh, former Secretary of the Army and former Congressman from Virginia
- National Response Framework (NRF) and Emergency Support Functions (ESF)—George Foresman, former Under Secretary for Preparedness, DHS
- NIMS—Steve Grainer, Chief, IMS Programs, Virginia Department of Fire Programs
- NSC—Lisa Gordon-Hagerty, former Director, Combating Terrorism, NSC Staff
- DHS Secretariat—Josh Filler, former Director, State and Local Government Coordination, DHS
- HHS/ASPR/PHEMCE—Bill Helming, Vice President, Public Health and Biodefense Practice, PRTM’s Global Public Sector Group
- National Guard/Reserves—Dan McKinnon, Commissioner, Commission on the National Guard and Reserves
- DoD Interfaces—COL Bob Fitton, USA (Ret.), former Army Director of Military Support (DOMS)
- Coast Guard—VADM James Hull, USCG (Ret.), former Commander, Atlantic Area
- Communications Interoperability/Situational Awareness/Data Fusion—Tom Steele, CIO, Delaware Department of Safety and Homeland Security
- Law Enforcement (Local)—Capt. Joe Watson, Operations Chief, Culpepper County (VA) Sheriff’s Office, former Incident Commander, Moussaoui Trial NSSE
- Law Enforcement (Federal)—Joe Trindal, former Director, National Capital Region, Federal Protective Service, Immigration and Customs Enforcement (ICE)
- Medical Support—Jerry Mothershead, Physician Advisor, Medical Readiness and Response Group, Battelle Memorial Institute
- Public Health—Steve Harrison, Assistant Director, Emergency Operations, Logistics and Planning, Virginia Department of Health
- Grants, CI/KR Protection—Tim Beres, former Director, Preparedness Programs, DHS
- State Government/Transportation Security—John Contestabile, Director, Engineering and Emergency Services, Maryland Department of Transportation
- Local Government—Fire Chief Lynn Miller, Emergency Management Coordinator, Winchester (VA) Emergency Management
- Private Sector—Charlie Latham, Business Executives for National Security (BENS)
- NGOs—Joe Becker, Senior Vice President, Preparedness, American Red Cross
- Standards—Matt Deane, Director, Homeland Security Standards, American National Standards Institute
- Procurement/Contract Management/Professional Workforce Development—Greg Rothwell, former Chief of Procurement, DHS
- Contractor Community—Stan Soloway, President & CEO, Professional Services Council
- Academic Consultant—Sam Clovis, Professor, Morningside College and Fellow, Homeland Security Institute
- Advisor—COL John Brinkerhoff, USA (Ret.), Institute for Defense Analyses, former Acting Associate Director, National Preparedness, FEMA
- Intern—Creighton Vilsack, The George Washington University

\* Except where cited, the views expressed in this problem analysis are those of the team members and reflect only their expertise in their respective fields and not those of their former or current affiliations or sponsoring agencies.

## PROBLEM STATEMENT

### CORE PROBLEM

*The fragmented national security and homeland security structure—between and within all levels of government—fails to require and empower systematic collaboration, coordination and integration of strategy and policy development, resourcing and aligned operational execution in steady-state or crises.*

*Symptomatic of the core problem is the ambiguity in many national security and homeland security roles and missions within the Executive Office of the President (EOP) which creates confusion and impedes clear lines of presidentially-delegated authority to lead policy development and Federal-level operational execution.*

*Strong workforce cultures in each department, agency and intra-DHS stovepipes have prevented full institutionalization of a homeland security culture. With respect to DHS, no organizational entity above the DHS agencies—whether in the mission or back offices—effectively drives a common culture.*

*The currently inefficient budget process does not vest the Office of Management and Budget (OMB) with the appropriate authority to oversee and make recommendations on all Federal homeland security and national security budgets to identify and eliminate duplication of effort among and within departments and agencies.*

*Current legislative-branch mechanisms (structure, processes, culture, etc.) drive further fragmentation and inefficiencies in execution of executive branch national security and homeland security responsibilities.*

*Despite the language of such foundational policy documents as the National Security Act of 1947, Homeland Security Act of 2002, Intelligence Reform and Terrorism Prevention Act of 2004 and others such as National Response Framework (NRF), the National Security Council (NSC) and Homeland Security Council (HSC) have no standardized process to solicit and receive state, local, private sector and NGO input into the development of national policy.*

*DHS, the Department of Justice (DOJ), DoD, the Office of the Director of National Intelligence (ODNI), the HSC and other Federal entities with homeland security mission responsibilities—along with their state and local partners—have failed to institutionalize a comprehensive and workable information sharing structure and a responsibility to provide information sharing culture.*

*Implementation of comprehensive national security and homeland security planning at the state and local levels is uneven.*

*Homeland security grant mechanisms work against collaboration, fragment state and local planning and reinforce Federal stovepipes.*

## I. INTRODUCTION

**The Importance of the Topic:** Twenty-first century events like 9/11 and Hurricane Katrina have made us aware of how future national catastrophes could rise to the level of threatening our ability to maintain our constitutional form of government. The Constitution expresses in the Preamble the expectation that constituted government among other things will “insure domestic tranquility, provide for the common defense, promote the general welfare.”

Any structural assessment of homeland security needs first to define “the proper boundaries of ‘national security’ concerns in the 21<sup>st</sup> century global security context.”<sup>1</sup> In the two previous centuries, that expectation in the Preamble was satisfied by a national security system structured to meet threats deemed to arise from traditional state adversaries external to U.S. borders. By incorporating what is now called homeland security, national security concerns are now both external and internal to American borders, involving threats posed by states and non-state entities, e.g., terrorist networks, which may or may not be state-sponsored. While different presumed stakeholders have their own delimitations of scope for *homeland* security, current expectations necessitate including within that scope catastrophic natural, medical or technological disasters on such a scale which could jeopardize the nation’s constitutional system of government, i.e., in addition to catastrophic threats posed by an adversary.

Homeland security is thus at least a subset of, or more appropriately co-equal with national security. Hence, the effective and efficient structuring of the homeland security system is at the heart of the ability to maintain the American constitutional form of government. For if that ability catastrophically fails by virtue of an immediate or cascading failure to maintain continuity of government and operations, then that failure would put at risk continuance of civil society in America. Succinctly put: It is bad enough to lose a “war” overseas; it is potentially fatal to lose one at home, be it to America’s enemies or to Mother Nature.

## II. THE CURRENT SYSTEM

The structure of the U.S. homeland security system is an amalgam of structures for four functional disciplines that pre-date 9/11 and Hurricane Katrina: emergency management, civil defense, war mobilization and counterterrorism. These structures have had both interagency and intergovernmental (Federal/state/local) dimensions which have been increasingly extendable to include (although not fully formalized) the private sector and nongovernmental organization (NGO) communities. In the 1990s, these four disciplines began to converge with calls for institutionalizing them together into a single structural entity, e.g., as per the recommendations of the Hart-Rudman Commission. At the same time, the military began to use the terms homeland defense or defense of the homeland.

The April 1995 truck bombing in Oklahoma City underscored an escalating terrorism trend line and prompted the Clinton administration to issue Presidential Decision Directive 39 (PDD-39), *The U.S. Policy on Counterterrorism*. PDD-39

---

<sup>1</sup> CRS Report for Congress “Organizing the U.S. Government for National Security: Overview of the Interagency Reform Debates,” April 18, 2008. p. CRS-3.

included consequence management and thus incorporated what had been the realm of domestic emergency management into a national counterterrorism strategy. PDD-39 assigned agency roles and responsibilities and charged the NSC, specifically empowering a senior NSC staff official, Richard Clarke, to take an interagency approach to coordinating terrorism policy issues to ensure implementation of Federal counterterrorism policy and strategy. Among other things, Clarke established a public/private sector study group officially titled the President's Commission on Critical Infrastructure Protection, which in late 1997 identified computer-based infrastructure attacks as a new and serious threat and proposed a government-industry partnership to protect key critical physical infrastructures generally. The following year, two PDDs released in the spring solidly addressed the consequence management piece of PDD-39 and the application of FEMA'S Federal Response Plan (FRP) to a terrorist attack. PDD-62, *Combating Terrorism*, promoted interagency cooperation and coordination in counterterrorism planning and execution. PDD-63, *Protecting America's Critical Infrastructures*, effectively implemented the findings of the 1997 Commission, pending a National Infrastructure Assurance Plan.

State and local authorities also had a role, recognized by the Federal government which accepted some measure of responsibility to support development of their capacities and capabilities. In 1996, Congress established the Nunn-Lugar-Domenici Domestic Preparedness Program. Nunn-Lugar was a Pentagon-led, interagency program (which ran to 2000) to provide training and equipment for better preparing 120 selected cities for weapons of mass destruction (WMD) consequence management. In 1998, the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) established the Office for State and Local Domestic Preparedness (OSLDP), later the National Domestic Preparedness Office (NDPO) which would coordinate all Federal efforts, including those of the Department of Defense (DoD), Federal Emergency Management Agency (FEMA), Department of Health and Human Services (HHS), Department of Energy (DOE) and the Environmental Protection Agency (EPA), to assist state and local first responders with planning, training, equipment, exercises and health and medical support for response to conventional or non-conventional WMD incidents. In 2000, Congress moved Nunn-Lugar functions into OSLDP.

By 2000, a number of quarters in Washington were active with studies and proposals for organizing counterterrorism preparedness. A number of bills and related proposals offered answers to the question of whether the structural focal point for counterterrorism should be in the Executive Office of the President (EOP) or a lead Federal agency.

Following 9/11, this background informed the establishment of the Office of the Director of National Intelligence (ODNI) and eventually the Department of Homeland Security (DHS), i.e., to succeed the initial stand-up of the EOP Office of Homeland Security. The shock of the 9/11 terrorist events predisposed an initial defining and structuring of homeland security in terms of prevention and protection vis-à-vis adversaries. Hence, the structuring of DHS reflected its absorption of legacy agencies—e.g., the Coast Guard, Transportation Security Administration (TSA), Bureau of Customs and Border Protection (CBP)—oriented toward prevention and protection functions as opposed to response and recovery. These latter functions were the focus of the FEMA,

which for over two decades had been building a set of inherited relationships with state and local authorities and which also merged into DHS.

With respect to the Federal relationships with state and local authorities regarding prevention/protection, however, a core issue is the structuring of information sharing, assumed to follow a national security paradigm of top-down, Federal-level sharing with state/local levels. The post-9/11 understanding now recognizes that the homeland security information sharing paradigm (both for counterterrorism intelligence and critical infrastructure protection) is more correctly one which is a two-way street.

After Hurricane Katrina, DHS attempted to rebalance prevention/protection and response/recovery priorities under the mantle of “all-hazards” preparedness. Congressionally-mandated restructuring took place, affecting FEMA in particular, which regained some of its authorities (e.g., for preparedness) lost when it was initially rolled into the initial and second-stage DHS structures. (Congress also took advantage of the national scrutiny of the Katrina response to mandate restructuring within HHS, in view of the manifest need to plan and prepare for pandemic influenza.)

\* \* \*

Throughout the nation’s history, the assumption has been that disasters and even catastrophic events are locally managed. The “Response Doctrine” in the National Response Framework (NRF), the current doctrinal basis for all-hazards response planning, includes this core tenet:

- “Incidents must be managed at the lowest possible jurisdictional level and supported by additional capabilities when needed.”<sup>2</sup>

Beginning in the formative years of the Cold War, however, the Federal government, particularly the executive branch, assumed an increasing role in disaster response and recovery and has been structuring itself accordingly. By the time of Hurricane Andrew (1992), the expectation had arisen that in extreme disasters the Federal government would have the capabilities to execute the primary responsibility for resourcing response/recovery.

Independently in the 1970s, the fire services in the State of California adopted a hierarchical, temporary network approach to incident management for use in fighting cross-jurisdictional wild fires. The approach is called the Incident Command System (ICS). Following its establishment in 1979, FEMA began development of an interagency concept called Comprehensive Emergency Management (CEM) which divided an incident into phases, at the time, four: mitigation, preparedness, response and recovery.

Currently, this all-hazards preparedness spectrum is expressed in terms of five missions: prevention, protection, mitigation, response and recovery. Loosely, a dichotomy is made between preparedness and response; in practice, preparedness—to include planning—undergirds all missions. Mitigation officially is a separate and traditional emergency management mission which includes such natural disaster issues as catastrophic insurance and building code regulations. The PNSR State/Local Issue Team would argue that it is more accurately a functional area within protection. Recovery is

---

<sup>2</sup> National Response Framework, January 2008, p. 10.

now regarded as having two distinct phases—short-term and long-term—which may suggest two distinct mission areas.

In 1983, FEMA brought forth the all-hazards approach for disaster planning with the Integrated Emergency Management System (IEMS) that included, quoting FEMA, “direction, control and warning systems which are common to the full range of emergencies from small isolated events to the ultimate emergency—war.” IEMS was a forerunner to FEMA’s work on a Federal Response Plan (FRP) for a Catastrophic Earthquake in California which ultimately would become a national plan as simply the FRP. Embodying ICS concepts, the FRP informed the process whereby Federal support would plug into state and local incident management of a disaster. Unfortunately, FRP implementation in 1992 did not come in time for Hurricane Andrew, at the time the most catastrophic hurricane to hit the U.S. in the post-war era.

The shock of Andrew resulted in two key developments. At the Federal level, FEMA was dramatically empowered by a new administration which appointed an experienced and activist administrator, James Lee Witt, to lead it. Among Witt’s many successes at FEMA was his thorough development of his agency’s vertical, intergovernmental relationships with the states.

At the state level, governors and emergency managers realized that in addition to the expectation of greater Federal support for response/recovery they needed also to formalize enhanced horizontal, state-to-state relationships for mutual aid in disasters of such scale. The Southern Governor's Association (SGA) and Virginia’s Department of Emergency Services (DES) led the effort to develop a state-to-state mutual aid agreement called the Southern Regional Emergency Management Assistance Compact (SREMAC), adopted in 1993. Two years later, southern governors voted to extend membership to any state or territory wishing to join, which resulted in an expanded agreement, the Emergency Management Assistance Compact (EMAC), administered by the National Emergency Management Association (NEMA). The following year, Congress ratified the EMAC as law making it the first ratified national disaster compact since the Civil Defense Compact of 1950. EMACs cover many of the issues associated with deployed emergency personnel such as licensing, credentialing, liability, workers compensation and reimbursement.

The current homeland security system is thus characterized by the following three dimensions:

- Horizontal interagency relationships at the Federal, state and local levels, needing further formalized extension to the private sector and nongovernmental organizations (NGOs)
- Vertical, intergovernmental relationships, stressed by two (and in home rule states three) levels of shared “sovereign” governance of the same people in the same territory
- Preparedness and operational hierarchical, collaborative networks (temporary in crisis) for prevention, protection/mitigation, response and recovery based on or derived from ICS.

### III. CURRENT HOMELAND SECURITY STRUCTURES

**Federal Structures:** The Homeland Security Council (HSC) and National Security Council (NSC) provide the President with strategic and policy advice. In addition to the President, the members of the HSC are the Vice President, Secretary of Homeland Security, Secretary of the Treasury, Secretary of Defense, Attorney General, Secretary of Health and Human Services, Secretary of Transportation, Director of National Intelligence, Director of the Federal Bureau of Investigation and Assistant to the President for Homeland Security and Counterterrorism (Homeland Security Advisor). The following senior officials are invited to attend any HSC meeting: the Chief of Staff to the President, Chief of Staff to the Vice President, Assistant to the President for National Security Affairs (National Security Advisor), Counsel to the President, Director of the Office of Management and Budget (OMB) and Chairman of the Joint Chiefs of Staff (JCS). Other senior officials are invited to attend HSC meetings pertaining to their responsibilities or otherwise as appropriate.

The HSC is supposed to ensure coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies. It is chaired by the Assistant to the President for Homeland Security and Counterterrorism. As does the NSC, the HSC structure includes the Principals and Deputies Committees. It also has eleven Policy Coordination Committees (PCCs) at the assistant secretaries level, as well as the Domestic Readiness Group (DRG) and the Counterterrorism Security Group (CSG).

As per HSPD-5, *Management of Domestic Incidents*, and the Homeland Security Act of 2002, the Secretary of Homeland Security is the principal Federal official for domestic incident management to implement *coordinated* Federal response. “By Presidential directive and statute, the Secretary is responsible for coordination of Federal resources utilized in the prevention of, preparation for, response to or recovery from terrorist attacks, major disasters or other emergencies.”<sup>3</sup> The FEMA Administrator is a principal advisor to the President, the Secretary of Homeland Security and the HSC for emergency management. The FEMA Administrator also operates FEMA’s National Response Coordination Center (NRCC), supports all Emergency Support Functions (ESFs) and manages the core homeland security grant programs.

The ESF Annexes to the National Response Framework (NRF) align Federal support with fifteen specified ESFs and ten support areas. They define interagency response roles, policies, operational structures and capabilities and assign a Federal lead to the department, agency or other entity best suited to a function or area. Each Annex designates a primary agency or agencies (those with significant authorities, roles, resources or capabilities for that ESF) and support agencies (those having specific capabilities or resources to support the primary agencies).

The ESF structure is supposed to provide the primary operational-level mechanisms for Federal assistance. Through its NRCC, which in an incident increases staff with ESF representatives, FEMA attempts to coordinate ESF departments and agencies through Pre-Scripted Mission Assignments (PSMAs) formalized in interagency agreements. Correspondingly at the regional level, ESF staffs augment the FEMA

---

<sup>3</sup> National Response Framework, January 2008, p. 25.

Regional Response Coordination Center (RRCC) in an incident. At the Joint Field Office (JFO)/Emergency Operations Center (EOC) and incident command levels, field-level ESF staffs integrate into a single branch or group within the respective operations sections.

With respect to the ICS-based and derived National Incident Management System (NIMS), “HSPD-5 requires all Federal departments and agencies to adopt NIMS and use it in their individual incident management programs and activities, as well as in support of all actions taken to assist state, tribal and local governments. The directive requires Federal departments and agencies to make adoption of NIMS by state, tribal and local organizations a condition for Federal preparedness assistance (through grants, contracts and other activities).”<sup>4</sup>

Under HSPD-5, the Secretary of Homeland Security’s operational coordination *excludes* law enforcement coordination which is assigned to the Attorney General and delegated to Director of the FBI. The Attorney General has lead responsibility for criminal investigations of terrorist acts or threats, as well as for coordinating law enforcement to detect, prevent and disrupt terrorist attacks. In an Incident of National Significance (INS), the Attorney General may appoint a Senior Federal Law Enforcement Officer (SFLEO) who allocates law enforcement requirements and resources at the regional or state level. The NRP Terrorism Annex provided for the DHS Secretary to appoint an SFLEO (from any Federal law enforcement agency with primary jurisdictional authority in the incident) in consultation with the Attorney General. Under the NRF, the Attorney General now makes the SFLEO agency designation and appointment unilaterally.

The SFLEO essentially oversees the combined Federal, state and local law enforcement response to the incident. Joint Field Office (JFO) procedures hold that the SFLEO directs intelligence/investigative law enforcement operations related to the incident and supports on-scene the law enforcement component of the Unified Command. NRP language defined the SFLEO as a field-based LE coordinator. SFLEO language is consistent in the NRF which states that the SFLEO is a member of the Unified Coordination Group and, as such, is responsible to ensure that allocation of law enforcement requirements and resource allocations are coordinated as appropriate with all other members of the Group.

As for coordination of the military, while DoD is a full partner coordinated through the NRF, command of Federal military forces for civil support runs from the President to the Secretary of Defense to U.S. Northern Command (NORTHCOM), the combatant command for North America, to the Commander, Joint Task Force (CJTF) who exercises operational and administrative control over Title 10 forces, i.e., Federal or “federalized” military forces.

DoD response thus comes via NORTHCOM, which has a steady-state presence in the 10 Defense Coordinating Officers (DCOs) who serve in the 10 FEMA RRCCs. A DCO processes requirements for military support and forwards mission assignments to DoD. In a crisis, sometimes a DCO will have a Defense Coordinating Element (DCE) to support activated ESFs.

---

<sup>4</sup> National Incident Management System, FEMA 501/Draft August 2007, p. 3.

If an incident requires a major DoD footprint with Title 10 forces, NORTHCOM will assign a CJTF who will co-locate the task force command and control element at the JFO. The CJTF, however, will not replace the DCO/DCE as part of JFO unified coordination staff. The DCO remains the DoD single point of contact in the JFO for requesting assistance from DoD. (Of note, the CJTF does not have operational control of any deployed Army Corps of Engineers which will remain under the Department of the Army.) DoD hence speaks not of *unity of command* but rather of *unity of effort*, reinforcing the fact that Title 10 DoD forces do not operate under command of incident commander or under a unified command structure.

In terms of state and local issues, it is thus apparent that although Federal support to the state level is supposedly coordinated by DHS, law enforcement and military assets owned by the Attorney General and the Secretary of Defense and provided by their respective stovepipes are excluded.

Thus, at the Federal level, structure potentially impedes both unity of command and unity of effort and does not conclusively support unified command at the state and local levels as provided by ICS doctrine.

The Intelligence Reform and Terrorism Prevention Act of 2004 established a director of national intelligence (DNI) and the Office of the Director of National Intelligence (ODNI) to coordinate intelligence sharing. The DNI provides oversight on the newly configured Intelligence Community (IC) which is a confederation of 16 agencies. Only the CIA has a direct reporting relationship to the DNI, who does not have operational control, but resources all 16 member agencies. Of note, DNI has budget authority over the FBI's National Security Branch; DoD intel budgets, however, remain separate. ODNI has the program manager for information sharing. A key ODNI entity is the National Counterterrorism Center (NCTC) which is responsible for integrated analysis and strategic operational planning.

Among the 16 component IC agencies is the DHS Office of Intelligence and Analysis (OIA) led by the Chief Intelligence Officer. Among its responsibilities is the sharing of threat information and assessments with state and local governments and the private sector. Congress designated DHS as the lead agency for coordinating Federal participation in local- and state-owned and operated fusion centers nationwide. To that end, OIA has been working with the Interagency Threat Assessment and Coordination Group (ITACG) to assist the NCTC in producing Federally-coordinated terrorism information products for use by state and local law enforcement.

Under the NRF, the National Operations Center (NOC) is the Secretary of Homeland Security's headquarters-level support structure. "The NOC is the primary national hub for situational awareness and operations coordination across the Federal Government for incident management."<sup>5</sup> The NOC includes NOC managers, all levels of law enforcement, liaison with the Intelligence Community provided by the DHS Chief Intelligence Officer, operations analysts and watch standers. The DHS Director of Operations Coordination is the Secretary's principal advisor for departmental integration of incident management operations and runs the NOC.

The NOC's steady-state operational components are FEMA's National Response Coordination Center (NRCC) and the National Infrastructure Coordination Center (NICC). Supporting Federal operations centers are other DHS operations centers, as well

---

<sup>5</sup> National Response Framework, January 2008, p. 55.

as the Pentagon's National Military Command Center (NMCC), the Office of the Director of National Intelligence's (ODNI's) National Counterterrorism Center (NCTC) and the FBI's Strategic Information and Operations Center (SIOC) which maintains liaison with the National Joint Terrorism Task Force (NJTTF).

The DHS Office of Infrastructure Protection (OIP) leads a coordinated national effort to reduce critical infrastructure/key resources (CI/KR) all-hazards risk. It released its National Infrastructure Protection Plan (NIPP) in June 2006 and the 17 (now 18) supporting Sector-Specific Plans (SSPs) in May 2007. The Homeland Security Act of 2007 realigned OIP which last August issued its FY2008-2013 Strategic Plan.

The NIPP sets national priorities, goals and requirements for funding and resources for CI/KR protection. The NIPP structure incorporates the 18 supporting SSPs to provide a coordinated approach for Federal, state, local, tribal and private sector security partners to revise and update CI/KR protection roles, responsibilities, information sharing and risk management. The NIPP structure includes a State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) and each CI/KR sector's private Sector Coordinating Council (SCC) and Government Coordinating Council (GCC). Each sector has a designated Federal Sector-Specific Agency (SSA). DHS provides to states Protection Security Advisors (PSAs) to liaise with state administering agencies (SAAs) to apply and administer funds for CI/KR protection. The NIPP also provides for a Cross-Sector Cyber Security Plan and Cross-Sector Cyber Security Working Group (CSCSWG) to address cross-sector cyber risk and explore interdependencies across the 18 CI/KR sectors.

**Regional Structures:** The Federal interface with the states for preparedness and response must take into account a number of structural considerations, some of which may involve constitutional issues. DHS has been moving in the direction that emphasizes a regional approach. Federal regional structures are for the most part standardized, if not familiar, e.g., the FEMA and Environmental Protection Agency (EPA) regions, Federal court system, Federal Reserve Districts and historical military and naval districts.

In March of 2008, FEMA transferred some authorities and staff from its National Preparedness Divisions to its enhanced regional structure. The FEMA regions are augmenting with elements from the Radiological Emergency Preparedness Program, Chemical Stockpile Emergency Preparedness Program, Community Preparedness, Assistance to Firefighters Grant program, Continuity of Operations (COOP) and Regional Investment Officers.

The new Federal Preparedness Coordinators (FPCs) at the regional level lead FEMA's efforts to coordinate the broad scope of preparedness missions for all-hazards, particularly with respect to information sharing and relationship building. However, the role and reporting requirements remain somewhat unclear. FEMA is also planning to form a new Grant Programs Division in each region to serve as the central location for administration and management. The realignment hopes to strengthen FEMA relationships with state, local, tribal and NGO partners.

Other regional structures like the New York Port Authority and the Tennessee Valley Authority are organizational governance options along the lines of a public corporation. One homeland security example is the Capital Wireless Information Net (CapWIN). A partnership among the State of Maryland, the Commonwealth of Virginia

and the District of Columbia, CapWIN is developing an interoperable first responder data communication and information sharing network. As such it is a model of an interstate compact agreement and organization.

Another is the Mid-Atlantic All Hazards Consortium (AHC), a non-profit organization, funded by National Capital Region (NCR) Urban Area Security Initiative (UASI) grants. The consortium is guided by the regional states of North Carolina, the District of Columbia, Maryland, Virginia, West Virginia, Delaware, Pennsylvania, New Jersey and New York. The AHC mission is to help create new resources and funding opportunities for the states to support regional multi-state collaboration efforts among all the stakeholders from government, private sector, higher education and non-profit/volunteer organizations.

Enhanced state-to-state relationships have long been underway with state-led alternatives to Federally-imposed regionalization. The most well-known initiative is the state-to-state Emergency Management Assistance Compact (EMAC), as discussed above. During the Katrina and Rita response, EMAC operations involved all member states which deployed a total of 65,929 personnel to the affected areas of Louisiana, Mississippi, Texas, Alabama and Florida. Implementation of NIMS and in particular resource typing will improve the effectiveness of the EMAC structure. (NIMS resource typing is the standardized formatting for categorization and description of response resources that are commonly exchanged in disasters through mutual aid agreements.)

**State/Local Structures:** State governmental structures of course are not uniformly the same. States have their own constitutions. They are internally sovereign and thus have variously organized themselves.

Of the 50 states, four are commonwealths: Kentucky, Massachusetts, Pennsylvania, Virginia. The difference between these commonwealths and the other 46 states is in name alone. The four simply elected to call themselves commonwealths, drawing on a term long familiar in political theory. Whether or not a state is a commonwealth represents no practical difference

However, most states are so-called home rule states. Home rule transfers from state law the authority to act in municipal affairs. The legal basis derives from action by a state general assembly or local charter, adopted and amended by the voters. The responsibility for local governance thus resides in the local community—a county, borough or township—and not with the state legislature. Thus, home rule compounds the challenges posed by federalism, for it presents at the municipal level a third level of shared sovereign governance of the same people in the same territory.

The home rule concept took form in the late 1860s when communities sought local decision-making in response to concentrated corporate powers—trusts—which were beginning to exercise inordinate influence in state and Federal governments. The corporate control over state legislatures had been preventing popular majorities from enacting laws to protect local businesses, natural resources, workers rights and community values.

Today, 43 states have home rule provisions either in law or within the body of their constitutions. Thirty-six provide for municipal home rule in their state constitutions. Eight states provide it by legislative statute. Only Alabama, Idaho, Indiana, Mississippi, Virginia and Vermont do not provide for municipal home rule.

States and territories differ as well in how they have organized for emergency management and how they are structured to receive Federal grant assistance for homeland security.

Of the 55 states and territories, 22 have merged emergency management and homeland security into one department, and four have separate departments with one homeland security director. Some states have incorporated their homeland security and emergency management functions under the adjutant general (TAG) of the National Guard. Eight have the TAG head the emergency management agency or homeland security department. In Florida, Minnesota and New Jersey, the state police run emergency management or homeland security.

As for administration of Federal grants, each state and territory has designated an agency to serve as a so-called state administrative agency (SAA). In some states, the SAAs are their public safety agencies. In others, the emergency management agency serves as the SAA. Each type of agency understandably applies its own institutional bias in developing the state's grant strategy, making it difficult for DHS to integrate a cohesive grant strategy at the Federal level. If the state emergency management agency is its SAA, then grant priorities are in response; if the SAA is a public safety organization, then the funds tend to go to supporting prevention and protection missions.

“Homeland security is thus far more than a technical issue. It is more than a national security issue or a puzzle of federalism. It is, at its core, a problem of governance. And it is one that demands strong and effective political leadership to make the necessary decisions and to shape the necessary trade-offs.”<sup>6</sup>

**A Primer on the Incident Command System (ICS):** Given the interagency and intergovernmental dimensions of domestic management of Incidents Of National Significance, one must be careful not to apply military command and control models. Moreover, one must accept that presidential authority does not extend to directive authority over sovereign state or local components. Hence, it is important to understand the principles of the Incident Command System (ICS), i.e., those which govern management of complex, multi-site incidents involving multiple jurisdictions and levels of government.

Management of a disaster or crisis requires a mix of skills and capacities beyond a single hierarchy and therefore calls for a network of responders. It also demands rapid decision making and decisive, coordinated action which are otherwise associated with hierarchies. Because disasters and crises frequently involve jurisdictional and functional agency overlaps, the purely hierarchical military command and control model does not work. Civil authorities thus have come to rely on ICS for managing complex incidents.

ICS blends hierarchical and network organizational models. A hierarchical network “is a form of social coordination that uses hierarchical control, in the form of unified and centralized command, to help manage a network of organizations pursuing a shared goal.”<sup>7</sup> ICS is a temporary hierarchical authority which establishes in an incident

---

<sup>6</sup> Donald F. Kettl *System under Stress: Homeland Security and American Politics*, Washington: CQ Press, 2004, p. 90.

<sup>7</sup> Donald P. Moynihan *From Forest Fires to Hurricane Katrina: Case Studies of Incident Command Systems* (IBM Center for The Business of Government, 2007. p. 6.

certainty and clarity about the chain of command in order to coordinate a responder network.

The National Incident Management System (NIMS), promulgated by FEMA, is based on ICS-derived principles for modular organization of the Incident Command Post (ICP). Under NIMS, when an incident falls within a single jurisdiction, it is managed at the ICP by a single Incident Commander (IC), e.g., a fire chief, police chief or public health officer, depending on the nature of the incident. “The IC is responsible (within the confines of his or her authority) for establishing incident objectives and strategies. The IC is directly responsible for ensuring that all functional area activities are directed toward accomplishment of the strategy.”<sup>8</sup>

Complex multi-jurisdictional or multi-agency incidents may require ICP management by a Unified Command (UC). NIMS provides that under unified command “[t]he individuals designated by their jurisdictional or organizational authorities (or by departments within a single jurisdiction) must jointly determine objectives, strategies, plans, resource allocations, and priorities and work together to execute integrated incident operations and maximize the use of assigned resources.”<sup>9</sup> Unified command allows officials/responders who have authorities/responsibilities under an appropriate law, ordinance or agreement to work together effectively without affecting individual agency authority. The UC provides direct, on-scene control of tactical operations.

ICS is structured to facilitate activities by section chiefs in five major functional areas—command, operations, planning, logistics and finance/administration. In the case of a terrorist event, an ICS structure would include a chief for a sixth functional area, intelligence/investigation. Resident at the ICP, these section chiefs serve as the “general staff” for incident management and report to the IC or UC.

The IC or UC exercises tactical control via one Operations Section Chief who directs all tactical efforts. This Operations Chief normally comes from the organization with the greatest jurisdictional involvement. (Agencies that are heavily involved in the incident but lack jurisdictional responsibility are defined as supporting and/or assisting agencies.)

ICS thus is a predefined hierarchy which includes a chain of command and delineated responsibilities for every position, uniform terminology for identifying resources and organizational functions, modular organizational structure which the IC or UC can expand or contract as needed, incident action plans which are updated for each operational period and manageable span of control.

Under ICS, the concepts of command and unity of command have legal and cultural meanings which are distinct from military forces and operations. In the military context, command runs from the President to the Secretary of Defense to the commander of the combatant command to the commander of the forces. With ICS, chain of command refers to the orderly line of authority within the ranks of the incident management organization. Unity of command means that all individuals have a designated supervisor to whom they report at the scene of the incident. These principles

<sup>8</sup> National Incident Management System, FEMA 501/Draft August 2007, p. 50.

<sup>9</sup> *Ibid.*

clarify reporting relationships and eliminate the confusion caused by multiple, conflicting directives. Incident managers at all levels must be able to direct the actions of all personnel under their supervision.<sup>10</sup> (NB: Military forces do not now operate under the command of the IC or under the unified command structure.)

Crucially, ICS depends on personal relationships which build on network norms of trust and reciprocity. In a steady-state, network hub members (i.e., those having capacity) work together on preparedness and planning and thereby to develop trust and an ICS culture. As the military says, “Train as you fight.” “Key related aspects of network management are time and stability, both of which are needed to allow network actors to interact with each other repeatedly—which in turn helps to foster agreements, establish shared norms and build trust toward one another.”<sup>11</sup> Also vital is the importance of centralizing information in one place to allow incident commanders comprehensive information to make operational decisions.

As referenced above, the National Response Framework (NRF) response doctrine holds that “Incidents must be managed at the lowest possible jurisdictional level and supported by additional capabilities when needed.”<sup>12</sup> Responsibility for the establishment and expansion of the ICS modular organization ultimately rests with the incident commander. “As incident complexity increases, the organization expands from the top down as functional responsibilities are delegated.”<sup>13</sup>

For complex, multi-site incidents, an Area Command oversees management coordination of the incident(s) and separate ICS organizations with multiple incident management teams. In addition, a Multi-Agency Coordination System (MACS) element, e.g., a communications/dispatch center, emergency operations center (EOC) or MAC Group, coordinates support activities above the field level and prioritizes the incident demands for critical or competing resources. The EOC, hence, is not synonymous with the Incident Command Post (ICP) although it applies NIMS standardized structures and tools to its organizational model. Standing EOCs are usually led by an emergency manager. State-level response would have state EOC over the local EOC which directly supports the IC or UC at the Incident Command Post.

Under principles of unified command, a Unified Coordination Group (UCG) at the FEMA Regional Response Coordination Center (RRCC) coordinates Federal support. The UCG includes a FEMA official, the Federal Coordinating Officer (FCO), and a State Coordinating Officer (SCO) appointed by governor, along with senior officials from the state and key federal departments and agencies and the state. Should the incident intensify, the UCG shifts from the RRCC to a Joint Field Office (JFO). (In a multi-state incident, UCGs and JFOs are established in each state.) At the JFO, the UCG exercises unified command and relays all requests for support from the governor to the Federal government. The JFO is thus a support entity for coordinating Federal support and does not exercise tactical control over any ICS organizations.

---

<sup>10</sup> cf. National Incident Management System, FEMA 501/Draft August 2007, p. 47.

<sup>11</sup> Donald P. Moynihan *Leveraging Collaborative Networks in Infrequent Emergency Situations* (IBM Center for The Business of Government, June 2005, p. 7.

<sup>12</sup> National Response Framework, January 2008, p. 10.

<sup>13</sup> National Incident Management System, FEMA 501/Draft August 2007, p. 45.

#### IV. UNDERLYING ASSUMPTIONS

From its analysis, the PNSR Structure Working Group has observed how national security structure generally reflects three underlying assumptions. If the PNSR State/Local Issue Team were to translate them for homeland security structuring, they would read:

- The president can effectively delegate presidential authority to a lead agency or czar who would effectively integrate homeland security missions.
- Building good capabilities is more important than integrating them well.
- Greater emphasis is placed on manipulations of functional stovepipes than on new structures aimed at integration.

While these assumptions are good observations as to issues of horizontal, interagency integration, by themselves they ignore the vertical intergovernmental dimension which is the reality for any homeland security structure. The matter of presidential delegation of authority thus applies only to Federal structure, and indeed, only to one branch—the executive.

Fully stated, the PNSR State/Local Issue Team recognizes the following underlying assumptions for homeland security structuring—as well as for process and sense-making:

*America’s current national security model—premised on the National Security Act of 1947 and historically driven by issues of national defense—is biased toward addressing situations beyond our borders and only addresses those within our borders which are the most extreme, e.g., acts of war.*

*The constitutional separation of powers with its checks and balances has historically impeded a unified national—and not simply Federal—approach to national security. Unintentionally, these provisions exacerbate fragmentation within and between levels of government with regard to national security and homeland security policy development and operational execution. In a truly national domestic crisis—one which by perception or fact constitutes a threat to our national security—Congress and the American people expect a level of command and control among all responsible Federal and non-federal entities.*

*A high-end terrorist attack falls between a criminal act and an act of war. Absent Federal ability to “command and control” non-federal assets, especially in ambiguous events that may or may not constitute a national security situation, the optimal political and practical goal is to have shared and agreed-upon policy, doctrine and operational capabilities among all levels of government which are not subject to multiple interpretations in the midst of a crisis forming or as it is occurring.*

*Given the above contradictions, the PNSR State/Local Issue Team has concluded that the current 21<sup>st</sup> century risk environment—which includes high-end acts of terrorism and catastrophic natural disasters—no longer permits the easy segregation of national security/defense and the security and safety of the homeland. The presently ill-defined*

*boundaries of 21<sup>st</sup> century national security and homeland security (to include emergency management) frustrate policy development and operational execution.*

## V. PROBLEM ANALYSIS

**The Root Cause of Poor Performance:** *The practical effect of national security and homeland security bifurcation is the creation of parallel policy, doctrine and operational environments—sometimes intersecting, sometimes not. Irrespective, effective management of domestic prevention, protection/mitigation, response and recovery activities requires unity of effort among all levels of government, civilian and military entities and elements of the private sector. Multiple approaches used to address a crisis—in advance or after occurrence—hamper unity of effort and produce ambiguity about the nature of the crisis event itself, i.e., whether it is a national security or homeland security issue and correspondingly which structural mechanisms should manage it.*

*National security policy development has been historically the exclusive domain of the Federal government and has never formally engaged state and local levels. Irrespective of the debates about the efficacy of separating homeland security and national security, even under the current environment, states have a vital and critical policy development and operational role in America’s national security. Structures and/or processes do not harness non-federal governmental capabilities to address exigent national security situations within the borders to supplement and in certain cases perform primary missions to support Federal national security priorities. However, national security and homeland security policies do not always define the roles, responsibilities and authorities of the Federal government, sovereign state and local governments, the private sector and non-governmental organizations (NGOs).*

### CORE PROBLEM

*The fragmented national security and homeland security structure—between and within all levels of government—fails to require and empower systematic collaboration, coordination and integration of strategy and policy development, resourcing and aligned operational execution in steady-state or crises.*

Divided authorities at the Federal level and the persistence of Federal stovepipes affect sense-making. The Federal government does not truly provide an integrative mechanism—other than by defaulting to the president—for effective and efficient facilitation of collaboration and coordination.

The question “Who owns the problem?” extends beyond the interagency dimension to the intergovernmental. In theory, sovereign Federal/state/local authorities having common interests collaborate, coordinate and if necessary integrate effort. However, the structural interagency and intergovernmental mechanisms—such as they exist—are still inadequate to facilitate and resource efficient and effective collaboration, coordination and integration even when perceived common interests are present.

The lack of unity of effort, the absence of shared expectations and inconsistent definition of outcomes are some of the more generalized symptoms of this core problem. Specific examples translate into the following issue areas:

- Ineffective and inefficient alignment of the interagency and intergovernmental homeland security structure
- Ineffective and inefficient alignment of congressional oversight with executive branch homeland security functions
- Lack of clarity as to the Secretary of Homeland Security's role in domestic incident management and improper alignment of certain departmental functions
- Inadequate non-federal stakeholder engagement in policy development
- Improper structuring of homeland security resourcing
- Stovepiped constraints on information sharing

#### **A. Ineffective and Inefficient Alignment of the Interagency and Intergovernmental Homeland Security Structure**

**Homeland Security Council/National Security Council Issue Overlaps:** As presently configured, the NSC and HSC are unequal in status—whether culturally or statutorily. The NSC and the position of National Security Advisor were created by statute, the National Security Act of 1947, whereas the HSC and the position of Homeland Security Advisor came from an executive order (EO), EO 13228 of 8 October 2001. While the HSC ultimately received a statutory mandate in the Homeland Security Act of 2002, it does not have statutory authority to receive appropriations.

While the National Economic Council (NEC) was also created by an EO in 1993, its status vis-à-vis the HSC has not been a problem. The NSC and NEC do not have anywhere near the same degree of membership overlap as do the NSC and HSC. Issue overlaps are infrequent. One such example has been in discussions over long-term recovery policies.

Practically speaking, in the day-to-day, steady-state working of policy, the NSC/HSC membership overlap creates a significant problem in terms of duplication of meetings and attendance. Staffs who sit on working groups for both councils have not the time to attend both sets of meetings which deal with the same issue. Because of the status relationship between the NSC and HSC, most are inclined to attend only the NSC staff gatherings. Best efforts are thus not fully in play in support of the HSC, a junior partner which is still establishing itself. Duplication also gives rise to separate information flows for national and homeland security which (1) degrade information sharing with the state level and (2) increase the probability of intelligence gaps which adversaries will continue to exploit.

Duplication of effort and overlap of missions has led to ambiguity as to which NSC or HSC directorate owns a problem and has the lead. This ambiguity has manifested principally in four issue areas: security of nuclear materials, pandemic strategy, border security and national security emergency communications. In other instances, it has resulted in the subordination of borders-in policy priorities and resourcing: most notably in the realm of counterterrorism where international issues directly relate to and in some cases affect “domestic” homeland security policy.

**EOP/DHS Failure to Integrate Strategic-level Guidance:** After its creation and prior to the establishment of DHS, responsibility for compelling unity of effort was a function of the White House Office of Homeland Security, a function which the office failed to realize. DHS has been no more successful. As former Congressional Budget Office (CBO) Assistant Director Cindy Williams notes, a key explanation behind the DHS failure involves planning and resourcing. More than half of the homeland security budget goes to other Federal departments, and White House planning does not drive a resource allocation strategy.<sup>14</sup>

A recent Center for Strategic and International Studies (CSIS) report maintains that the profusion of strategy and guidance documents reflects confusion as to roles and responsibilities both within the Federal government and between Federal and state/local governments.<sup>15</sup> The Williams study informed much of the CSIS thinking in this regard. According to Williams, most of the homeland security strategy documents and HSPDs are written by committee with the result that “the strategies become a hunting license for agencies wishing to press their own agendas, rather than an articulation of top national priorities.”<sup>16</sup> Elsewhere, she observed, “Unless backed by resources, however, such strategy documents [e.g., *The National Strategy for Homeland Security*] are little more than rhetoric.”<sup>17</sup>

Williams identifies the key EOP players currently advising the President on various aspects of homeland security: the NSC, HSC, OMB and Office of the Vice President (OVP). HSC and NSC staffs chair various PCCs and sometimes co-chair, e.g., the information sharing and maritime security PCCs. The PCCs have issued some 50 National Security Presidential Directives (NSPDs) and 20 HSPDs, some of which overlap. The President has signed some 12 homeland security executive orders since 2001. However, notes Williams, the NSC and HSC “staffs typically do not examine the costs of policy changes.”<sup>18</sup>

To return to DHS, while the Department’s failure to integrate its own “interagency” activities has compromised its ability to integrate homeland security activities across the Federal government, it has also compromised its ability to serve as the lead Federal agency for homeland security support and facilitation for state and local integration of their own corresponding homeland security activities. As a consequence, this effect reinforces Federal stovepipes that undermine ICS at the bottom-up, mission level for local and state authorities which otherwise are beginning to integrate very well. This condition is particularly detrimental with respect to the prevention and protection missions and the public safety community. At the local and state levels, the steady-state relationships now forming between law enforcement and other homeland security

---

<sup>14</sup> Cindy Williams “Strengthening Homeland Security: Reforming Planning and Resource Allocation,” IBM Center for The Business of Government, 2008, pp. 21, 23.

<sup>15</sup> Christine E. Wormuth *Managing the Next Domestic Catastrophe: Ready (or Not)?*, A Beyond Goldwater-Nichols Phase 4 Report, Washington: CSIS Press, June 2008, p. 10.

<sup>16</sup> Williams, p. 29.

<sup>17</sup> Williams, p. 10.

<sup>18</sup> Williams, p. 24.

stakeholders *by themselves* are beginning to translate to vastly improved linkages with the response and recovery emergency management community which in a crisis will make for dramatic efficiencies and effectiveness in unified command.

*Symptomatic of the core problem is the ambiguity in many national security and homeland security roles and missions within the Executive Office of the President (EOP) which creates confusion and impedes clear lines of presidentially-delegated authority to lead policy development and Federal-level operational execution.*

**The Incomplete Authorities of the Secretary of Homeland Security:** In announcing his proposal for a new Department of Homeland Security on June 6, 2002, President Bush told Americans, “This reorganization will give the good people of our government their best opportunity to succeed by organizing our resources in a way that is thorough and unified.” The official description of the DHS seal reads, “The eagle’s wings break through the inner circle into the outer ring to suggest that the Department of Homeland Security will break through the traditional bureaucracy and perform government functions differently.” Unfortunately, DHS has failed to realize the president’s intent or the DHS vision expressed in its seal, i.e., as a department configured as a 21<sup>st</sup> century government enterprise. Considering DHS reality, once the department was up and running, economic sociologist Frank Dobbin characterized it as a “holding company, not a department.”<sup>19</sup>

DHS’s overarching homeland security mission did not replace the old missions of its legacy agencies but rather added a new one. These legacy agencies continue to have their priorities and cultures and are not in a hurry to surrender autonomy to the DHS Secretary, the Office of the Executive Secretary (ExecSec) or elsewhere among the senior DHS leadership, i.e., those who report directly to the Secretary. As such, they have merely moved from their previous holding companies to another—DHS. Resourcing is not thorough and unified, nor is the DHS bureaucracy performing its functions differently.

Absent an empowered DHS Secretary, ExecSec and senior leadership—for the sake of simplicity, “the DHS Secretariat”—intra-DHS agency relationships have been dysfunctional. Most crucially, the fragmented DHS structure perpetuates the pitting of the response and recovery mission stakeholder, FEMA, against the stakeholders in prevention and protection, e.g., Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE) and Transportation Safety Administration (TSA). Intra-DHS agency stovepiping imposes resourcing constraints on homeland security missions above the agencies’ legacy missions. Reinforced by byzantine congressional committee oversight relationships, these stovepipes perpetuate strong workforce cultures in these and other DHS agencies which resist melding at the senior DHS level. For example, the back offices—whether human resources or procurement—have their own training programs and workmen’s compensation packages.

Despite the rhetoric of official documents which attempt to foster a joint, homeland security culture, DHS has failed to institutionalize such a culture even within

---

<sup>19</sup> Quoted in Stephen M. Duncan *A War of a Different Kind: Military Force and America’s Search for Homeland Security*, Annapolis: Naval Institute Press, 2004, p. 96.

its own domain. Hence, intra-DHS relationships are virtually an interagency problem set in themselves, and structurally integration is failing due to the absence of full DHS empowerment at the Secretary level.

This dysfunctional organizational structure has government-wide ramifications, for it particularly weakens DHS in its lead Federal agency role with respect to its dealings with DOJ and to a great extent with HHS in terms of FEMA's managing the interagency aspects of the ESF structure. Because DHS has not been able to move beyond a holding company structure and culture, it continues to reinforce the ability of agencies like the FBI to regard its parent (DOJ) similarly as a holding company, thus perpetuating a resistance by disparate agencies with strong cultures to integrate homeland security policy development and operational execution.

While the Department's failure to integrate its own "interagency" activities has compromised its ability to integrate homeland security activities across the Federal government, it has also compromised its ability to serve as the lead Federal agency for homeland security support and facilitation for state and local integration of their own corresponding homeland security activities. As a consequence, this effect reinforces Federal stovepipes that undermine the Incident Command System (ICS)—the process of unified command—at the bottom-up mission level for local and state authorities which otherwise are beginning to integrate very well. This condition is particularly detrimental with respect to the prevention and protection missions and the public safety community.

*Strong workforce cultures in each department, agency and intra-DHS stovepipes have prevented full institutionalization of a homeland security culture. With respect to DHS, no organizational entity above the DHS agencies—whether in the mission or back offices—effectively drives a common culture.*

**Vagaries in the Homeland Security Budget Process:** As currently organized by statute, OMB exercises its Federal budget reviews via four Resource Management Offices (RMOs) for natural resource programs, human resource programs, general government programs and national security programs. With respect to its review of homeland security budget functions, OMB has a single homeland security branch (established by the White House along with the HSC) under the Transportation, Homeland, Justice and Services Division of the General Government Programs RMO which provides the DHS oversight. However, oversight of non-DHS homeland security areas fall under other RMOs.<sup>20</sup>

Homeland security, thus, does not have a cross-cutting, interagency Federal budget function. According to Williams, the FY08 budget authorities for homeland security spread across 17 budget functions for a total of \$60 billion. The largest amount was \$21.9 billion for homeland security in the National Defense budget function, followed by \$18.4 billion in Administration of Justice, \$9.5 in Transportation, \$4.4 in Health, \$2.3 billion in Community and Regional Development and \$1.3 in International Affairs. The remaining 11 budget functions each had homeland security sums under a billion.<sup>21</sup>

---

<sup>20</sup> Williams, p. 26.

<sup>21</sup> Williams, p. 28.

In addition, definitions of what do and do not constitute a homeland security function have varied over time. “The imprecise treatment of split program elements and abrupt shifts of activities from one side of the ledger to the other side make OMB reports a less useful and reliable tool than they should be for policy makers or analysts wishing to use them to track broad trends in spending.”<sup>22</sup> She concludes, “The absence of a federal budget function for homeland security impedes sound resource allocation in the executive branch and Congress.”<sup>23</sup>

In its report, CSIS noted the lack of an institutionalized OMB/NSC partnership and the failure of the HSC, NSC and EOP staffs to participate systematically in OMB budget reviews. “Cabinet agencies have sometimes used the absence of defined requirements as a reason not to invest in the homeland security area. Without a well-defined process for developing requirements for homeland security, specific capabilities cannot easily be linked to the budget process.”<sup>24</sup> Based on interviews with senior HSC staff, the PNSR State/Local Issue Team notes, however, that current personal relationships between HSC and OMB senior officials did yield positive—albeit ad hoc—budgetary and strategic alignments.

*The currently inefficient budget process does not vest the Office of Management and Budget (OMB) with the appropriate authority to oversee and make recommendations on all Federal homeland security and national security budgets to identify and eliminate duplication of effort among and within departments and agencies.*

**Uncoordinated Intergovernmental Interfaces.** State and local governments do not have a single point—a “one-stop shop”—in the Federal government for coordination of homeland security policies, programs and activities. Initially until the 2006 restructuring, DHS had an Office of State and Local Government Coordination which managed the department’s relationships with states and localities.

According to one former DHS senior official, virtually every DHS component now has a state and local office, but few, if any, of them speak to each other or coordinate their activities relative to states and localities. For example, “S&T [the DHS Science and Technology Directorate] rarely communicates with FEMA, which rarely communicates with the Office of Infrastructure Protection, on a whole host of programs and initiatives.” As a result, no one entity at DHS has the full picture of the department’s state and local efforts; consequently, many programs and policies overlap or even conflict with each other. State and local governments are left struggling to prioritize their own expenditures of time and effort. “It’s a free for all, and states and localities are being pulled in multiple directions simultaneously.”

Policy development has suffered. The State and Local Office led the creation of a state and local working group for the first drafting of the NRP and NIMS in 2004. However, following the transfer of DHS Preparedness Directorate functions to FEMA in

---

<sup>22</sup> Williams, p. 28.

<sup>23</sup> Williams, p. 30.

<sup>24</sup> CSIS, p. 11.

March 2007, the re-write of the NRP into the NRF had little state and local input. Such input only occurred early in the revision process when issues were identified and draft segments written and during the final phase for comments on the draft. However, DHS deviated from the work plan and did not provide state and local representatives with the first full revision draft in the intermediate phase before it conducted a closed, internal Federal review of the draft. As such, the comment phase generated a storm of revisions which delayed issuance of the final NRF by several months and fed state and local mistrust of DHS “partnership rhetoric” about a national as opposed to a Federally-driven response framework.

The stand-down of the State and Local Office also had its operational impacts. The overall communication between DHS and states and local authorities has dropped precipitously since the dismantling of the State and Local Office desk at the National Operations Center (NOC). The 2007 Virginia Tech shooting incident is illustrative. The absence of a state and local seat in the NOC on the day of the shooting was a major factor in the NOC’s inability to communicate with state and local operations centers around the country.

### **B. Ineffective and Inefficient Alignment of Congressional Oversight with Executive Branch Homeland Security Functions.**

In her study on homeland security resourcing, former CBO Assistant Director Cindy Williams enumerates the many problems associated with the current patchwork of congressional oversight over interagency homeland security missions. Says Ms. Williams, “Congress has so far failed to adopt the 9/11 Commission’s recommendation for putting its own house in order.”<sup>25</sup>

“The annual authorization acts that could set the stage for resource allocation have been absent.”<sup>26</sup> “The tangle of committee jurisdictions, insufficient engagement of the congressional support agencies, and the absence of a budget function for homeland security stand in the way of a unified approach to homeland security within the Congress....[L]egacy jurisdictions make it difficult for the secretary of homeland security to exercise his responsibility to align resources to strategy....[I]ntersecting jurisdictions within each chamber make it difficult to pass important authorizing legislation.”<sup>27</sup>

Her recounting of the problem is worth further quoting at length. Whereas the Senate Homeland Security and Governmental Affairs Committee has oversight over part of DHS, “[t]he House Committee on Homeland Security has purview over government-wide homeland security policy.”<sup>28</sup> In the House, “oversight of FEMA’s activities aimed at preparing for and responding to natural disasters falls not under the new committee, but with the Transportation and Infrastructure Committee. Oversight over CIS [Citizenship and Immigration Services] and the Secret Service remains with the Judiciary

---

<sup>25</sup> Williams, p. 31.

<sup>26</sup> *Ibid.*, pp. 32-33.

<sup>27</sup> *Ibid.*, p. 34.

<sup>28</sup> *Ibid.*, p. 31.

Committee. Policy related to customs revenue in CBP remains with the Ways and Means Committee.”<sup>29</sup> Because these committee structures in the House and Senate have different homeland security jurisdictions, DHS leaders have to report to many committees and subcommittees. In addition, the profusion of committees with homeland security oversight means that Congress can’t itself mark budget priorities, audit and review links between planned and executed budgets.

Former DHS officials have made very clear to the PNSR State/Local Issue Team that the fighting among committees has been real and has had a direct and negative impact on their ability to develop homeland security policy. One official spoke of the particular effect congressional squabbling had on preparedness issues, e.g., how various staffs could not agree on where preparedness should be housed within DHS. These tugs-of-war among committees which perceive to have a stake in homeland security has led to programmatic paralysis. The official noted that at one point DHS could not get a full authorizing bill and only recently has been able to get an authorizing bill for the Urban Area Security Initiative (UASI) grant program, among others.

In truth, DHS is not alone among Federal departments in terms of oversight by multiple congressional committees. Broad departments like HHS and Commerce also have numerous congressional overseers, due to the breadth and importance of their programs. In the case of HHS, that department must even engage with several appropriations subcommittees which have funding authority over its many programs. Some make the argument that DHS can in fact benefit from having multiple overseers who can promote greater congressional support through sheer number of stakeholders.

Others disagree, noting that DHS has no analog in other agencies in terms of the extent of oversight given the department. The dimensions of scope and scale, the bifurcated mission elements in DHS (homeland security and non-homeland security), the maturity of DoD, State, HHS, and any number of other exceptions somewhat invalidates such comparisons. DoD, for example, has a budget 15-times larger than DHS and is overseen by only 36 committees, of which a mere six have a real stake. DHS, on the other hand, must respond to 86 such committees. With the continuing management problems at DHS, the bench is not long enough to send subordinates as does Secretary of Defense when Congress requests DoD testimony.

Committee staffers themselves are unabashed in admitting how they use reporting requirements as a means to bully DHS into compliance with one or another priority which their panels might emphasize. In short, congressional oversight harms a struggling department, draining its time and energy.

*Current legislative branch mechanisms (structure, processes, culture, etc.) drive further fragmentation and inefficiencies in execution of executive branch and national security and homeland security responsibilities.*

---

<sup>29</sup> *Ibid.*, p. 32.

### **C. Lack of Clarity as to the Secretary Of Homeland Security’s Role in Domestic Incident Management and Improper Alignment of Certain Departmental Functions.**

As stated above, since the Hurricane Katrina response, the confusion as to the roles and responsibilities of the Principal Federal Official (PFO), Federal Coordinating Officer (FCO) and the Secretary of Homeland Security has generated much debate and discussion. The distinction between the Secretary of Homeland Security as the Federal coordinator for incident command and the FEMA Administrator as the principal advisor to the President and to the DHS Secretary for emergency management is still poorly defined.

The current chain of command among Federal agencies for domestic incident management involving catastrophic disasters is unwieldy and inefficient. The roles and authorities of the Defense Coordinating Officer (DCO), who ultimately reports to the Secretary of Defense, the Senior Federal Law Enforcement Official (SFLEO), who ultimately reports to the Attorney General, the FCO, who reports to the FEMA Administrator, and the PFO in the field, who reports directly to the Secretary of Homeland Security, among others, are less than clear. While HSPD-5, *Management of Domestic Incidents*, designated the Secretary of Homeland Security as the PFO for domestic incident management, the directive bestows no additional authority to the Secretary to execute that mission and does not affect existing statutory authorities vested in other cabinet secretaries, i.e., the Secretary of Defense and the Attorney General.

In regional terms, when FEMA transferred into DHS, its regional structures atrophied. Recently, however, DHS and FEMA have embraced the concept of empowering regional Federal structures for homeland security. Their emphasis thus far has been on the FEMA structure in the context of emergency management response and recovery. FEMA manages its regional relationships with states through its regional administrators who continue to build the capabilities of multi-state operational areas (regions) and the Regional Response Coordination Centers (RRCCs). At present, the FEMA Federal Preparedness Coordinator (FPC) is the key Federal homeland security official at the regional level and is central to the regional-national preparedness framework. However, the focus of the FPC is on preparedness for the entire homeland security mission continuum—not just response or recovery.

In the context of regional empowerment, this new FPC position is apparently one which is both vested and weighted. Thus, the Federal regions now have four Federal positions in the DHS/FEMA “chain of command”—the PFO, FCO, FEMA Regional Administrator and the FPC—each having their own potentialities for the management of a domestic incident and for dual-hatting. However, rather than clarifying the delegation of presidential authority, the creation of yet another empowered Federal official to serve at the regional level compounds the potential for confusion and conflict.<sup>30</sup>

---

<sup>30</sup> Cf. below “NRP Design,” pp. 54-55.

#### **D. Insufficient Non-Federal Stakeholder Engagement in Policy Development.**

*The PNSR State/Local Issue Team takes the view that the National Response Framework (NRF)/National Incident Management System (NIMS)/Emergency Support Function (ESF) construct based on and derived from incident command system (ICS) principles will work for all-hazards incident management from the routine to events approaching the scale of a Katrina hurricane. Exercises and execution in future incidents will generate iterative improvements.*

*The NRF and on-going efforts to develop national planning doctrine for use among all civilian agencies reflect response and recovery imperatives revealed by the 9/11 attacks and reinforced by Hurricane Katrina. Yet the NRF constitutes an operational capability primarily targeting Stafford Act events and to a much lesser extent national security emergencies or broader coordination of domestic prevention and protection operations. Because the national experience is limited with respect to the prevention and protection missions as well as in dealing with national security events and the needed coordination among all Federal and non-federal entities, the National Security Council and Homeland Security Council have not adequately developed shared and understood policy, doctrine and plans.*

**The Intergovernmental Effect of Failed Interagency Leadership:** Domestic homeland security operational doctrine embodied in the NRF and NIMS proposes to institute ICS structures/processes and execution according to principles of unified command. However, the HSC and the DHS Secretary, the executive agent for homeland security, have failed to enforce interagency NIMS compliance. According to one former senior Federal official, the Federal law enforcement community, for example, lags well behind the state and local law enforcement in NIMS compliance. In his view, the White House has provided no incentives for Federal law enforcement entities to expend strapped resources in meeting NIMS mandates, widely perceived to apply primarily to state and local first responders. In early 2007, only some ten percent of Federal Protective Service (FPS) personnel were NIMS training compliant. The percentage was even lower for the rest of the Immigration and Customs Enforcement (ICE) of which the FPS is currently a branch. Quantifying NIMS compliance at the Federal level is difficult, however, absent incentives which drive state and local agency compliance by requiring documentation to qualify for and retain certain Federal grant funds.

This interagency failure has its intergovernmental effect which degrades the ability of state and local jurisdictions to institute ICS. State and local authorities have become especially resentful of what they see as a hypocritical Federal policy which makes their continued eligibility for homeland security grants conditional on their NIMS compliance, when Federal agencies themselves aren't fully NIMS compliant.

Despite the Federal government's professed spirit of partnership, mutual mistrust and scorn result. From the state and local perspective, the Federal government saddles states and localities with unfunded mandates, while it fails to practice what it preaches. From the Federal perspective, state and local governments look for handouts to underwrite responsibilities which are their own. The Federal attempt to discipline the relationship with such grant strictures as the 80/20 rule, which requires states to forward 80 percent of grant allocations to local authorities, works against state-wide planning for

regional collaboration and pits states against localities, in effect replicating fractured Federal/state relationships.

### **The Failure to Engage Proactively Non-federal Stakeholders in Policy**

**Development:** Policy development is a process—more accurately a continuum running from strategic-level guidance to policy development, policy implementation and finally operational execution. For homeland security, the continuum has interagency, intergovernmental and public/private dimensions. Despite the Federal rhetoric of a partnership with state and local authorities, the private sector and NGOs, the HSC and DHS have not systematically brought them into the appropriate phases of the continuum.

At neither the interagency, department or agency level does the Federal government fully or formally engage non-federal stakeholders. To the extent that the current policy development structure and process accommodates non-Federal stakeholders, it does so by putting them in a reactive mode. Despite the Federal rhetoric about *national* policy, the result has been a Federal-centric homeland security policy which lacks consistent and professionally sound standards.

At the HSC level, state and local government policy development input from the responder and emergency management community flows via the Domestic Readiness Group (DRG). However, that input is not heard directly but rather is conveyed via DHS and FEMA representatives.

DHS has the Homeland Security Advisory Council (HSAC) which is comprised of leaders from state and local government, first responder communities, the private sector and academia. HSAC provides advice and recommendations to the Secretary on matters related to homeland security. However, its advice and recommendations come in the form of academically prepared reports reflecting consensus. HSAC products are not formally in the policy development process—i.e., they are not directive.

FEMA's National Advisory Council (NAC) is supposed to incorporate state, local and tribal government, private sector and NGO input in the development and revision of the national preparedness goal, the national preparedness system, the National Incident Management System (NIMS), the National Response Framework (NRF) and other related plans and strategies. With respect to NRF development, establishment of the NAC did not meet Post-Katrina Act deadlines and thus limited the Federal government's collaboration with all non-federal stakeholders. Moreover, FEMA lacks guidance and procedures for including non-federal stakeholders in developing both national response doctrine and future NFR revisions.

**Failed Private Sector/NGO Engagement:** Governmental definitions may support engagement, but doctrinal statements have not translated into operational substance, particularly as relates to the private sector. Agencies often cite constraints posed by proprietary and competitive information sharing issues. Workarounds, such as the use of a non-profit representative to provide good offices for representing private sector inputs, do not wholly resolve competitiveness and equitability concerns. Firms who are not members of a particular non-profit could raise objections. Other approaches like the U.S. Chamber of Commerce agreement with FEMA to have a representative in the National Response Coordination Center (NRCC) raise additional questions, e.g., who

bears the costs of such representation. On the other hand, the private sector views such issues as “tactical problems” capable of resolution.

No FEMA or DHS office serves as an empowered sponsor for a public/private partnership. FEMA has Cindy Taylor, the director of its Private Sector Liaison Office, but neither Ms. Taylor nor anybody else in a senior position in FEMA has line authority to manage the relationship. DHS has Al Martinez-Fonts, assistant secretary for the DHS Private Sector Office, a division under the Office of Policy. However, the Private Sector Office does little beyond facilitating a public/private dialogue. It is not empowered to institutionalize public/private partnerships. Like FEMA’s Private Sector Liaison Office, it is not charged to manage the private sector, nor do either have the motivation or incentive to do so. For the most part, the mechanisms at the state and local levels mirror these Federal-level approaches.

Operationally, the private sector and NGO communities do not fully participate in exercises and planning. Indeed, Federal agency support to state and local exercise programs is uneven and in rural regions often non-existent. Exercises are the fora for validating inputs for threat assessments and gap analyses and provide a critical means for assessing state- and local-level capabilities. Without a full intergovernmental, public/private partnership—which includes participation in exercises and planning—critical infrastructure sectors and individual private sector entities are forced to do assessments and gap analyses in isolation to determine their own capabilities and gaps. As a result, findings by individual firms and companies do not accurately reflect their vulnerabilities nor their surplus capabilities to support community response.

State and local private/non-profit coordination are more consequential for local outcomes than for the Federal government. However, Emergency Support Function (ESF) policy development has been top-down and Federal-centric. ESFs do not presently include a private sector component—for that matter, neither do state-to-state Emergency Management Assistance Compact (EMAC) mechanisms. From the private sector perspective, ESF mechanisms support only government outcomes—life saving and protection of property. This Federal top-down approach is disconnected from the private sector’s bottom-up approach to ESF policy development for supporting *community* outcomes. Private sector organizations define these outcomes in terms of resiliency—restoration of community self-functioning as quickly as possible.

Because the Federal government has not formally engaged national corporations in the policy development process, private sector disaster response policies have no commonality at the national level. Absent a common set of private sector expectations, community-level corporate entities are left to plan on their own, making it difficult to develop scale-up capabilities for catastrophic incidents.

The Federal top-down approach is reinforced by law which does not support bottom-up community building. The Stafford Act along with the nationwide body of disaster law does not include the private sector and does not facilitate the integration of business into disaster response planning at the Federal, state or local levels. The law does not designate the private sector as a critical component of a comprehensive disaster response mechanism. Moreover, Stafford Act preferences work against participation by local businesses.

At the state and local levels, emergency operations centers (EOCs) do not have consistent representation from critical infrastructure industries or other

industries/companies vital to community viability and continuity in crisis situations. In some cases, inputs, such as they are, must be funneled through the EOC Liaison Officer that operationally can result in bottlenecks.

**FACA Constraints on Executive Privilege:** Formal participation in homeland security policy development by non-federal stakeholders is constrained by concerns over executive privilege and the application of the Federal Advisory Commission Act of 1972 (FACA). Executive privilege was an issue in two high-profile policy development cases: First Lady Hillary Clinton's healthcare reform panel in the early 1990s and Vice President Dick Cheney's Energy Task Force in 2001.

The law governing executive privilege remains unclear, despite its having been invoked since the time of George Washington. The Constitution nowhere expressly mentions executive privilege. Presidents have long claimed, however, that the constitutional principle of separation of powers implies that the executive branch has a privilege to resist encroachments by Congress and the judiciary, including some requests for information. Otherwise, key advisors would hesitate to speak frankly if what they said in counsel could become a matter of public record. On matters of national security, for example, executive privilege provides for an accepted degree of confidentiality.

Under FACA, if a government group includes a member who is not an officer or employee of the government—e.g., a non-federal homeland security stakeholder—then the group's proceedings must be available to the public. FACA mandates that certain documents, task force members, meetings and decision-making activities be open to the public. FACA thus needs to square with the contention that executive privilege extends to conversations between executive officials and persons outside the Federal government.

Not restricted to the Federal level, this FACA/executive privilege issue extends to policy development and operational conversations at the state and local levels. For example, conversations in EOC deliberations are governmental and sensitive and are not categorized as public information. Under current law, however, if a private sector or NGO representative is present, EOC deliberations would not be exempt from the Freedom of Information Act (FOIA) or covered by executive privilege.

FACA was not written with the idea of homeland security and national security discussions, many of which are time sensitive and do not lend themselves to the Act's notification requirements. In these cases, virtually no current mechanism engages state, local, private sector and NGO perspectives in a meaningful and decisional way. Agencies are precluded from talking about issues with their constituents, because of classification or pre-decisional deliberation requirements, and most of those are legacy issues from a time when state, local and private sector entities did not have the stake they do today. Hence, FACA's time consuming requirements impede the very coordination needed among Federal, state, local, private sector and NGO representatives for both homeland security and national security policy development, especially under exigent circumstances.

*Despite the language of such foundational policy documents as the National Security Act of 1947, Homeland Security Act of 2002, Intelligence Reform and Terrorism Prevention Act of 2004 and others such as National Response Framework (NRF), the National Security Council (NSC) and Homeland Security Council (HSC) have no*

*standardized process to solicit and receive state, local, private sector and NGO input into the development of national policy.*

No Federal department or agency relies more heavily on state, tribal and local governments for the success of its mission than DHS. However, since 2006, DHS has gone without a State and Local Government Coordination Office to work directly for the DHS Secretary with resources and authorities to fulfill its mission as originally set forth in the Homeland Security Act of 2002. State, tribal and local officials lack a one-stop shop for information, policy input and issue coordination among the various DHS components. With the myriad of programs and policies emanating from DHS, its engagement with these critical stakeholders is fragmented and often conflicting.

### **E. Improper Structuring of Homeland Security Resourcing.**

*The cross-cutting, interagency structure for national security and homeland security resourcing fails to translate effectively and efficiently capability requirements into budgeting and programming.<sup>31</sup>*

Too many grant programs with too many requirements overwhelm state and local authorities which have not the infrastructure to handle them. While some grant programs, specifically the Urban Area Security Initiative (UASI) grant program, have encouraged multi-jurisdictional coordination, others have mechanisms which work against collaboration, fragmented state and local planning and reinforce Federal stovepipes.<sup>32</sup>

**Deficient Risk Analysis Capabilities.** Risk is supposed to guide DHS priorities and the nation's overall homeland security actions. Risk analysis drives operational decision-making, and its products support the missions of the DHS components (e.g., CBP and TSA) and other Federal agencies.

This support is especially important for state and local governments. However, DHS has proved incapable of adequately assisting state and local risk analysis and management efforts. The department lacks the technological capabilities and strategic vision to collect all risk data and analyze them for trends and patterns, including suspicious activity reports—particularly reports on those activities which may involve terrorist pre-operational surveillance against critical infrastructure. According to one former senior DHS official, DHS cannot link in real-time—if at all—a suspicious activity collected by the Federal Protective Service in New York City with one collected by the NYPD or a private security guard.

Risk analysis informs the measures in place to secure national critical infrastructure under the National Infrastructure Protection Plan (NIPP). However, despite DHS's new regulatory authority over the chemical sector, specific data on vulnerabilities

---

<sup>31</sup> Cf. below “Inadequate Planning Compromises Effective Resource Decision-making,” pp. 45-47.

<sup>32</sup> Cf. below “Resourcing via a Fragmented Grant Structure,” pp. 48-52.

and consequences are not readily available to merge with intelligence to create a comprehensive and detailed risk picture for that sector.

The deficiency in the DHS risk analysis capability results from the department not having a risk analysis center—or centers—to drive and support operational components and those components' planning and operations to mitigate identified risks. The activities of the DHS Homeland Infrastructure Threat Reporting and Analysis Center (HITRAC), the most logical place to house this capability, are primarily focused on intelligence and terrorist threats and do not include a broader view of vulnerability and consequence data to include threats posed by nature and accident.

The only meaningful risk analysis currently ongoing at DHS is in the Grants Program Directorate at FEMA where it informs allocation of preparedness grant funding. However, since 9/11, the Federal government has provided well over \$20 billion in grant funds to states, localities and tribes. DHS can provide details on what actions or activities have been produced as a result of that spending. It can itemize the number of radios purchased in a given locality, border patrol agents hired, first responders trained in WMD response or intelligence fusion centers established across the U.S., and so forth. However, it cannot adequately account for the benefits or increased level in capability resulting from such actions/activities, nor can it demonstrate what level of capability is sufficient, given the risks a jurisdiction, critical infrastructure or key resource sector may face. As such, absent a robust DHS risk analysis capability, risk management has been more about measuring outputs than outcomes.

It's a given that the nation does not have the resources to protect everything from every threat. Nor is it easy to agree on performance measures for prevention and protection outcomes—if nothing happens, has prevention been successful? Absent a catastrophe, homeland security drops off the radar, and other priorities come to the fore to compete for the resourcing.

*Currently, the Federal government and DHS have no satisfactory definitions for homeland security risk, outcomes or end-state, nor objective measures of performance for operational success.*

## **F. Stovepiped Constraints on Information Sharing.**

At the Federal level, persistent stovepiping in knowledge management degrades performance across the prevention, protection/mitigation, response and recovery missions. Problems are particularly evident with regard to interagency, intergovernmental and public/private information sharing. Residual interpretation by the Federal law enforcement and intelligence communities with regard to information which in another time would be classed as need-to-know undercuts progressive efforts by state and local authorities which are independently moving toward a responsibility-to-provide information sharing culture which encompasses all-hazards.

**Security Classifications and Clearances:** The right type of information sharing does not fully flow via the National Response Framework (NRF) and the Emergency Support Function (ESF) structure across the full spectrum of homeland security missions: prevention, protection/mitigation, response and recovery. As a consequence, the

NRF/ESF structure does not properly work in a nebulous situation where classified information is involved or in a complex set of incidents not bound by a specific site.

At the heart of the obstacles to information sharing is the matter of standards for security classifications and clearances. The National Security Act of 1947 defines classification authority for information sharing. The Homeland Security Act and to a lesser degree the Intelligence Reform and Terrorism Prevention Act have modified that authority. During the Cold War, the National Security Act standards were clear, but in today's threat environment such classifications as Sensitive But Unclassified (SBU) and Law Enforcement Sensitive (LES) are far too subjective. Rather than clarify, the Homeland Security Act and the Intelligence Act have further obscured objective interpretation.

DHS has been trying to set a new paradigm to expand to the private sector and clear appropriate representatives to the secret level, but DOJ, DoD and ODNI are not aligned with this effort. As a result, the substance of DHS information sharing has been less than desirable

The solution hinges on three definitional security criteria for information: what would be the potential consequences if the information were released; how would it be wrongfully released; and whose hands would be the wrong ones to have it.

DHS also finds difficulties in intra-agency information sharing. For example, Immigration and Customs Enforcement (ICE) constraints are generally identical as those of other components within DHS from the standpoint of handling national security information. However, the immigration and naturalization part of ICE responsibilities presents some additional constraints from a privacy standpoint. ICE is prohibited from releasing a lot of information from its "A-files"—the legacy INS term for its investigative files. "Illegal" alien information cannot be shared except under special conditions.

The structural response to the 9/11 attacks attempted to address what was identified as a failure of information sharing—the inability of the intelligence and law enforcement communities to "connect the dots." Heightened bureaucratic, legal and cultural barriers to sharing had existed ever since the revelations of domestic spying during the Church Committee hearings in the mid-seventies. Since 9/11, the reexamination of the trade-off between civil liberties and security among other things has been driving an evolution from a need-to-know, through a need-to-share to a responsibility-to-provide information sharing culture. In terms of homeland security, information sharing is the critical enabler for the prevention and protection missions. Connecting the dots today still depends on an interagency and intergovernmental structure/process.

**Failure to Determine Responsibilities for Collection:** Despite the establishment of the Office of the Director of National Intelligence (ODNI), information sharing and collection is still a major problem. ODNI remains unable to implement an overall/overarching process or policy for determining the most important collection requirements from a multi-agency perspective.

Each intelligence agency charged with collection develops its own collection requirements—whether based on the intelligence analyst's recommendations, agency policy or operational requirements. It is more the exception than the rule for an agency to have "unique" intelligence requirements, for which no other agency requires the

intelligence. Because more than one agency often has the same or similar intelligence requirement(s), duplication of efforts invariably exist. For example, despite the intelligence community's shake-up over the past few years, DoD intelligence agencies are still not integrated with or coordinated by ODNI, reinforcing invariably duplicative collection efforts.

ODNI is unable to determine which, if any, agency is collecting, and equally problematic, whether multiple agencies are collecting on the same sources. As a consequence, it can neither determine whether some intelligence data, useful to fulfill a requirement for another agency, are sitting in an agency nor whether an agency has already collected or concluded that no intelligence sources are available.

For the prevention and protection homeland security missions, the delegation of presidential authority is far from clear. When DHS attempts to do the trade-offs and decision-making vis-à-vis its legacy agencies, it has too many cooks in the kitchen, whether it is HSC, ODNI or some other semi-empowered Federal entity. In its struggle to coordinate information sharing and define the hydra-headed homeland security missions, DHS finds that mission boundaries are less mission-driven than politically determined.

**Applying the Positive Example of Joint Terrorism Task Forces (JTTFs):** To a degree, within the narrowly defined prevention and protection missions, Federal/state/local information sharing has been improving, as evidenced by the Joint Terrorist Task Forces (JTTFs). Today, 102 JTTFs across the country operate as cross-functional teams with state and local law enforcement officers benefiting from their service in a collaborative, interagency/inter-governmental network. The Government Accountability Office (GAO) assessment of the JTTF concept notes: its “defined and articulated common outcome; mutually reinforcing or joint strategies; leveraging common resources; agreed roles and responsibilities; and compatible policies and procedures among other elements.”<sup>33</sup> JTTFs are “structured to meet mission requirements rather than managerial vision per se.”<sup>34</sup> The JTTF structure owes its relative success to its composition and tasking. JTTF members essentially come from two related disciplines, law enforcement and the military, and are tasked with a single mission, counterterrorism.

Focused composition and mission tasking have similarly worked elsewhere for prevention and protection. Notable examples are the DoD-led Joint Interagency Task Force (JIATF) which coordinates the counter-drug mission and the DEA-led El Paso Intelligence Center (EPIC) which serves as a very capable data repository for all transnational threats. However, less certain is the success of the DoD-led Joint Interagency Coordination Group (JIACG) which may support a number of other missions but is not accountable for immediate demands of a mission of its own.

The problem is that prevention and protection are only two homeland security missions along the homeland security mission continuum—prevention, protection/mitigation, response and recovery. The JIACG concept poses a challenge to

---

<sup>33</sup> Will Goodman “Making Consequence Management Work: Applying the Lesson of the Joint Terrorism Task Force” *Homeland Security Affairs Journal*, to be published later this year.

<sup>34</sup> *Ibid.*

DoD, with its military mission set, and civilian Federal agencies, with core prevention and protection missions. For them, the interagency homeland security space is still not comfortable if it means having to share information with departments and agencies whose taskings fall across the full range of homeland security missions and require integration both in process and structure. Unfortunately, the effect of their retreat into their Federal stovepipes gets magnified when it comes to the intergovernmental dimension. It often undoes the interagency collaborative cultures for information sharing at the state and local level which authorities—independent of the Federal government—have successfully established.

**Fusion Centers and All-hazards Applications:** The problems with the Federal fusion center initiative is a case in point.

Intelligence/information fusion is a key management mechanism for sharing. Last year's National Strategy for Information Sharing made fusion centers the keystone for information sharing with state and local authorities. Fusion centers serve as a structured process for collection, analysis, archiving, tasking and dissemination which is ongoing with state, local and private-sector entities. This Federal effort has been underway to support and network state, local and major urban area fusion centers which now total some 43 such centers nationally. Originally instituted for law enforcement applications, fusion centers are resident in state police or public safety agencies, but unlike JTTFs their representation is multi-disciplinary. As such, many states have chosen to leverage their capabilities for the broader all-hazards missions. By doing so, they bump into information sharing barriers imposed by Federal agencies which frustrate collaboration and reinforce mistrust.

Recent advances in platform and bridging technologies provide the means for fusion centers and the like to overcome some of the technological barriers to sharing which have arisen in the IT transformation of the last 20 years. Yet the perennial bureaucratic, legal and cultural barriers remain.

For its part, DHS has been slow to provide funding to sustain the centers. Its grants are supposed to sustain the baseline of a state's fusion center capabilities. However, compliance requirements and uncertain funding levels are casting doubts on the program. DHS and Justice collaborated in developing fusion center guidelines. Now, Justice is complaining that states are using grants for all-hazards applications beyond purely counterterrorism, the FBI's preferred focus. The FBI is thus pressuring fusion centers to adopt restrictive information dissemination policies where information cannot go beyond law enforcement in a timely manner by reason of the potential to compromise investigations. In some states, fusion centers have begun to scrub information to the point where it is ineffective or annotated Law Enforcement Sensitive (LES) as opposed to For Official Use Only (FOUO). According to one state official, DHS and Justice have recently cut their information dissemination to state fusion centers by some 70-80 percent—possibly in response to state information sharing policies.

The Federal displeasure with states' using fusion center grant funds to expand their centers' all-hazards capabilities instead of narrowly applying them to criminal and intelligence applications represents a fundamental structural failure. DHS and Justice fusion center policy exemplifies persistent Federal stovepiping to build narrow capabilities instead of *integration* of capabilities.

Some states have thus chosen to opt out. For example, Delaware went with establishing its own fusion center, the Delaware Information Analysis Center (DIAC), using significant state resources combined with Federal funding. The DIAC has gone beyond serving as an intelligence center. It focuses on collecting, analyzing and distributing information and intelligence to agencies throughout the state for fire, emergency medical system (EMS), public works, corrections, medical services and other Federal, state, local and industry agencies. In addition is the contribution of a statewide computer-assisted dispatching system, the state Transportation Management Center, Delaware Emergency Management Center and DIAC planning currently under implementation throughout the state. This approach provides linkage and analysis to a far greater reach of public and private sector entities. Reflecting the transition from law enforcement to homeland security, the DIAC addresses the broader security and safety challenges by taking a new government/private sector business perspective. DIAC chose apply precious state funds with Federal monies to expand the fusion center concept to one for all hazards, but not all states can afford that option.

Major municipal-level authorities have also engineered their own alternatives to problematic Federal mechanisms to sharing. Well-resourced police departments in New York and Los Angeles have created their own networks which they are leveraging regionally, and, in New York's case, nationally. NYPD's Operation Shield and its related nationwide Operation Nexus provide networks of information sharing with the private sector. Its Operation Sentry leverages its capabilities to enhance and partner with regional law enforcement for a two-way street in counterterrorism information sharing. LAPD has a similar effort with its Joint Regional Intelligence Center (JRIC).

With respect to incident management and situational awareness, the National Guard Bureau (NGB) is attempting to overcome institutional and cultural impediments to civil/military information sharing by putting a direct link between the National Guard's Joint Force Headquarters-State (JFHQ-State) and NORTHCOM. JFHQ-State provides C<sup>4</sup>I for all military units (Title 10 Federal forces and Title 32 National Guard forces) in a response and is very capable. But information does not go directly to NORTHCOM but rather via the NGB. This spring, the NGB was circulating a draft concept of operations (CONOPS) for putting a Guardsman in each state fusion center with links to NORTHCOM, but such an approach raises Posse Comitatus Act concerns (as were raised with respect to military membership in the JTTF structure). Because such information sharing cannot be formalized in a steady-state environment, "trust" issues are factors in both pre-incident and incident phases. NORTHCOM has attempted a work-around for establishing a common operating picture (COP) and enabling crisis information sharing by deploying some 15 Federal teams to get their own data, in some cases necessarily in an unclassified form, which presents another set of issues.

Though supposedly well-intentioned, these kinds of work-arounds unwittingly reinforce institutional boundaries, mission overlap and confusion over roles and responsibilities. The National Response Framework (NRF) itself is not without blame. For example, the DHS National Operations Center (NOC), the FEMA National Response Coordination Center (NRCC) and the National Park Service's National Interagency Fire Center (NIFC) all serve as Federal emergency operations centers for wildland firefighting. While not a 9/11 or a Katrina, for Western states, wildfires can be major regional catastrophes. Hence, in its current form the NRF appears to be unable to resolve

these Federal stovepipe issues for situational awareness and management of a domestic incident.

**Effect on Unified Command:** Strictures against intergovernmental information sharing hamper both operational effectiveness and exercising. The PNSR State/Local Team is aware of three recent examples involving the relationships among state officials, fusion centers and Federal law enforcement agencies which indicate the corrosive effect of Federal information stovepiping on the establishment of unified command.

The first case was a possible bioterrorism incident where intergovernmental information sharing strictures not only prevented establishment of unified command but also delayed diagnosis. This delay placed patients, presenting with symptoms due to unknown causes from a potential intentional exposure, at risk.

Routinely, state and local law enforcement and health officers work side-by-side to assure collection and analysis of samples in a way to protect evidence/chain of custody and make results immediately available for health practitioners. Health officers will use a certified Laboratory Response Network (LRN) lab to obtain preliminary or actual results, generally within 12 hours, which provides those results to the state health officials and health practitioners treating patients who present and require treatment due to a presumed exposure.

According to a state official, in this particular incident “the FBI intervened in the response effort, sequestered the samples and significantly delayed the availability of results to public health and health providers involved in the case.” He further stated, “The FBI Liaison told me the decision was made to sequester the samples, conduct testing at his [FBI] laboratory and withhold the results, because the event, while causing adverse health effects, did not appear to involve an infectious agent. There was no need for non-law enforcement officials to be informed of the results so as to prevent any compromise to the investigation.”

In a second incident, a threat was made by a known individual with a criminal past against a specific hospital system. The state fusion center disseminated that information specifically to law enforcement agencies. It was not until a full day later that the center notified security/emergency preparedness individuals at state-level public health and the hospital of concern. The fusion center maintained that “Federal LE [law enforcement] did not want the potential for compromising the investigation.” “On the health side,” this state official observed, “we felt that the safety of hospital personnel and critical infrastructure would have been jeopardized if that threat had materialized.”

A third example is an instance where state emergency planners were involved in developing a multi-agency, Federal/state/local exercise involving a simulated intentional event. According to a state official, the particular FBI Regional Office policy was to collaborate on the exercise with non-law enforcement state and local agency officials only through another Federal agency. “This policy forced me, the state's lead agency exercise director, and the Regional FBI officials whose subject matter expertise was needed in order to fully develop the scenario/MSEL [Master Scenario Events List], to travel to a distant out-of-state city where the third party Federal agency was headquartered, to discuss the exercise. This was an unnecessary and unreasonable demand, particularly since the involved state agencies and FBI Regional Office are

located only a few miles from one another. It is, however, indicative of the poor level of trust demonstrated by the FBI to non-law enforcement agencies on a day-to-day basis, though these are the same agencies the FBI must work with when responding to an event." According to the official, "The FBI had taken the view that 'to discuss scenario events directly with a state organization could compromise law enforcement-sensitive information collection and investigative processes.' This was for just a simple exercise where the state officials wanted to invoke the FBI for the purpose of collaborative planning efforts and response strategies."

**Critical Infrastructure Protection Information Sharing:** While information sharing with respect to the prevention of and protection missions may appear to be focused vis-à-vis terrorist threats, it actually overlaps with sharing for all-hazards critical infrastructure protection. Thus far, DHS has not been wholly successful in its engagement with the private sector, which, as is oft cited, owns 85 percent of the nation's critical infrastructure. Poorly managed critical infrastructure information sharing contributes to the lack of operational components and mechanisms for the private sector and local communities to participate fully in National Infrastructure Protection Plan (NIPP) risk management framework. While top-down Federal information sharing is somewhat adequate within the 18 critical infrastructure/key resources (CI/KR) sector "pipes," sharing is not occurring at the community level across those pipes.

One of its principal failures has been DHS's patchy implementation of Protected Critical Infrastructure Information (PCII) accreditation (which many states do not yet have). The DHS PCII program is intended to enhance information sharing between the private sector and the government. DHS and other Federal, state and local governments are trying to use PCII to analyze and secure critical infrastructure and protected systems, identify vulnerabilities, develop risk assessments and enhance recovery preparedness measures. The problems with PCII reflect general public-private tensions arise over inclusive collection, selective sharing and cyber vulnerability, e.g., worries especially intense in the electric utilities sector. A further issue is how the Federal-level is going to accommodate with the states the private sector's preference for national (vice state) standards and as well as for standards applying to tools specific to each of the 18 CI/KR sectors. Yet to be determined are the answers to the questions who owns the problem, who pays for what and in what proportions. Steady-state information sharing for critical infrastructure protection (CIP) presents a structural challenge that has consequences in a crisis. In the words of former DHS Undersecretary for Preparedness George Foresman, "The public sector can relate to the private sector as a victim, a vendor or a partner. Both understand the vendor and victim parts pretty well, but they don't yet know what it means to be partners." This disconnect complicates planning in a major way at the state and local levels.

Without continuously updated CIP information sharing, government planners have no accurate sense of private sector vulnerabilities in terms of protection or capabilities in terms of response. DHS has failed to engage the private sector to resolve their concerns over information sharing and competitiveness and Federal of Information Act (FOIA) issues. That failure, for example, hinders any attempts to bring the private sector into deliberative planning and Emergency Operations Center (EOC) operations during the execution phases of an event.

*DHS, Justice, DoD, ODNI, the HSC and other Federal entities with homeland security mission responsibilities—along with their state and local partners—have failed to institutionalize a comprehensive and workable information sharing structure and a responsibility-to-provide information sharing culture.*

## **A. ASSESSMENT OF PERFORMANCE**

### **A. Policy and Strategy Development:**

In 11 June 2008 testimony before the House Homeland Security Subcommittee on Management, Investigations and Oversight, William O. Jenkins, Jr., the GAO director of homeland security and justice, said that DHS has failed to engage state and local stakeholders fully in catastrophic preparedness development.

In his written testimony, Jenkins summarized the GAO report on the DHS process to review the National Response Framework (NRF)—the foundational doctrinal statement for national response. GAO said, “DHS deviated from the work plan it established for the [NRF] revision process that envisioned incorporation of stakeholder views throughout the process and did not provide the first full revision draft to non-federal stakeholders for their comments and suggestions before conducting a closed, internal federal review of the draft.”<sup>35</sup> Not a departure from the norm, GAO cited a similar pattern with respect to development of the 2005 National Pandemic Strategy and 2006 National Pandemic Implementation Plan. “Key non-federal stakeholders, such as state and local governments, were not directly involved in developing the National Pandemic Strategy and Implementation Plan, even though these stakeholders are expected to be the primary responders to an influenza pandemic.”<sup>36</sup>

**Interagency National Cargo Security Strategy Development:** Development of a national cargo security strategy would suggest an interagency drill which would involve stakeholders from the staffs of the NSC, HSC and NEC, as well as the Coast Guard, Department of State and other Federal departments and agencies and non-Federal public and private stakeholders. It was, however, a DHS-led effort with mixed results.

The difficult task of merging varied and numerous governmental agencies and functions into the Department of Homeland Security was initially made even more difficult when it was apparent that the Administration originally opposed DHS’s creation. This lack of “status” hindered selection of agency leaders and allowed turf issues to remain unresolved. Security protocols premised on the “need to know” rather

---

<sup>35</sup> Government Accountability Office *Emergency Management: Observations on DHS’s Preparedness for Catastrophic Disasters*, June 11, 2008, p. 8-9.

<sup>36</sup> *Ibid.*, p. 9.

than the “need to share” further hindered effective inter-agency and federal-state and public-private coordination.<sup>37</sup>

Since 9/11, port authority stakeholders had been pushing the terrorist threat to ports and cargo as a transportation security issue worthy of equal time to airports. As Deputy DHS Secretary, James Loy embraced an effort in 2004 to develop a national cargo security strategy which was to build on a number of national and international initiatives such as the Container Security Initiative (CSI), Customs Trade Partnership Against Terrorism (C-TPAT), International Ship and Port Facility Security (ISPS) Code, etc. However, this particular challenge, otherwise expressed as “container security,” transmuted into far too big a problem. Supply chain experts made the point that cargo security went beyond just port security to include intermodal dimensions which included the railroad, trucking and warehousing sectors. Linked to the larger issues of transportation security, port security approaches overlapped with aspects of passenger security as well. The cargo security strategy thus bounced into the too-hard category with no final policy to guide acquisition or grants, simply stated: who gets what and who pays. Loy’s effort fell flat after his departure in March 2005. As for the ports, the eventual grants were for minimal amounts, sums used more for “guns, gates and guards” than for container security devices and hand-held and portal monitors.

Cargo security had already become rhetorical fodder for the Democrats in the 2004 presidential campaign. Not prepared to rely on DHS’s ability to manage port security, port stakeholders had already lobbied Congress to take the lead. Among the champions was South Carolina Democratic Senator Fritz Hollings, author of the Maritime Transportation Security Act (MTSA), the nation’s first Federal maritime security law. Hollings pushed funding for Project SeaHawk, the Charleston Harbor Operations Center (CHOC). Focused on the Port of Charleston, the second largest container port on the East Coast and fourth largest in the nation, SeaHawk was a benchmark project administered by the U.S. Attorney’s Office for the District of South Carolina. Its goal was to enhance port protection, security and infrastructure and serve as a national model.

Port security/cargo security has since metastasized into intermodal security that begins with overseas container stuffing to break-bulk distribution at U.S. warehouses. It is perhaps the most complex homeland security prevention and protection issue, with international, intergovernmental and interagency, public-private dimensions. The mission boundaries have expanded to infinity. Everybody agrees that more has to be done, but nobody agrees on who should pay or how to share costs.

According to one former senior HSC official, the failure of DHS or some form of interagency NSC/HSC/NEC-led process to drive successful national cargo security strategy development lay in the rank immaturity of the department and homeland security policy development processes generally.

Observes Randall Yim who, as Director of the Homeland Security Institute, managed Admiral Loy’s national cargo security strategy development:

---

<sup>37</sup> Randall Yim, *Draft Case Study for the PNSR on the Development of the National Cargo Security Strategy*, p. 23.

A critical task will be assuring that the various benefits of security, speed and efficiency align more directly with those asked to pay. This task inherently involves interagency coordination and cooperation. A difficulty has been identifying and designating an entity or office with sufficient authority (both political clout and budgetary persuasion) to make and enforce decisions between and among the competing interests and agency perspectives, particularly when the “outrage” factor causes agencies to become more risk averse or because of “self-preservation” instincts desire to spread “risk” by deferring critical decisions to other involved entities. The issue is not merely stating and understanding that interagency coordination is critical; someone or some entity must be empowered to make it happen. Otherwise, necessary coordination is slotted into the “too hard to do”; “too many moving parts”, or “somebody else’s responsibility” categories.<sup>38</sup>

## **B. Planning**

**Uneven Institution of Integrated Planning:** In part because current national security and homeland security policy has not been developed with formal, systematic and up-front input from domestic non-federal partners, the Federal government has not been able to institute in the steady-state preparedness environment fully integrated planning at any governmental level.

Moreover, implementation of integrated planning has been uneven across the homeland security missions of prevention, protection/mitigation, response and recovery.

**Relative Success for Prevention and Protection:** Credible interagency and intergovernmental planning has been successful in the prevention and protection mission space, largely due to military planning expertise. Pentagon officials say with respect to these missions DoD access to the HSC has been direct and has led to actions getting done. From the DoD prevention and protection perspectives, development at the Principals Committee level has been successful for the pandemic, maritime, aviation and chemical/biological/radiological/nuclear/explosive (CBRNE) strategies. The national strategy for a pandemic—with the above-cited process flaw identified by the GAO—was completed in 2005. National strategies for maritime and aviation security were completed in 2005 and 2007 respectively and have signed presidential directives; supporting plans are being implemented. For CBRNE, the chop is finished with work completing on the sourcing solutions. Development is currently underway on the comprehensive border security policy which will determine the strategy and five supporting plans.

The aviation strategy development, led by the Federal Aviation Administration (FAA), presented a particular intergovernmental challenge. The national strategy for aviation security has seven supporting plans. While the majority of the responsibilities are Federal, the plans require local implementation. The comment phase for discussion of the air defense identification zone (ADIZ) for the National Capital Region (NCR) generated 40,000 state and local comments in the *Federal Register*. Each had to be

---

<sup>38</sup> *Ibid.*, p. 4.

adjudicated. While this ADIZ example was an exceptional case, its development illustrates the practical challenge of building an intergovernmental consensus around a strategy and supporting plans.

**Shortcomings for Response and Recovery:** While interagency and intergovernmental mechanisms for the prevention and protection missions appear to be working and capable of resolving issues, integrated planning efforts for the response mission have been less successful.

Planning involves a range of deliberate, critical tasks needed to build and sustain the ability to execute plans. For response and recovery, Federal agencies (DHS, FEMA, DoD, HHS, CDC, etc.) have independent and often competing notions of what those tasks may be. Thus far, no structure or process has fully succeeded in facilitating representatives from all levels of government, the private sector, service organizations and citizens to come together, collaborate and plan. At all levels of government, preparedness/planning remains an ancillary duty for many homeland security professionals—an afterthought, rarely funded for those who do not have a direct emergency management mission.

The interagency process is cumbersome. It is also a top-down process that takes time to clear legal authorities, do the chops and accommodate stakeholder comments—elements which informed the GAO statements cited above.

In December of 2003, the administration released HSPD-8, *National Preparedness*, which introduced the National Preparedness Goal (NPG), now expressed as the National Preparedness “Guidelines.” The NPG is one of three documents, plans and components—i.e., along with the National Incident Management System (NIMS) and the National Response Plan (NRP), not then released and now known as the National Response Framework (NRF). With its 15 National Planning Scenarios, Universal Task List (UTL) and Target Capabilities List (TCL), the NPG constitutes the essential element of what is now called the Integrated Planning System (IPS), today’s national system or approach for emergency preparedness and response.

The HSC, in partnership with DHS, Federal, state and local homeland security agencies, developed the 15 all-hazards National Planning Scenarios for use in national, Federal, state and local homeland security preparedness activities. Collectively their purpose is to depict a broad range of natural and man-made threats and guide homeland security planning efforts at all levels of government as well as those by the private sector and NGOs. Refinement and revision over time are supposed to ensure the scenarios remain accurate, represent the evolving all-hazards threat picture and embody the capabilities necessary to respond to domestic incidents. These scenarios supposedly form the basis for national planning, training, investments and exercises needed to prepare for emergencies of all types. DHS maintains that by design these scenarios are the foundational structure for the development of national preparedness standards from which to measure homeland security capabilities.

However, the Federal strategic plans to support these 15 scenarios only indirectly drive the detailed planning required to identify specific *Federal* capabilities which may be requested by states. In the opinion of CSIS, “The NPS [National Planning Scenarios] were not originally intended to be the foundation of interagency deliberate planning, but rather were designed to be a planning and exercise tool for the Federal, state and local

levels of government. ...Because the NPS were not created at the outset to be the foundation of Federal interagency planning, many argue they do not necessarily reflect the highest risk scenarios and are at best an imperfect starting point for detailed planning and identification of necessary requirements.”<sup>39</sup>

**Failed Integration with State Planning:** Increasingly since 9/11, state emergency managers have done a lot of planning. However, state planning is not comprehensive. State plans infrequently integrate with Federal plans and do not fully engage with all the state-level stakeholders. Moreover, state interaction with local planning is uneven nationwide. According to the National Governors Association (NGA), barely 50 percent of local governments are “significantly” involved in strategic planning.

State and local planning is not usually scenario-based. In fact, in many cases, state and local authorities resist the approach, because they do not accept the assumptions behind a Federal focus limited to the 15 specific scenarios. State and local plans are more often functionally-based to identify common tasks to be performed under all-hazards planning. A second type are capabilities-based plans which evaluate a mix of training, organizations, plans, personnel leadership and management, equipment and facilities to perform generally required response tasks. A more recent approach is a concept called “game planning,” which combines elements of scenario-, functional- and capability-based planning.

As a result, state planning does not fully identify capability gaps and thus does not accurately inform regional or Federal capability requirements for response. Further, no single Federal agency currently has the wherewithal to translate these differing approaches into a comprehensive repository detailing what state and local capabilities exist, where they are found and how they might be used. From the perspective of rural jurisdictions, the Federal government thus does not walk the preparedness talk. They see Federal agencies not really embracing a coordinated interagency and intergovernmental effort and thus reluctant to cooperate.

FEMA had high hopes for its Gap Analysis Tool as a means to address the intergovernmental capabilities disconnect. The Tool rolled out last year with state and local agencies in the hurricane prone states. Regional planners used it to identify asset gaps at the local, state and national levels. The Tool identifies and reviews seven critical areas: debris removal, commodity distribution, evacuation, sheltering, interim housing, medical needs and fuel capacity along evacuation routes.

FEMA’s intent was to continue the rollout nationwide, adapting it for hazards specific to other FEMA regions. However, the Tool failed to translate its application to the regions threatened by the New Madrid Fault, and officials responsible for it concede that it is not yet ready for nationwide all-hazards applications. In addition, some state emergency managers are resistant, given the time and paperwork demands of the gap analysis process. This failure begs the question whether this and other Federal-level planning efforts will resolve the intergovernmental planning disconnect as they mature, or whether this disconnect is evidence of a problem requiring a structural solution.

---

<sup>39</sup> CSIS, p. 48.

Despite seven years of effort since 9/11, no mechanism currently exists to integrate mutually reinforcing comprehensive plans at the local, state and Federal levels into a credible *national* response plan.

**Ignoring Local Planning Efforts:** At the local level, authorities, particularly those in rural areas of the country, are looking to intra- and inter-state regional collaboration where participating jurisdictions understand that individually they do not have the resources for preparedness. Such localities are attempting to forge regional planning approaches to deal with threats, hazards and common concerns on the basis of what will work and/or has the potential to work.

However, Federal agencies are not currently serving to facilitate coordination at the local level. Despite supporting language, Federal programs do not sustain the development, testing/exercising, evaluation and maintenance stages of such regional efforts. Regional initiatives have suffered under the changing political circumstances which appear to local authorities to be prompting Federal officials to undercut their own programs and relapse into stovepiped business-as-usual attitudes. The result is a lack of continuity, an inability to systematize processes and program failure.

From this local perspective, current Federal policy thus does not address the real capability requirements of localities and their need to align with regional initiatives in a realistic manner to create and maintain capabilities for planning, preparedness and response. As such, local efforts for regional coordination are not able to mature into organizational models when state and particularly Federal agencies get involved.

Post-9/11, the Federal homeland security funding stream flowed forcefully to the state and local authorities in a manner which was more scatter-gun than systematic. While local jurisdictions recognized some positive accomplishments, they also observed a great deal of waste from which no benefits were achieved. Now the Federal funding stream is evaporating, and these jurisdictions see the DHS drive to institute additional NIMS criteria and restrictive compliance dates as attempts to place mandates.

The Federal government may not be able to require state or local agencies to use NIMS, but it does require NIMS compliance for jurisdictions to get Federal reimbursement for expenses and losses and homeland security grants. Local authorities sign annual NIMS compliance letters for submission to state emergency management agencies which act as agents for DHS to audit compliance—another Federally induced stressor on state-local relationships. Local authorities budget to meet compliance criteria by certain dates. However, the FEMA NIMS Integration Center (NIC) continues to add new criteria for NIMS compliance. Even for those jurisdictions which choose not to apply grant funds to NIMS compliance, these new criteria translate to additional costs. For the local budget officers, NIMS compliance hence reads as an unfunded mandate.

**Federal Non-participation in Exercises:** Despite the FEMA language, the agency can demonstrate no follow-through. The effect on the state and local partners is most obvious in the various exercise programs, where the Federal agencies have been under-engaged. DHS doesn't fund exercises sufficiently, and Federal agencies do not fully participate in them. They see exercises tying up staff, incurring costs which must come from operational accounts and negatively affecting execution of routine responsibilities. Federal agencies do not have line-item funding "fenced" for exercise

participation with states and locals. Nor do they have set-aside monies for NIMS training.

States and localities have used and are using Urban Area Security Initiative (UASI) grant money for NIMS training, and local agencies find they have to drain monies from their operations accounts to fund non-routine drills. Because the Federal agencies have no requirement to participate in exercises, state and local personnel have to “play Feds” during an exercise with the result that Federal/state/local relationships and an intergovernmental NIMS culture fails to form.

State and local authorities view Federal non-participation as evidence of a lack of leadership. According to one rural emergency management coordinator, “On the surface they would want you to believe we are all one big happy family. Behind the scenes there is an environment of non-cooperation....This disconnect may be due to past policies and or difference in interpretation. From my perspective, the disconnect appears to be by design, geared to self-preservation, turf issues, rather than comprehensive service and organizational functionality.”

This dysfunction creates the perception that the Federal and state/local authorities are working from two different sets of rules. The draft output of an intergovernmental working group with DHS representation developing policy on law enforcement protection for first responders makes the point. The draft policy which emerged from the group contained no language referring to NIMS or ICS accountability. Not surprisingly, given the DHS representation in the group, this output was for local-level officials yet more evidence that the Federal level was not practicing NIMS as it preached.

#### **Inadequate Planning Compromises Effective Resource Decision-making:**

The inability to integrate Federal scenario-based planning with comprehensive state-level planning has a detrimental effect on resourcing decisions. The Federal-level scenario-based plans are supposed to guide development of the interagency and departmental concept and operational plans to support the 15 scenarios. Absent corresponding, comprehensive state plans, Federal agencies have been generally estimating shortfalls—or unavailabilities as the case may be—in state capacities. Such planning estimations fail to make any logical assessment of actual capability requirements which vary from state to state. Instead, planning takes a “worst case in worst place” approach which not only magnifies a perceived problem but reinforces the drive to a Federal response solution which is unaffordable and which no level of government actually wants.

In its December 2007 release of HSPD-8 Annex 1, HSC made a requirement for a DHS-led Integrated Planning System (IPS) for homeland security. IPS is building on a number of interagency planning efforts. DHS says it has completed the IPS vetting process, and the system is almost ready for approval. The question remains whether better leadership or resourcing would have improved process, or whether integrated planning requires a structural solution.

The responsibility to implement strategic-level interagency planning is in the DHS Office of Operations Coordination (OPS), which leads the IPS effort and also oversees the National Operations Center (NOC). Resident in OPS is a interagency planning capability in the Interagency Management Planning Team (IMPT) which has a core of 15 planners and 38 on-call staff. The IMPT has a “shared planning culture” which is building upon the Interagency Incident Management Group (IIMG) and other

interagency efforts. Interagency coordination has been positive, and attendance has been good. The team is adjudicating 800-900 comments on the IPS and is currently working the 15 National Planning Scenarios. HSPD-8 Annex 1 has standardized the interagency planning process, and to date some 500 Federal-level planners have been trained.

According to June testimony by Wayne Parent, OPS deputy director, the Federal Partnership Guides are supposed to put meat on the NRF but are not done yet, although DHS has them in draft and does have a hurricane concept of operations (CONOPS). The strategic guidance statements and strategic plans for the 15 National Planning Scenarios are in draft and are 95 percent completed. DHS is waiting for approval of the IPS, after which the guidance and CONOPS are supposed to flow rapidly.

Despite this hopeful report, in terms of response, the interagency national/homeland security process is not working as it should. In terms of ESF coordination, FEMA is not sufficiently weighted to serve as the single Federal entity to compel other Federal departments and agencies for emergency management coordination. The agency appears to be unable to get cabinet-level leadership to comply fully with their individual departments' ESF responsibilities. Intergovernmentally, the IPS process does not allow the right engagement with the state and local authorities, the private sector and NGOs to manage all-hazards risks.

FEMA and NORTHCOM have a most serious planning disconnect that so far has prevented translation of state capability gaps into DoD civil support capability requirements. This spring, the Punaro Commission on the National Guard and Reserves issued its final report to Congress. Recommendation 5 read as follows:

In accordance with Section 1815 of the 2008 National Defense Authorization Act, the Secretary of Homeland Security, with the assistance of the Secretary of Defense, should generate civil support requirements, which the Department of Defense will be responsible for validating as appropriate. DoD should include civil support requirements in its programming and budgeting. As part of this effort, DoD should determine existing capabilities from all components that could fulfill civil support requirements and rebalance them where appropriate (consistent with their other obligations), shifting capabilities determined to be required for state-controlled response to domestic emergencies to the National Guard, and shifting capabilities currently resident in the National Guard that are not required for its state missions but are required for its federal missions either to the federal reserve components or to the active duty military, as appropriate.<sup>40</sup>

On the DoD side, NORTHCOM has some achieved some concepts of operations, including CONOPS for CBRNE consequence management (CBRNE CM) and defense support to civil authorities (DSCA) for the 15 National Planning Scenarios. However, one Pentagon official with well over a decade's experience in DSCA-type relationships is skeptical of their worth. In his view, while DoD may say it is able to execute Concept Plan 3501 (CONPLAN 3501, NORTHCOM's DSCA plan), he is assured that

---

<sup>40</sup> Commission on the National Guard and Reserves *Transforming the National Guard and Reserves into a 21<sup>st</sup>-Century Operational Force*, January 31, 2008, p. 107.

NORTHCOM lacks sufficient knowledge of the ESF structure. In reality, he says, NORTHCOM won't be able to execute CONPLAN 3501. In other words, at an operational level DoD will not know how to plug into a state or local ICS structure.

*Implementation of comprehensive national security and homeland security planning at the state and local levels is uneven.*

### **C. Resourcing via a Fragmented Grant Structure:**

Grants generally—and grants specifically for administration of programs—are at the core of Federal/state/local homeland security relationships.

In the abstract, the Federal government has no definitive measurement system for assessing effectiveness of its homeland security grants system. Departments and agencies responsible for homeland security grant programs have trouble identifying outcomes, and thus the risks to which they apply grants. DHS has no effective mechanism to track the performance based on agreed outcomes, which in any event are established at the Federal level with little state and local input. As such, grant programs do not have clear management objectives for their investment portfolios.

Structurally, the homeland security grant program is fragmented across some eleven different executive branch departments. DHS administers its Homeland Security Grant Program among other grant programs in the FEMA portfolio; however, HHS, Justice and the departments of Agriculture and Transportation are responsible for an additional 15 grant programs directly related to homeland security, which combined, distribute more funds to state and local governments than does DHS. Some grant programs, such as the Stafford grants, pre-date 9/11.

Grants to state and local authorities are one of three types: project grants for specific programs, block grants and categorical grants. Block grants allow states to develop programs and policies based on local needs rather than a one-size-fits-all Federal perspective. Categorical grants impose conditions on state and local compliance and rate performance on behaviors. Frequently these type grants require jurisdictions to match funding from the Federal government. This approach is a form of indirect taxation and has the effect of holding the state hostage to programs that may transmute into an unfunded mandate if the grant resource streams run dry.

The pre-9/11 FEMA and HHS legacy grants are project grants. These grants are extensions of programs that span national interest that meet evolving national needs, e.g., national flood insurance and national immunization, disease tracking and treatment programs. Over time, the Federal and state authorities have established relationships, resolved and put in place administrative procedures, made sub-national legislative arrangements and arrived at a resource equilibrium that has proved to be manageable and acceptable by all parties.

Project grants can roll into block grants that, from the states' perspective, are better for meeting needs and determining risks at the sub-national level. Block grants are best performing when effectiveness is measured. Where block grants perform poorly is when OMB's contentious Performance Assessment Rating Tool (PART) evaluation system is being used by the CBO and DHS to evaluate programs. PART measures outputs and not outcomes. Categorical grants are the least effective because of the

overpowering administrative requirements that consume the funding and divert resources from meeting the proposed outcomes of the program. Another reason for the low ratings for block grants lies in the fact that the PART ratings are obtained from a grant performance assessment tool designed around categorical grants. Although notwithstanding the results from faulty application of this metric, one block grant program, the 1996 HHS Temporary Assistance to Needy Families (TANF) program, is universally regarded as the best performing grant program.

Congress, the CBO and OMB put pressure on Federal grant administrators to ensure accountability which drives an impetus toward categorical as opposed to block grants. Most of the conditions in a categorical grant require behaviors from state and local entities which were not present before the Federal grant was offered. For jurisdictions to receive the money, they must comply with the conditions of the grant, e.g., state and local strategies, spending plans, resource allocation plans, etc.

The most troublesome imposed conditions could be in the grant program supporting the otherwise commendable National Incident Management System (NIMS). Notwithstanding the merits of NIMS itself, the national totals for even the most elementary efforts at NIMS compliance exceed state and local authorities' available own-source revenues by billions of dollars. Whereas NIMS seems to be accepted in theory by most state administering agencies (SAAs), they are professional people—not elected—who are eager to get funds to support their individual programs. The decision is simple. Comply to get the funds, or don't comply and get nothing.

Compliance requirements compound a state's problem. When state and local authorities apply for homeland security grants, they have to meet required conditions, whether it's NIMS compliance or homeland security planning requirements. Once they become dependent on Federal funding, compliance is the only political option. Since many of the programs receive grant funding for a limited time, or are under-funded from the beginning, they morph into a financial burden—unfunded mandates. Homeland security grant programs actually provide so little funding that the impact on state and local budgets is minimal.

The legislative and executive branches' insistence on fiduciary accountability through stringent compliance measures and reporting requirements yields an unintended consequence. State and local authorities lacking the administrative capacity, tax base and revenue streams are opting out of the homeland security grant system. "The current homeland security grant program is narrowly focused, preempts state and local prerogatives, is insensitive to the operational activities of state and local governments, and has associated costs which further limit distribution of funds to communities."<sup>41</sup>

Facing ever-tightening budgets, state and local elected officials will resource their conventional emergency management and public safety organizations to respond to the routine events, as opposed to the unconventional, homeland security events out of the norm. "There is little evidence to support the idea that citizens want more 'homeland security,' particularly if they have to pay extra for it."<sup>42</sup>

---

<sup>41</sup> Samuel H. Clovis, Jr. "Federalism, Homeland Security and National Preparedness: A Case Study in the Development of Public Policy" *Homeland Security Affairs*, Vol. II, No. 3, October 2006, p. 13, <http://hsaj.org/?fullarticle=2,3,4>, (accessed 5/28/2008)

<sup>42</sup> *Ibid.*, p. 14.

It is in the nature of homeland security: officials get few rewards for preventing attacks and hear the recurring argument that money is more urgently needed elsewhere, while complacency continues to build over time. Some states, like Florida, Iowa and Virginia—three of the leading emergency management states—are struggling over ways to comply and fit NIMS into their models of emergency management and public safety. However, these forward leaning states still must work around resistance at the local level from general managers—city and county managers, budget directors, i.e., those with broader responsibilities—who are not seeing any value added in complying with a program like NIMS.

Other states, like Ohio, Texas, Colorado, Arizona and Minnesota, will go along only if no costs are imposed and the programs can be molded to state and local needs. Some states simply do not “come up on the net.” They may submit their strategies and reports as required, but these activities may be pencil games to get the money and nothing more. As such, a number of states along with virtually all of the urban jurisdictions beyond the Urban Area Security Initiative (UASI) cities have opted not to engage fully in NIMS development or compliance. Thus, disengagement is an unintended consequence of the Congressional and DHS quest for accountability through stringent compliance measures and reporting requirements.

Non-compliant jurisdictions tend to build their capabilities around a steady-state functionality reflecting the preferences of constituents to which the elected officials respond. In a time of crisis, they will assume support will come from other jurisdictions with temporary excess capacity that will only be available for a limited period. Given these types of practical trade-off decisions at the local and state levels, the Federal government is not really in the best position for evaluating performance for states and localities that are attempting to comply with program requirements—certainly not to the degree the state and local jurisdictions can assess themselves.

As a result, the cross-cutting requirements and the regulatory compliance reporting required for receiving funds are inducing states to withdraw from programs. In 2003, when funding began to stabilize, local governments increasingly stopped applying for homeland security grant funding, because they could not overcome the transaction and opportunity costs involved in seeking grants. Today, only a few jurisdictions in each state actually apply for funding. The 80 percent pass-through required of the states is not fully embraced by state administrators. The administration requirements imposed by the Federal government force state administrators to “take” more of the money—a typical behavior when categorical grants are in play. Asking voters to support an increase to state taxes for homeland security preparedness is not an option. All studies have shown that states will not raise state taxes to increase revenue except perhaps for the most directly and demonstrably beneficial purposes.

Any executive branch failure at interagency coordination of the homeland security grant programs is exacerbated by congressional oversight via the committee structure enables additional fragmentation. With its multiple, overlapping committee structure with oversight of homeland security, Congress provides more oversight to DHS than to any other department, and not surprisingly lawmakers have used grants as vehicles for pork-barrel spending. Nevertheless, homeland security grant funding has steadily declined for every year following an initial surge prompted by 9/11. “Unfortunately, the homeland security grant funding represents more ‘talking the talk’ than ‘walking the

walk.’ Although homeland security seems to be on the tongue of every representative, less than one percent of the total redistribution of funds to state and local governments is found in homeland security grants.”<sup>43</sup> At best, state-level grant management has to account for uneven funding streams; at worst, states find the streams declining and themselves left with unfunded mandates.

Considerable ill-informed attention has gone to the grant formula process that focused on “big state-little state” issues, particularly in the Senate. Small population states, or rather those with a homogeneous electorate, tend to return senators with longevity whose seniority gives them more power in committees and the ability to influence where others cannot.

The UASI (focused on large, densely populated urban areas) grants have helped balance the scales. The UASI grants are based on risk calculations rather than a revenue sharing formula. The per capita distribution moves nicely toward large population states with this simple adjustment in formula.

The amount of money involved in the grant program is not much in terms of state budgets. Homeland security grant funding actually totals less than 0.3 percent of the overall operating revenue of state and local governments.

As indicated above, the interface with states in the grants program is at the core of intergovernmental relationships. Who pays for what and what strings should be attached? At the state level, the state oversight of emergency management programs and grants is highly uneven. For a start, state governmental structures are not the same. States have their own constitutions. They are internally sovereign and have thus variously organized themselves. In so-called home-rule states, a third level of shared sovereign governance of the same people in the same territory exists at the municipal level. The U.S. Census Bureau puts the number of general-purpose jurisdictions in the U.S. at 39,000.

Notwithstanding the detrimental effect of the Federal-level fragmentation of the homeland security grant programs on state and local authorities, states and localities have their own reasons for highly uneven management of grants and emergency management .

The vast majority of state budget cycles are not in sync with the Federal fiscal year which runs from 1 October to 30 September. In 41 out of 50 States, the fiscal year runs from 1 July to 30 June. Of the remaining, only one or two states are aligned with Federal fiscal year, while the others have yet different budget cycles. In a very few instances—involving either home rule states or states with large metropolitan areas—city budget cycles do not align with that of the state. These kinds of disconnects mean that a state may not be able to allocate its Federal grant money until its following fiscal year budget cycle. This leaves the state or locality the dilemma of having to project spending requirements based on highly uncertain federal budget processes. These disconnects can create bookkeeping solutions and frustration for the Federal grant administrators and their congressional, CBO and OMB administrators. Federal grant mechanisms fail to take any of these considerations into account.

State and local authorities without the tax base and revenue streams to support full-time homeland security or emergency management staff are opting out of the homeland security grant system. Poorer states tend to have below-par accounting mechanisms which compound the accounting problems, and many states generally lack a

---

<sup>43</sup> *Ibid.*, p. 10.

structural capability in their emergency management agencies, due to lack of state funding, administrative capacity and turnover in the workforce. To sustain their emergency management capability and capacity, these states may be dependent on FEMA Emergency Management Performance Grants (EMPG) program to fund emergency management personnel. To what degree is the Federal government responsible for supporting and enhancing state and local capability and capacity? The problem may be in the nature of federalism itself.

*Homeland security grant mechanisms work against collaboration, fragment state and local planning and reinforce Federal stovepipes.*

#### **D. Operational Execution—The Structural Performance of the Katrina Response:**

**Degraded FEMA Capacity:** When the Bush administration arrived in Washington in 2001, its first two FEMA administrators effectively presided over the dismantling of the FEMA capacity they inherited from James Lee Witt. Many experienced senior emergency management officials left the agency; vacancies were not filled; funding was reduced; and morale plummeted.

The post-9/11 FEMA absorption into the newly created DHS put an agency whose primary mission was to provide states with support for disaster response/recovery into a department whose legacy agencies were now focusing on counterterrorism in addition to their previous mission sets. Additionally, FEMA's preparedness function moved to other entities in the DHS structure. "The loss of the preparedness function limited FEMA's ability to influence state preparation and weakened relationships with state responders...Reduced resources also directly impacted FEMA's ability to build relationships through planning efforts."<sup>44</sup>

**The National Response Plan (NRP)—the New Framework for Response:** The shock of the 9/11 attacks prompted the administration to revise FEMA's Federal Response Plan (FRP). In February 2003, a month before DHS was officially established, the White House released HSPD-5, *Management of Domestic Incidents*, which called for implementation of the ICS-based National Incident Management System (NIMS) to establish standardized training, organization and communications procedures for multi-jurisdictional interaction and identify authority and leadership responsibilities. In December of 2003, it issued HSPD-8, *National Preparedness*, which introduced the National Preparedness Goal (NPG), today expressed as the National Preparedness "Guidelines." As previously discussed, the NPG was one of three documents, plans and components, i.e., along with NIMS and a National Response Plan (NRP)—not then released—which together constituted the essential elements of what was then called the National Planning System (NPS), a national system or approach for emergency preparedness and response.

In January 2005, DHS released the NRP, its framework for a comprehensive, all-hazards approach to domestic incident management. With NIMS as its doctrinal basis,

---

<sup>44</sup> Donald P. Moynihan *From Forest Fires to Hurricane Katrina: Case Studies of Incident Command Systems*, IBM Center for The Business of Government, 2007, p. 32.

the NRP—itsself a doctrinal statement for planning—also attempted to provide a means for private and non-profit institutions to plan and integrate their own preparedness and response activities.

The NRP maintained the FRP’s formalization of Federal response via 12 Emergency Support Functions (ESFs) which assigned lead and supporting agencies by function. In 1995, a Clinton-era modification to the FRP briefly summarized the organizational role of the military in a Federal response environment. Another revision in 1997 added a Terrorism Incident Annex to the FRP to implement PDD-39, *The U.S. Policy on Counterterrorism*. The FRP, thus, had been the first “plan” to coordinate the government response to natural, accidental or terrorist disasters, emergency situations or other incidents requiring Federal assistance under the 1988 Stafford Act. It described the basic mechanisms and structures through which the Federal government mobilizes the resources and conducts activities to augment state and local response efforts. The FRP both facilitated the provisions of Federal assistance and used the 12 ESFs as its functional approach to group the types of assistance that a state was most likely to need. Under the NRP/NIMS construct, in an event a local or state authority is to replicate the ESF structure in its emergency operations center (EOC) and its on-site incident command in the operations section into which Federal support plugs.

The post-9/11 NRP updated the FRP with revisions designed to incorporate more of a law enforcement component in view of the presumed threat of further domestic terrorist incidents. These events would require a national response whose operations were both consequence management, the traditional FEMA and emergency management role, and crisis management, an FBI and law enforcement responsibility. Notwithstanding the all-hazards language maintained in the NRP, the predisposition behind its crafting reflected the immediate post-9/11 “sense-making” toward preparedness for terrorist incidents vice natural disasters.

The response to Hurricane Katrina was the NRP’s first major test, and it exposed a number of implementation and design flaws.

**NRP Implementation:** DHS began the NRP implementation process in December 2004 and announced April 14, 2005, as the date for implementation at the Federal, state and local levels—four months prior to Katrina. However, during the post-Katrina hearings, Gil Jamieson, the FEMA director of the NRP implementation body, the NIMS Integration Center (NIC), spoke of a DHS strategy for a multi-year, phased implementation to avoid getting a “knee-jerk reaction to a very hard-hitting federal mandate.”<sup>45</sup>

The NRP was not a self-executing document. In fact, certification could come via self-administered on-line training. The April 2005 TOPOFF 3 “was the first national preparedness exercise that used the NRP and NIMS as the framework for the incident response and management.”<sup>46</sup> The exercise revealed to DHS widespread unfamiliarity

---

<sup>45</sup> U.S. Senate Committee on Homeland Security and Governmental Affairs *Hurricane Katrina: A Nation Still Unprepared*, Chapter 27 “Failures in National Response Plan: Unified Command”, Washington, DC: Government Printing Office, 2006, pp 551-574, p. 560.

<sup>46</sup> *Ibid.*

and a fundamental lack of understanding of the principles and protocols of unified command, the NRP and NIMS—at all three governmental levels. Notwithstanding this knowledge, FEMA continued to implement the NRP without any planning to support it.

According to the FEMA Federal coordinating officers in both Louisiana and Mississippi, DHS failed to approve funding requests for training and exercises for NIMS-ICS which contributed to staff deficiencies in both states' unified commands.

“The NRP is a high-level plan....not designed to address specific scenarios or geographic areas, or to provide operational details.”<sup>47</sup> Under the FRP, FEMA had developed regional plans tailor-able for states. Because no such plans yet existed for the NRP, it was implemented without any planning to support it.

On the basis of these above reasons alone, NRP implementation was thus manifestly inadequate.

**NRP Design:** Coast Guard VADM Thad Allen, who served as the second principal Federal official (PFO) for the response, told Congress that the NRP as written “doesn’t contemplate” a catastrophe on scale of Katrina (Senate Report, p. 554). It had a number of structural flaws, of which principally two contributed to a lack of clarity among the Federal command and coordination relationships that proved confusing for officials in the field.

First, with respect to the delegation of Federal authority in the field to support state response/recovery, the introduction of the PFO position and the NRP’s definition of PFO authorities complicated unified command and reporting relationships in the state-level Joint Field Offices (JFOs), the Federal/state interface to support incident management. The PFO position was created by HSPD-5 and introduced in the 2003 Top Officials 2 (TOPOFF 2) national counterterrorism exercise. As defined by the NRP, the PFO is designated by the DHS Secretary for an incident requiring extraordinary coordination to promote Federal collaboration in the on-scene unified command structure managing the response and provide the DHS Secretary with situational awareness. However, the PFO is not supposed to have directive authority over the senior FEMA, Federal law enforcement or military officials on site for the incident.

Promoting Federal agency collaboration is not the same thing as having operational authority to “lead” the Federal response, although that has been the perception. This ascription of a PFO leadership role has led to confusion with respect to the traditional roles and responsibilities of the Federal Coordinating Officer (FCO). That position originated in the 1969 Disaster Relief Act which in part had been a previous attempt to formalize coordination of Federal response during a major incident. The FRP had provided for the FCO to be a FEMA official, but like the PFO, the FCO had no operational authority under the NRP. Yet, under the Stafford Act, the FCO could have statutory authority on behalf of President when recorded in *Federal Register* as part of the disaster declaration. The NRP, however, put the PFO, a non-statutory position, in the DHS chain, i.e., independent of the FCO chain via FEMA. The distinction between roles and responsibilities of the two was thus unclear, as had been discovered in the April 2005 TOPOFF 3 exercise.

In the Katrina response, DHS Secretary Chertoff appointed FEMA Administrator Michael Brown as the PFO on August 30, one day after landfall and the day he declared

---

<sup>47</sup> *Ibid.*, p. 554.

the hurricane an Incident of National Significance. Aside from his lack of operational emergency management experience, the appointment removed Brown from his headquarters, degrading his effectiveness as a presidential advisor and his authority over FEMA ESF coordination at the Federal-level and potentially preventing him from effectively leading his agency in the event of simultaneous disaster(s). As FEMA administrator, Brown did have direct authority to oversee the three FCOs operating in each of the three states in the region, Louisiana, Mississippi and Alabama. However, Admiral Allen, who relieved Brown on September 9 as PFO, had no such authority. As a work-around Allen was dual-hatted as FCO on September 21 in each of the three affected states, relieving the three FCOs, who correspondingly became deputy FCOs.

In the case of Mississippi, Allen had been perceived not to have paid any attention to the response issues in that state until he became the FCO. The dual-hatting presented a new problem since Allen as an FCO in three states could not simultaneously co-locate in the joint field office (JFO) in each of the three states as provided by the NRP. This ad hoc arrangement raised the question in each state as to who was the primary holder of FCO legal authority under ICS principles and thus compromised clear unity of command in each JFO.

The NRF has not fully resolved the unclear authorities in the PFO/FCO relationship which compromises effective management of a coordinated Federal response in a multi-state catastrophic disaster. The confusion prompted the Florida Emergency Management Agency to name Governor Jeb Bush as the incident commander during Hurricane Wilma which followed Katrina in October 2005, so as to preempt a Federal appointment of a PFO to exercise Federal authority in the response.

The confusion over the reporting lines and unclear command relationships of the PFO and FCOs back to Washington to the DHS Secretary and FEMA Administrator was reminiscent of the confusion over Federal management of the response to the 2001 anthrax attacks which the creation of DHS was supposed to prevent.

Second, each Emergency Support Function (ESF) annex to the NRP assigned to its function an ESF coordinator, a department/agency for management oversight of the ESF under a unified command approach, and an ESF primary agency, one which has significant authorities, roles, resources or capabilities for a particular function with the ESF. The NRP added three ESF functions to the original 12 in the FRP ESF annexes: ESF-13 Public Safety and Security, ESF-14 Long-Term Community Recovery and Mitigation and ESF-15 External Affairs. As such, these annexes provided ESF structures unfamiliar to the homeland security community at all three governmental levels.

Under the NRP ESF-13, Justice shared its ESF coordinator and primary agency duties with DHS. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) led ESF-13 Public Safety and Security coordination. The DHS counterpart was the assistant director of Immigration and Customs Enforcement (ICE), who later admitted to having only a “fleeting familiarity” with the NRP.

With respect to ESF-15 External Affairs, DHS did not establish its Federal Joint Information Center (JIC) until September 6—over a week after Hurricane Katrina made landfall. This failure to coordinate messages to the media left news presenters with no guidance. As such, their messages may have worked against the evacuation of New Orleans. The most notorious example was a reckless statement in the August 29 morning exchange between Matt Lauer and Brian Williams on the *NBC Today Show* that “New

Orleans dodged the big bullet,” which gave the impression to city residents that the threat to their safety had passed, when the actual catastrophe came with the failure of the levee system and consequent flooding of the city.

Confusion over shared ESF coordination surfaced in pre-existing ESFs as well. ESF-6 Mass Care in the FRP had assigned the American Red Cross (ARC) as the primary agency. Under the NRP it became Mass Care, Housing and Human Services with the ARC the primary agency and FEMA the ESF coordinator and co-primary agency for Housing and Human Services.

Under the FRP, ESF-9 was Search and Rescue, and the primary agency was FEMA. Under the NRP, ESF-9 became Urban Search and Rescue with FEMA the ESF coordinator and primary agency. This change resulted in confusion for agencies with waterborne search and rescue capabilities, notably the Department of Interior’s National Park Service waterborne assets which could have been employed in the response.

In January 2008, FEMA issued the National Response Framework (NRF) which officially replaced the NRP in March. Lessons learned from the Katrina response informed many of the revisions. Key modifications to the ESF structure have clarified authorities. While the role of the SFLEO is essentially the same under NRF, Justice is now the sole ESF-13 coordinator and primary agency. Under the NRF, ESF-14 is now Long-Term Community Recovery. FEMA remains the ESF coordinator. The primary agencies are the Department of Agriculture, DHS, Housing and Urban Development (HUD) and the Small Business Administration (SBA). Under ESF-15 DHS served and continues to serve as the ESF coordinator with FEMA as the primary agency. Under the NRF, ESF-6 is now Mass Care, Emergency Assistance, Housing and Human Services with FEMA as the ESF coordinator and primary agency. Related to ESF-8 Public Health and Medical Services, because FEMA and HHS did not fully coordinate prepositioning and deployment of the National Disaster Medical System (NDMS) Disaster Management Assistance Teams (DMATs) during the Katrina response, NDMS transferred from FEMA to its original home, HHS, the ESF-8 coordinator and primary agency. The NRF has returned to ESF-9 the title Search and Rescue and designating FEMA as the ESF coordinator and FEMA, the Coast Guard, National Park Service and DoD as the primary agencies.

**NRP Execution:** At the Federal level, DHS and FEMA did not to respond under the provisions of NRP’s Catastrophic Incident Annex (CIA) and Catastrophic Incident Supplement (CIS) for extreme disasters.

The CIA essentially provided the principles for a proactive Federal response, turning a “pull” system into a “push” system for deployment of resources to mobilization centers. The CIA authorized Federal agencies to “take immediate actions to protect life, property, and critical infrastructure under their jurisdiction, and provide assistance within the affected area.”<sup>48</sup> The CIS provides the operational details, and its Execution Schedule serves as an acceleration model for resources which the NRP had already identified. The CIS is the basis for the capabilities-based planning effort and time-phased deployment schedule that is in place. The Pre-Scripted Mission Assignments correspond to standard recommended packages and their costs which provide the president with a basis upon

---

<sup>48</sup> *Ibid.*, p. 557.

which to decide whether to order the packages sent and OMB to find the money to pay for it.

A catastrophic event as defined by the NRP is “a natural or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.”<sup>49</sup> Under the NRP, the DHS Secretary or his/her designee could initiate CIA implementation. Under the NRF, the Secretary still has the authority, though it is more of an evolutionary process than an on/off switch.

The CIA was not activated for the Katrina response. Administration officials during the Katrina hearings told lawmakers that the annex was for use only in no-notice events. No such language appeared in the CIA, however. The still-to-be-cleared CIS says the provisions were for no-notice and short-notice events. GAO testimony held that the CIA “should be supported and supplemented by more detailed and robust operational implementation plans.”<sup>50</sup>

As for the CIS, it had not been issued by Katrina. DoD withheld approval owing to its objection to the provisions for reimbursement of costs. A Pentagon official this spring told the PNSR State/Local Issue Team that DoD and other departments and agencies are now comfortable with the CIA. However, while most of the other departments and agencies have signed off, DoD still has reservations. The Pentagon regards the CIS as too top-down with “no assessments.” The issue for DoD is no longer the reimbursement provisions, but rather “as currently written [the CIS] is logistically unattainable.” DoD wants the wording in the CIS to reflect Pentagon agreement to prepare support packages, but send only “what is required.” William Carwile, the Mississippi FCO during Katrina, has questioned whether the CIS has sufficiently incorporated a robust, catastrophe-focused planning.

As for the execution of the NRP in Katrina, one former senior DHS official relayed to State/Local Issue Team his opinion that “the NRP (and CIA) was not trained, tested or validated, yet it was the plan in place.... Depending on whom you asked on what day and in which executive branch department, you got vastly different answers pointing to a lack of shared understanding of the NRP.”

The CIA was not activated for the Katrina response, and neither was the CIS fully approved for issuing. In view of the foregoing, it would thus appear that the Federal reaction to Katrina was a “sense-making” issue: DHS did not initially see the hurricane on the same scale as a catastrophic terrorist incident, which the Annex was intended to address.

As for failures of execution at the state and local levels, the assessment must account for performance differences in Louisiana and Mississippi.

In Louisiana, the storm and flooding decimated emergency management capacity. Mississippi’s Carwile observed sympathetically, “In a situation, a catastrophic disaster, it is very difficult to build from the bottom up if there is no bottom.”<sup>51</sup> The Senate Report

---

<sup>49</sup> *Ibid.*

<sup>50</sup> *Ibid.*, p. 554.

<sup>51</sup> *Ibid.*, p. 562.

identified as the “real problem” Louisiana’s emergency managers’ unfamiliarity with the NRP and NIMS.<sup>52</sup> (Important to note: The Louisiana EOC in fact had been staffed by trained National Guardsmen who were unavailable due to their deployment overseas in Iraq.) The situation was not helped by FEMA’s incident action plan (IAP) planners not getting to the Louisiana EOC until after landfall. As for the Louisiana JFO, it was not operational until 12 days after Katrina came ashore. In essence, the Federal response had no capacity in Louisiana to support. The same was true for the 500 volunteer organizations which responded. The fundamental problem was the failure to establish unified command in Louisiana and New Orleans, meaning that the governor and the mayor never had more than partial control of the response.

In the Katrina response, Justice was not able to assign a SFLEO in Louisiana until six days after the hurricane’s landfall. The SFLEO was not able to establish an FBI Joint Operations Center (or Secret Service Multiagency Command Center) as defined by the NRP. Instead, he stood up the Law Enforcement Coordination Center (LECC) to address the identified gaps in the law enforcement response unique to New Orleans following Katrina’s coming ashore. Essentially, his decision was in response to the fact that New Orleans had neither exercised nor stood up its EOC into which he could plug his law enforcement support. Among other things, the LECC attempted to coordinate law enforcement efforts and National Guard and active duty DoD operations and provide basic investigative and criminal law enforcement resources until the New Orleans Police Department returned to an operational capability requiring no support.

In Mississippi, NRP execution was quite different. Officials were able to establish a successful ICS two or three days after landfall, despite problems with communications. Federal and state officials successfully implemented unified command. Despite the DHS failure to approve funding requests for training and exercises, Mississippi had provided ICS training for state and local officials. Carwile, the Mississippi FCO, was experienced in hurricane response having been the Florida FCO in 2004 where he had partially implemented NIMS.

Mississippi’s unified command engaged elected officials. In general, unlike a lower-level routine incident that may rise to a level where ICS is required, for complex, multi-jurisdictional events, when elected officials enter the picture, they change the dynamics of authority, particularly with respect to response objectives based on priorities set by the incident commander. In the Mississippi response, incident commanders based their objectives on the priorities of the local officials who understood that incident command was hearing and acting upon their concerns, even given the resource shortages. Carwile observed from his experience in Florida and Mississippi the importance of the governor being in charge of the state response where he delegated his authority to vested emergency managers, i.e., through his authorized representative and the state coordinating officer (SCO) who works with FCO. In the case of Florida, Gov. Jeb Bush vested his SCO with statutory authority to report directly to him.

Notwithstanding FEMA’s degraded response capacity and the flaws in the design, implementation and execution of the NRP at the Federal level, Mississippi’s execution of ICS proved the workability of NIMS in catastrophic disasters on that scale—dependent on the understanding, embrace, training and exercising of ICS principles and procedures at all levels.

---

<sup>52</sup> *Ibid.*

Notwithstanding the enduring perception, the Federal/state/local government response to Katrina was not ad hoc. Rather it conformed to a strategy—albeit a work-in-progress—which was passively implemented and poorly executed.

## VII. CONSEQUENCES:

**OUTCOME:** The core problem strongly suggests that in a catastrophic crisis, coordination efforts will not prevent Federal departments and agencies from relapsing into go-it-alone support strategies which will undermine state- and local-level unified command.

**OUTCOME:** Further, in the short-term, this failure will put pressure on the legislative and executive branches of the Federal government to “federalize” the response in an attempt to appease expectations that are practically and logistically unobtainable. In the longer-term, such a response would be detrimental to shared sovereignty under the Constitution and if deemed to have failed would jeopardize public confidence in constitutional governance.

## VIII. CONVENTIONAL WISDOM

- The leader, not structure, is important. (Comment: Either way, the interagency and intergovernmental dimensions of homeland security require those with responsibility to develop and execute homeland security policy to be schooled thoroughly in network norms.)
- The president only has to insist on compliance, and he will get it. (Comment: To the extent this aspect of presidential leadership is true, it only applies directly to the interagency dimension of homeland security. Presidential insistence can only have its intergovernmental effect *indirectly* by example.)
- Preparedness for routine daily duties for high-probability events takes priority over seemingly low-probability, but high-consequence events which otherwise gets put into the too-hard category. (Comment: In the execution, therefore, structure and process for low-probability, high-consequence events must remain the same as for high-probability events because routine reinforces training and exercising of network norms. Moreover, it is not a given that intergovernmental sovereign stakeholders will unanimously agree an event “triggers” execution of a different structure/process.)

## IX. CONCLUSIONS/FINDINGS

**FINDING 1: The NRF is still in need of Federal-level structural and process improvement.** As indicated by the example of Mississippi’s execution of the Incident Command System (ICS), the State/Local Issue Team thus far generally finds the National Response Framework (NRF)/National Incident Management System (NIMS)/Emergency Support Function (ESF) structure (as exercised, but not yet tested by a catastrophic event)

represents a good model of a temporary hierarchical network for domestic incident management. Iterative improvements have been made since Katrina and will continue.

To this point, the Federal government has not sufficiently incentivized departmental and agency NIMS compliance. It has not meaningfully engaged up-front state and local authorities in the policy development process. Neither has it facilitated full and meaningful engagement of the private sector and NGO communities. The key structural defect which remains in the NRF is the stovepiping of Federal support to the state and local level principally via DHS, DOJ and DoD structures which, despite the language of unity of effort, do not integrate into unified command.

In terms of the response and recovery homeland security missions, states have embraced ICS—if not NIMS—but Federal departments and agencies have not. Federal stovepipes still exist in terms of C<sup>2</sup> and coordination of unity of effort. Federal behaviors impede state and local unified command.

A number of quarters apply these shortcomings to the argument for a Federal solution “for large disasters like a nuclear detonation.” They argue, “The Federal government needs a realistic response plan specific to the Day After scenario that marshals the resources of all agencies.” According to the authors of this scenario<sup>53</sup>, “[t]he Federal government should stop pretending that state and local officials will be able to control the situation on the Day After.” As such, an event of this magnitude requires “a lead Federal role in all aspects of response.”

These types of solutions miss the point: The problem is in Federal-level implementation of the NRF/NIMS/ESF structure/process to support state/local incident management rather than the latters’ inability to “control” such catastrophic situations.

**FINDING 2: The expectation is almost a given that the Federal government will provide and manage primary support.** The overall trend from the First World War, through the Depression and World War Two to the present day is toward big government solutions. While the Federal government continues to produce doctrinal statements supporting management of disaster response at the lowest possible level, the expectations since Hurricane Andrew through Hurricane Katrina has been that the Federal government will provide and manage primary support. While FEMA during the tenure of James Lee Witt may have fed those expectations, the Bush administration chose not to continue his emergency management priorities for FEMA. Nevertheless, the expectations remained. Expectations and stated doctrine are thus at odds and breed confusion.

Unrealistic expectations reinforce notions at all governmental levels that disaster response should be federalized. Unrealistic expectations can be self-fulfilling and give credence to allegations that some states are planning to default catastrophic disaster response to DoD. In truth, the Federal government has not fully resourced preparedness. Instead, without fully committing resources itself, it establishes Federal—vice national—priorities and forces them on states.

---

<sup>53</sup> Ashton B. Carter, Michael M. May, William J. Perry “The Day After: Action in the 24 Hours Following a Nuclear Blast in an American City” The Preventive Defense Project (Harvard and Stanford Universities, April 2007), pp. 10-11.

**FINDING 3: The assumption that Hurricane Katrina was America’s worst natural disaster reinforces that expectation.** An underlying assumption holds that Hurricane Katrina was the worst natural disaster ever to befall the United States. Because catastrophic events of that scale are clearly beyond the ability of a local or state government to manage them without external support, it follows that it should be primarily a Federal responsibility.

Hurricane Katrina was unusually catastrophic, to be sure. In terms of geographic size, the hurricane was exceptionally big. In terms of mortality and damage, however, it is worth putting the disaster in historical context.

The greatest natural disaster in U.S. history was arguably the September 1900 Galveston Island hurricane and surge in which at least 6,000 people died in the city alone. Totals for the city and outlying region were 12,000 deaths, while well over 3,500 structures were destroyed.

Other noteworthy pre-World War One disasters include the Chicago fire of 1871. While the death toll of 300 was comparatively small, the fire burned nearly five square miles of the city, incinerated almost 25,000 buildings and rendered homeless more than 100,000 persons. In the 1889 Johnstown flood, over 2,200 people died. The 1906 San Francisco earthquake and fire killed over 3,000, destroyed over 28,000 structures and burned an area twice the size of the Chicago fire (three-quarters of the developed area of the city). Of note: Notwithstanding the scale of these disasters, the principle of locally managed emergencies remained sacrosanct well into the 20<sup>th</sup> century. These disasters were deemed local incidents requiring primarily a local responsibility for management of the response and recovery. Moreover, in the case of Galveston and San Francisco, the management of the recovery was led by the private sector.

**FINDING 4: Primary responsibility and authority for homeland security may have to devolve from the Federal to the state level.** The Federal government has not structured itself effectively and efficiently to resource and support state and local authorities to execute integrated, national (to include the private sector and NGO communities), all-hazards, homeland security prevention, protection/mitigation, response and recovery, consistent with the NRF/NIMS/ESF doctrinal basis for coordinated planning and execution.

At the Federal level, an integrated, national preparedness and operational framework may facilitate, but does not compel interagency coordination and collaboration. Absent is a truly *national* model of governance. The Federal government does not “own” the infrastructure or emergency preparedness system on which it is vitally dependent to achieve national objectives. Thus, hierarchical “controls” do not work. Options include two key elements:

- Partnership and network-based models of collaboration which are sustainable for resilience, e.g., technical and financial assistance, as opposed to unfunded mandates, preemptions or a default to use of the military<sup>54</sup>

---

<sup>54</sup> An important instance, however, of *collaborative* use of the military occurred in May 1992 during the Rodney King riots in Los Angeles when President George H.W. Bush authorized deployment of Federal military personnel and law enforcement officers for law enforcement. In response to a request from the California governor who was faced with the city’s inability to control “domestic violence and

- Performance standards and goals, e.g., the EPA's use of negotiated rulemaking, voluntary state agreements like the Streamlined Sales Tax Project (SSTP) and cooperative standard-setting regimes like those established by the National Fire Protection Association (NFPA), as opposed to detailed prescriptive requirements, like the Target Capabilities List (TCL) and Universal Task List (UTL).

As a reflection of reality, the Federal role in a national preparedness and operational framework is facilitation of state support of community-level collaboration/coordination in steady-state preparedness. The outcome is de-centralized community resilience.

-endit-

---

disorder," President Bush issued Proclamation 6427, commanding "all persons engaged in such acts of violence and disorder to cease and desist therefrom and to disperse and retire peaceable forthwith." The proclamation was the legal basis for his same-day Executive Order 12804, which suspended the proscriptions of Posse Comitatus to allow Army and Marine units to suppress the violence and restore law and order. In the end, some 4,000 Federal military personnel took part in the operation.