

Planning for the Inevitable: The Role of the Federal Supply Chain in Preparing for National Emergencies



Robert Handfield
Bank of America University Distinguished Professor of Supply
Chain Management
College of Management
North Carolina State University



2010

COLLABORATING ACROSS BOUNDARIES SERIES

Planning for the Inevitable: The Role of the Federal Supply Chain in Preparing for National Emergencies

Robert Handfield

Bank of America University Distinguished Professor
of Supply Chain Management
College of Management
North Carolina State University

TABLE OF CONTENTS

Foreword	4
Introduction to Supply Chain Management	6
A Framework for Government Supply Chain Planning for Preparedness	8
Component One: Supply Chain Team Governance.....	9
Component Two: Supply Chain and IT Risk Assessment and Planning.....	10
Component Three: Strategic Stockpile Planning.....	14
Component Four: Supply Chain Education and Training.....	14
Assessing the Preparedness of the Federal Government Supply Chain	17
Assessing Supply Chain Team Governance	17
Assessing Supply Chain and IT Risk Planning.....	19
Assessing Strategic Stockpiling Planning.....	20
Assessing Supply Chain Education and Training	22
Recommendations	24
Endnotes	26
About the Author	27
Key Contact Information	28

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, “Planning for the Inevitable: The Role of the Federal Supply Chain in Preparing for National Emergencies,” by Robert Handfield, Bank of America University Distinguished Professor of Supply Chain Management at North Carolina State University.

Professor Handfield uses the recent H1N1 pandemic threat as an illustrative example of how the federal and state governments need to evaluate their supply chain capabilities in preparation for national emergencies. As we have seen in recent years, there has been no shortage of national emergencies—ranging from oil spills to hurricanes to the threat of a pandemic virus. In this report, Professor Handfield sets forth a framework in which governments can assess their supply chain preparedness prior to an emergency.

Over the last decade, the importance of an effective “supply chain” has become widely accepted in the both the public and private sectors. The federal government today clearly recognizes that an effective supply chain can lead to cost savings, and in certain instances, save lives. With the creation of the U.S. Department of Defense (DoD) Logistics Agency, the U.S. military recognized the critical importance of supply chain management to facilitate its multimissions and support its personnel. In addition to serving as an excellent introduction to supply chain management, Professor Handfield’s report increases our understanding of how to assess supply chain preparedness.

While acquisition officials have some responsibilities for supply chain management, the area of supply chain management has not been as developed by civilian agencies as it has been by DoD agencies. This will need to change in the years ahead, especially as government continues to respond to national emergencies with increasing frequency.

A key recommendation of Professor Handfield is the need for a governance structure to initiate the assessment and identification of emergency response plans for each government agency. This governance structure would include both program managers as well as acquisition specialists. Agencies should start today to create dedicated teams to prepare and evaluate agency plans.



Jonathan D. Breul



Leanne Viera

We trust that this report will be informative and useful to government managers as they increase their understanding of supply chain management, including the role of supply chain management in preparing to respond to national emergencies.



Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
jonathan.d.breul@us.ibm.com



Leanne Viera
Partner, Supply Chain Management
IBM Global Business Services
viera@us.ibm.com

Introduction to Supply Chain Management

By now, it is clear to many Americans that our nation will typically experience every year one or more national disasters that impact the economy, human lives, the environment, or the national infrastructure. Federal responses to disasters are a critical capability in the minds of the voting public as well as state and local governments. Unfortunately, the record is not good: government actions to respond to recent incidents have proven to be delayed and often ineffective. This suggests a critical lack of capability in federal emergency preparedness for and management of major disasters.

One of the key lessons learned from postmortem analysis of these incidents is that the federal government is highly dependent on an ever-changing network of private industry firms and contractors for response capability, or what is commonly referred to as a “supply chain.” More specifically, we define the federal supply chain in the following way:

The federal government *supply chain* encompasses all activities associated with the flow and transformation of materials and services from inbound upstream suppliers through to end users via downstream distribution and a service provider network. Material, services, funds, and information flow both up and down the supply chain.

Supply chain management is the integration of these activities through improved supply chain relationships to achieve an improved response capability for national disasters.

Within the context of this definition, the federal government has an *upstream supplier network* as well as a *downstream distribution and a service provider*

network. Supply chain activities in these networks include, but are not limited to:

- Management of information systems
- Joint planning
- Bidding and negotiation
- Sourcing and procurement
- Scheduling of supplier and distributor activities
- Contracting
- Order processing
- Inventory management
- Warehousing
- Customer service
- After-market disposition or recycling of waste and unused materials

The *supply chain network* consists of all organizations that provide inputs, either directly or indirectly, to the federal government and federal programs and to U.S. citizens. Within the context of the federal government, examples of upstream suppliers may include raw material and service suppliers, information technology (IT) vendors, building and infrastructure project contractors, third-party logistics providers, and many others.

In order to manage the flow of products and services between all of the upstream organizations in a supply chain, the federal government employs an array of “acquisition and contract managers” who ensure that the right materials arrive at the right locations, at the right time. These “supply managers” are responsible for ensuring that:

- The right suppliers are selected.

- The suppliers are meeting performance expectations.
- Appropriate bidding and contractual negotiations following federal guidelines are employed.
- A good relationship is maintained with the suppliers.

It is important to note that, from the federal government agency perspective, the supply chain includes internal functions, upstream suppliers, and downstream customers. The federal government in this case is defined as all of the *internal* agencies that contract with external agencies on behalf of U.S. citizens and the public good. These internal agencies provide services to American citizens. Examples include the Federal Aviation Administration (FAA), the Department of Health and Human Services (HHS), the Department of Defense (DoD), the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention (CDC), the Department of Homeland Security (DHS), and the Federal Emergency Management Agency (FEMA), to name a few.

Finally, a firm's *external downstream* supply chain encompasses all of the downstream distribution channels, processes, and functions that the product passes through on its way to the end customer. In the case of the federal government, this includes state and local distribution agencies and governments, third-party logistics, health care, military, and other services provided to the American public that have been procured from upstream suppliers, but which must be distributed to upstream parties such as specific state, local, and private agencies that work directly with American citizens. One major part of downstream management is transportation management, involving the selection and management of external carriers (e.g., trucking companies, airlines, railroads, shipping companies) or internal private fleets of carriers. Distribution management involves the management of packaging, storing, and handling materials at receiving docks, warehouses, and retail outlets, as well as the provision of payments and services to entities.

Although these concepts may seem simple, the challenges in managing these flows are immense and complex. Federal agencies need to view these different components of the supply chain as integrated and interconnected. Why? Because a disruption in

any single node of this integrated supply chain can disrupt other portions of it—upstream or downstream. For example, an event such as the April 2010 BP oil spill can hurt not only local agencies, but suppliers and distributors in multiple industries and agencies. How can federal agencies better manage and impact disruptions that occur and impact these supply chains?

A Framework for Government Supply Chain Planning for Preparedness

This report presents a simple, high-level planning framework for federal government agencies to follow in establishing preparedness plans and securing each agency's respective supply chains. The federal government supply chain is much more interconnected with private industry than most people realize. Our research posits that federal government agencies are part of a much larger supply chain that spans both public (e.g., state and local governments) and private (e.g., private businesses, forums, and cooperatives) enterprises.

One of the most important observations regarding preparedness planning is that 85 percent of the assets required to respond to any emergency resides within the private sector. As a result, the federal government must work collaboratively with its private sector partners in order to respond to and limit major systematic disruptions caused by a potential disaster. Because of the nation's recent experience in responding to the recent H1N1 pandemic, we will use the pandemic as an illustration of how the U.S. government used supply chain techniques to respond to that specific threat. This report, however, is applicable to multiple threats to public and private supply chains, and focuses on how the United States can prepare for future threats. Pandemic planning serves as a useful example for framing this discussion, as this recent threat included multiple federal government departments (HHS, including CDC and DHS), as well as multiple state health care agencies.

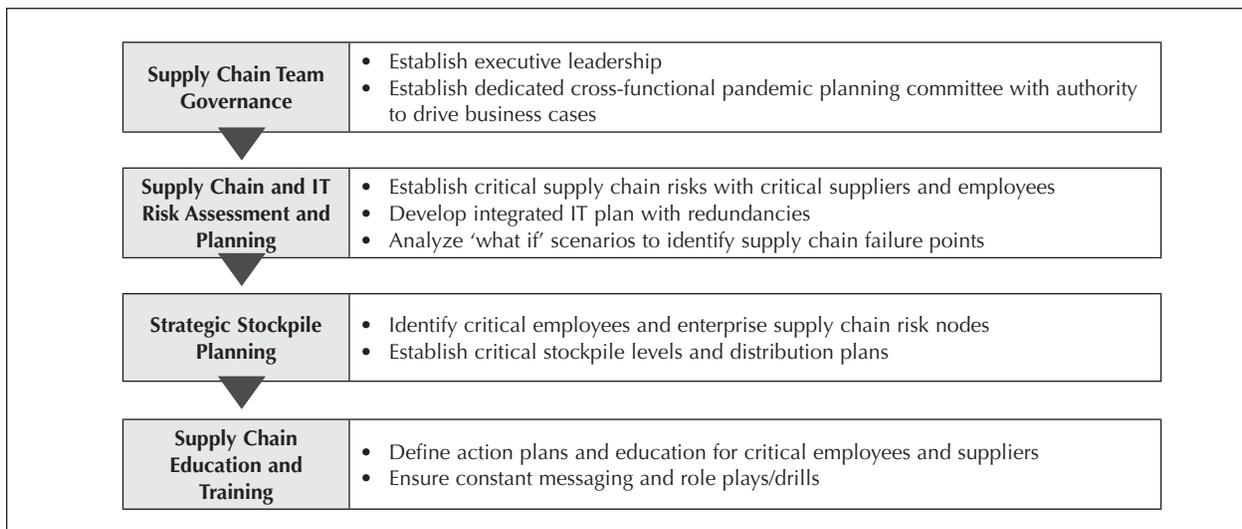
Our qualitative research indicates that a "multi-pronged collaborative approach" is fundamental to successful preparedness planning. Specifically, federal government agencies must collaborate and partner with private industry, as well as with state and

local governments, to establish aligned plans and objectives that are able to respond flexibly to different potential scenarios. The federal supply chain preparedness planning framework consists of a dedicated set of plans, policies, guidelines, training initiatives, and mitigation investments that form the basis for preparedness and resilience in the face of an emergency event.

The four primary components of creating a supply chain in preparation for emergencies are as follows (see Figure 1):

- Component One: Supply Chain Team Governance.** It is estimated that at least 10 percent of an enterprise's business continuity planning budget should be devoted to emergency planning in the supply chain. Ideally, a Supply Chain Planning Team (SCPT) is formed as a distinct entity focused on ensuring business continuity in critical supply chains. From the outset, federal executive leadership, appropriate funding, and sponsorship of the preparedness planning effort are required to support SCPT activities. Every federal agency should have an SCPT in place, with associated government roles and responsibilities established.
- Component Two: Supply Chain and IT Risk Assessment and Planning.** Once established, an SCPT needs to conduct an in-depth assessment of potential "at risk" agencies, enterprises, and nodes, as well as of critical employees and suppliers within each node. Leaders must engage in a full-scale "what if?" analysis to determine and identify high-probability failure points/nodes in the supply chain. The IT infrastructure should be assessed to determine the effect on servers and

Figure 1: Federal Supply Chain Preparedness Planning Framework



system broadband width, with an increase in telework in the event of an emergency.

- **Component Three: Strategic Stockpile Planning.** Strategic stockpile requirements need to be defined, with a specific focus on those high-risk nodes in the supply chain. The focus of these assessments first should identify the impact of a general class of disruption events, without specifically identifying what the nature of that disruption may be. Redundant asset investments may be required to deal with these issues. The investment should be justified on a business case basis, and approved by senior government leaders.
- **Component Four: Supply Chain Education and Training.** Training and education programs for staff at “at risk” agencies and their critical suppliers are critical. While the details of a training and education program may change based on different criteria, agency staff should be familiar with a high-level overview of different scenarios that might be possible so that they know what to expect.

In the following sections, each of the components of the federal supply chain preparedness planning framework is discussed in more detail.

Component One: Supply Chain Team Governance

Federal agency senior leadership support is critical in the creation of an effective preparedness plan. The

establishment of a preparedness governance structure and a dedicated pre-planning team should follow. During the avian flu, federal agency responses varied—ranging from ad hoc committees monitoring industry trends to periodic conference discussions and open forums for discussion. In the private sector, organizations put together cross-agency teams in 2008-2009 to view the issue, and have elicited significant levels of representation from private industry participants, including hospitals, pharmaceutical manufacturers, third-party logistics providers, financial services industry experts, and IT hardware providers and systems consultants. In some cases, these newly formed multi-industry pandemic planning councils have created important standing business continuity planning councils that meet on a regular basis, then gather to periodically measure and assess cross-industry risk issues that can impact federal government planning. Some have also established subcommittees to specifically identify risks associated with a forthcoming potential event.

The establishment of an executive steering committee guidance council is the first step in establishing a proper federal agency response planning team. Some of the key questions that should be addressed in forming such a team include:

- What other agencies that we deal with on a regular basis also would be impacted in the event of an emergency announcement?
- Which industries and state/local government agencies are in our supply chain, and would be impacted?

- Are we dependent on certain resources (IT infrastructure, logistics, lines of communication) that could impact our operations in an emergency?

In answering these questions, bear in mind that the goal is not to make the team composition too extensive, but rather to ensure that the “right” people are in the room. Other issues that should be addressed will include the following:

- What is the level of funding required for team meeting, planning, and industry analysis?
- Will third-party consultants be required to perform additional supporting analysis and/or subject-matter expertise?
- If significant government spending and/or policy impacts could arise, what is the appropriate level of approval required for these decisions?
- How often will the team meet? Will the team consist of a core and/or extended team?
- Who is the executive champion for the team?
- What are the specific scope and objectives of the team’s activities? What is in scope and out of scope?

These are fairly basic questions, but it is important that they be addressed early on in the formative stages of team development. At the most developed levels, agencies have established dedicated teams of supply chain professionals who collaborate with key government leaders and security officers to establish documented plans and pilot tests associated with unexpected events, with formal senior executive leadership reviews and business case funding development around the potential risks of an event. These types of activities represent a serious dedication of resources to planning, and often involve significant subject-matter expertise and simulation analysis to establish “what if?” scenario planning and contingency plans, leading to specific recommendations on stockpiling, training, supply risk management, and other outcomes. In many cases, these teams have the authority to establish specific policies and strategic planning coordination with executive functions to enable the right level of preparedness.

Once established, the team should develop a formal team project charter, establish a project plan, and communicate the project plan to all impacted

individuals. The first step of the team will be to conduct a risk assessment.

Component Two: Supply Chain and IT Risk Assessment and Planning

Supply chain and IT risk assessment and planning are the critical activities that the newly formed governance team must carry out. The process of developing a risk plan should include the following five planning steps.

Planning Step One: Identify all government agencies, partners, and suppliers that are potentially impacted by the emergency.

This activity involves conducting a series of “what if?” exercises, involving the creation of high-level value stream maps that define which government agencies and suppliers are involved in critical processes. It is impossible to be able to predict any specific event that will occur. Instead, it is more beneficial to think about general classes of events and focus on where they would have the greatest impact in terms of disruption of federal government services. For example, different families of events could include cyber-terrorist events, pandemics, disruptions of major transportation services (rail, truck, air), environmental spills, disruptions of the electrical grid, gasoline shortages, etc. Note that the root cause of these events is not identified—but the impact of these events can be translated into specific nodes and links in the federal government agency’s supply chain which have relevant meaning for planning purposes.

In private industry, this exercise may be easier to do than it may be in a government supply chain. For example, processing a stock trade involves communication between a trader and a customer, which largely can take place through electronic and telephonic communications. However, delivery of coal to an energy generation plant requires the physical presence of the coal supplier, the transporter, the railway, the bulldozer operator, and the generation plant personnel. While these scenarios may seem simplistic, it is important for the team to take a structured approach to mapping out how government services for the agency are carried out, and consider all impacted entities and agencies that might not be able to provide normal service, given an emergency scenario. For example, if an agency operates largely through meetings with state representatives, there is

a good chance that these individuals will not be physically present in the nation's capital or state capital cities, and may need to meet virtually. Similarly, if an agency relies on third-party distributors for dispensation of key medical and food supplies, these supply chains may be disrupted due to employee absenteeism at these third-party suppliers during a pandemic event. These employees/suppliers should be classified according to whether or not their physical presence or geographic proximity to the active supply chain location is required.

Planning Step Two: Identify systems and IT infrastructure impacts.

IT infrastructure planning involves identifying the critical backbone and support systems required to allow "social-distancing" for key workers who can work from home (also known as "teleworking"), as well as ensuring the security of transactions and communication with critical suppliers. In the latter category, suppliers who are not getting paid due to system failures may curtail their delivery of services or materials given the uncertainty of continued financial flows.

Further, social distancing training may need to be established for workers who are going to work from home. Robust work-from-home programs should include the distribution of secure laptops, Internet technology, and other materials to enable individuals to work from home. There also may be extensive requirements in terms of establishing technology requirements and access to records. For example, insurance companies and medical billers from hospital systems will need to be able to get access to patient records, and to be able to download and send materials. There may be challenges involved here, such as Health Insurance Portability and Accountability Act (HIPAA) regulations not allowing individual records to leave the server community. The best way to stress-test a system is to have employees work from home once a month, document the items that they were "missing" when they tried to complete their work, and establish mechanisms for creating access to these items.

Planning Step Three: Establish the criticality of associates and suppliers.

Next, the team needs to establish classifications of associates and suppliers who are impacted, and

then code them as to whether they must work on-site or not. In general, three categories will follow:

- **Category One: Individuals who are critical to the business and must work on-site.** Training and precautionary protection should focus on these individuals, and they may be targeted for a first round of antiviral drugs and protective measures.
- **Category Two: Workers who are critical, but can work from home.** Establishing work-at-home policies can be extensive, and may include specific portal development, laptop distributions, specialized Internet access backbones, and other technological elements. Workers must be able to access their office documents and files online, and this may require additional effort.

More mature organizations not only have established work-at-home policies, but have validated and tested them by having these workers actually work from home at least once a month to determine shortfalls and gaps in coverage. A pilot assessment should indicate that every employee must show that they can be productive while working at home.

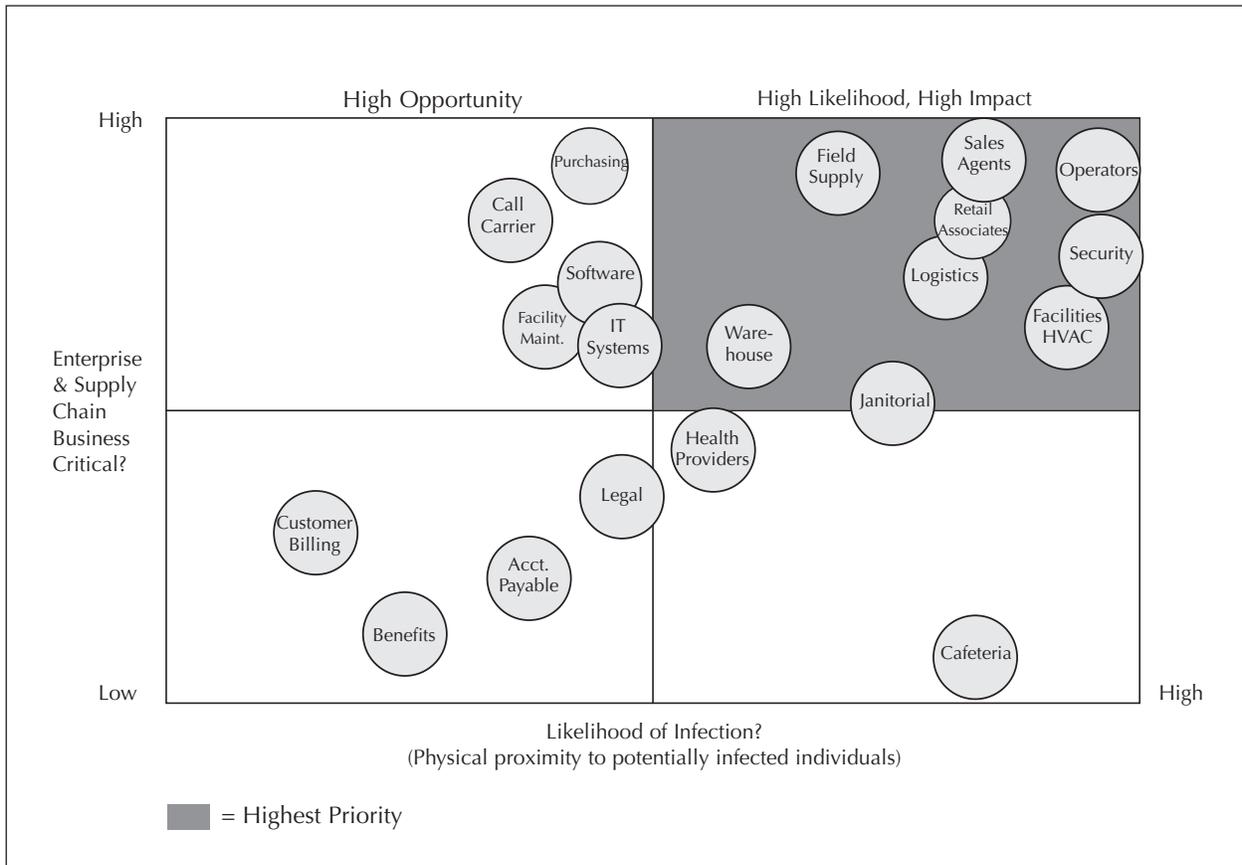
- **Category Three: Workers who are not critical.**

Training is especially critical for employees who fall into categories one and two, and specific programs should be directed for intensive training and education to this populace in the first wave.

Planning Step Four: Establish an Enterprise Function Risk matrix highlighting business-critical functions.

This matrix can be created based on subjective factors, but should reflect the relative impact on the business, and the likelihood of exposure. A sample enterprise *function* risk impact matrix is shown in Figure 2. Even a subjective set of assessments will provide an initial glimpse into the key associate groups that are considered critical to business continuity and the likelihood that they will be infected due to physical exposure. Examples of functions that are most likely to impact the business, and are likely to be exposed, include any individuals associated with operations, sales support, direct materials, customer service, logistics, or field service. Identifying the number of these individuals is an important step, as roles may have changed in the past 6 months,

Figure 2: Sample Enterprise *Function* Risk Impact Assessment



and specific individuals and suppliers need to be identified and contacted. The results of this analysis often may provide surprising results to the governance team. For example, individuals who must be on site for a facility to operate often include security guards, HVAC, facilities engineers and workers, and janitorial/waste management staff. These individuals often are considered low-wage workers, and may have a minimal amount of training, yet are considered critical to the operation.

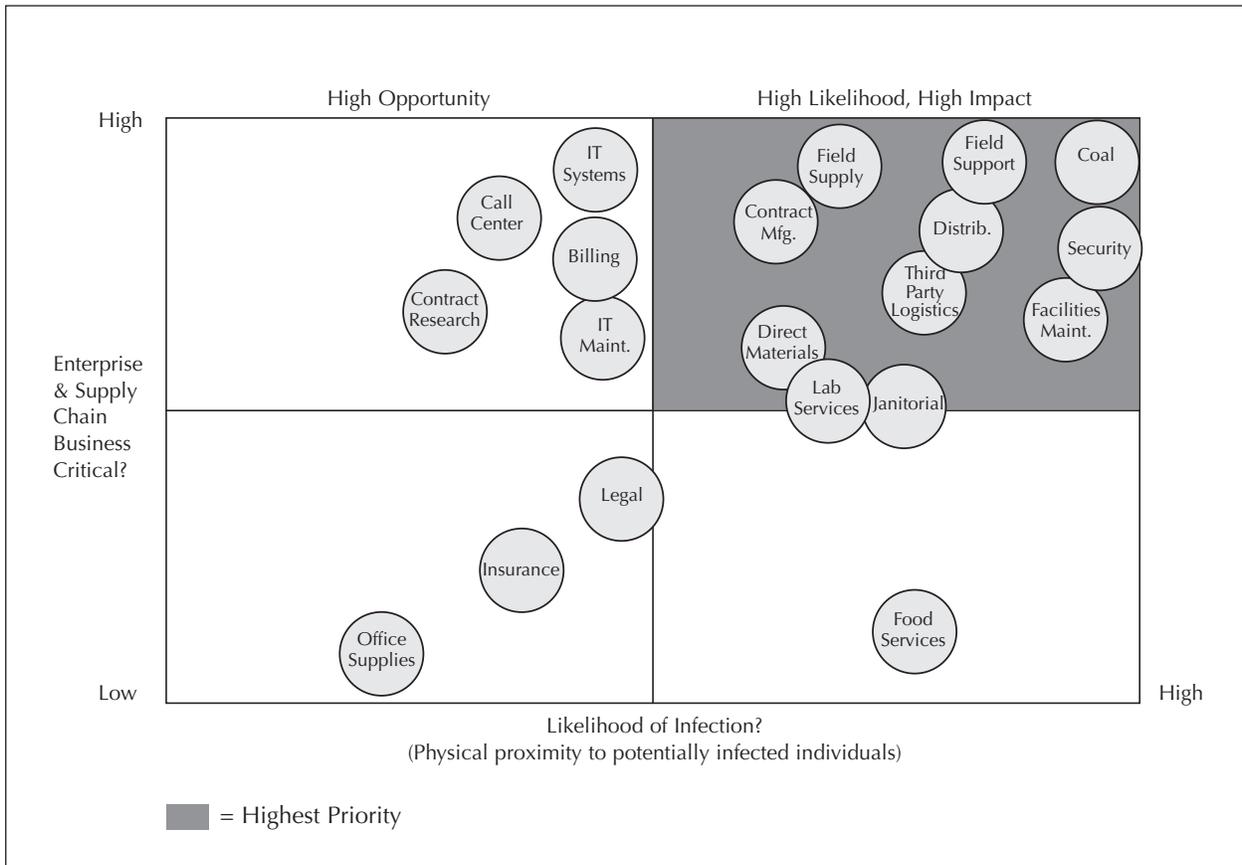
Likewise, an enterprise *supplier* risk impact assessment may identify critical categories of supply that can potentially disrupt operations (see Figure 3). For example, coal is considered a critical category that can impact energy generation supply. Likewise, rail transportation that delivers the coal is also considered a critical element. Chlorine for water plants is important, as many water-processing facilities only have 3 days of chlorine for water, and must keep higher numbers of tanker cars to ensure water continues to be available. In hospital operations, one area that is considered to be important is intravenous (IV) tubing for ventilators. Most ventilator

tubing is not produced in the United States, and although there is some domestic inventory of tubing, this supply would not be enough to support a full-blown emergency. If borders are shut down, this could become a highly critical situation. Other on-site services such as facilities, janitorial, distribution, customer field support, and other areas are considered critical supply areas that may not have been viewed as critical in the past from a supply management perspective. Under the rubric of risk planning, however, these now may become essential suppliers that must be included in a formal risk planning exercise.

Planning Step Five: Establish potential action plans.

Once key nodes in the internal and external supply chain delivery model are understood, preliminary plans need to be identified to establish business continuity actions. Several potential options should be identified through structured brainstorming sessions. For example, in a pandemic scenario, the most basic response is to ensure compliance to

Figure 3: Sample *Supplier Risk Impact Assessment*



cleanliness, by emphasizing through training and education the need for individuals to assume responsibility for washing their hands and using disinfectant products on them when using restrooms and prior to meals. The primary method of transmission of viruses occurs through hand contact with a virus that is subsequently passed to an individual through actions as simple as scratching an eyelid, the lips, or the nose. Training and education on personal sanitary precautions in the work environment during the early phases of an emergency can have a major impact on the rate of transmission.

Another set of activities involves closing noncritical facilities during a crisis, and encouraging employees to work from home. Social distancing reduces the frequency, proximity, and duration of contact between people in a pandemic scenario, which reduces the chances of spreading pandemic influenza virus from person to person. Teleworking is also important when a facility has been threatened or destroyed, assuming that individuals can access their organizational IT systems. This is clearly not always an option, as there are often activities that

require the physical presence of an individual to complete the necessary work.

Another set of measures involves creating for critical employees stockpiles of support materials that can provide a stopgap measure to ensure that workers continue to work during the event. This is covered in more detail in the next section, which discusses strategic stockpiling.

One important feature of organizations which have well-established, mature risk planning functions is that they not only create a risk matrix, but they also stress-test this matrix through scenario simulations that create a crisis environment. For example, several of the firms in the financial and energy sectors have had trial runs—during which a given percentage of workers worked from home—to determine the net impact on operational disruptions. These types of simulated activities create important “lessons learned” after a thorough postmortem takes place, and provide a higher level of resiliency and confidence in risk plans.

Component Three: Strategic Stockpile Planning

Stockpiling supplies and/or creating redundant sources of supply is one of the most often cited strategies associated with pre-emergency planning. The cost of stockpiling is not insignificant, and requires an investment in products that go into inventory and which may or may not be utilized in the short term. Typical inventory holding costs are in the range of 18 percent to 25 percent of the value of a good on an annual basis, and include opportunity costs, storage, interest, insurance, shrinkage, and obsolescence. Questions surrounding supply chain stockpiling of goods include the following:

- What types of supplies are required?
- What other types of redundancies can be identified (e.g., second source of supply, multiple transportation routes, etc.)?
- Who are the critical individuals requiring access to stockpiles?
- What is the right quantity of supply and redundancy?
- What is the relative cost of supply and redundancy?

Returning to our pandemic planning scenario, stockpiling ahead of an actual pandemic is an important strategy, and is made even more critical given the length of time required to develop and distribute vaccines. The length of time to isolate a strain and develop a vaccine is often 6 months or longer, so organizations should rely on other forms of prevention in the short term. Interviews with key experts also reveal that, once a vaccine is identified and isolated (which could take 6 to 12 months), the actual vaccine treatment requires two shots, spaced 21 days apart, which further lengthens the response time.¹

The most important supplies identified for stockpiles in a pandemic scenario fall into four categories:

- Hand sanitizers
- Masks
- Vaccines
- Antiviral drugs

Our research points to several important best practices that enterprises should consider in establishing necessary stockpiling approaches. More-mature organizations have developed sophisticated approaches to measuring and deploying stockpiles. As noted earlier, the costs of doing so are not insignificant. As such, a cost model to identify the different costs of stockpiling, relative to the lost wages and productivity associated with employee illness, was developed.

Stockpile cost modeling requires a supply chain team to identify the relative cost of stockpiled items (including inventory cost, warehouse costs, redundancy costs, etc.) and then weigh this against the lost productivity impacts of a major disruption in service. Such cost models are often difficult to estimate accurately, and should therefore be based on “most reasonable estimates.” The output of the model is intended to establish a baseline for decision-making relative to the level of investment an agency is willing to budget towards preparedness relative to a possible incident.

Component Four: Supply Chain Education and Training

In addition to stockpiling and redundancies, the training and education of staff and suppliers on preventive measures that can reduce the transmission of viral infection is a critical component of any enterprise preparedness plan. Ideally, every organization should develop mandated employee policies to enact in the event of a crisis, with subsequent measures to be put in place in the event of elevation to subsequent levels. All of these activities reduce the risk of an individual getting infected and transmitting a virus to others.

An industry expert we interviewed noted that several key elements in any enterprise’s arsenal to combat a pandemic scenario are travel policy, human resource policies, and educational programs. Employees should be trained not only on personal hygiene, but also on establishing clean work areas. For example, one enterprise has established a weekly routine of “Wipe-Down Wednesdays,” during which individuals are equipped with Clorox Handiwipes and asked to clean their respective desk, phone, keyboard, and mouse. Another organization has a pizza party twice

a year in a festive atmosphere to clean employees' workspaces. Other training should focus on coughing etiquette, and specific policies on social distancing in the event of an emergency.

As noted earlier, many of the staff or suppliers who are perceived as "low value-added" (including janitorial, HVAC, facilities maintenance, etc.) may fall into the "critical" category when viewed from a business continuity planning perspective. These individuals may be getting a minimum wage, and may have very little training. In such cases, specific training targeted on protecting these individuals, and having them trained in critical planning activities is foundational to success.

Preparedness training also fundamentally impacts human resource policies, especially in areas such as business travel procedures. Individuals should be encouraged not to travel if at all possible to avoid contact, including minimizing personal leisure travel. Human resource departments may need to change policies on sick days in the event that individuals contract the flu, and change the culture of the workplace to encourage people to stay home when they are sick without asking them to forfeit their sick days. This is often a major cultural change.

Mature levels of preparedness supply chain planning involve training not just for critical employees, but defined action plans for all workers and families. Organizations also should carry out pilot testing to ensure that workers follow standard operating procedures to ensure compliance with the plan. Effective training and communication involve using techniques that are very much aligned with prior efforts in the public health arena, such as the use of seatbelts and smoking cessation.

Training initiatives should include constant pressure over long periods of time, measurement of compliance, and intermittent teaching moments that are carried out as issues come up. Followup mitigation planning and additional training may be required, with detailed information sessions providing explanations about why certain procedures are required. This level of training goes beyond simple newsletters, into specific actions that individuals in different roles should take. Critical suppliers should also be included in these sessions to ensure that the overall supply chain is not impacted.

Assessing the Preparedness of the Federal Government Supply Chain

As part of our research, we interviewed more than 50 individuals in private and public organizations who were working on emergency planning initiatives of one form or another. These interviews were subsequently coded and examined to create a framework for assessing the relative maturity of an organization's supply chain preparedness. This framework provides a basis for assessing different levels of industry preparedness for a potential event. More importantly, this framework also serves as an auditing mechanism for federal governments to apply in assessing the relative level of preparedness for different federal government agencies.

We emphasize here that this framework model is based on preliminary research, and incorporates classic risk theory models around assessment, diagnosis, and root cause analysis for any type of supply chain risk. The model is intended to be used for assessing current emergency preparation levels, using the specific federal agency as the unit of analysis. The agency is the appropriate unit, as each plan will vary based on the stakeholders served by that agency, the particular characteristics and issues that these stakeholders face within their respective environments, as well as the level of maturity of that particular industry or public sector's own plans. For example, agencies such as HHS and DoD may have mature organizations in place, since their stakeholders already have mature plans in place (e.g., hospitals and military units). However, other government organizations may have less well-established programs, as planning has not been as much of an issue for their organizations.

This framework provides a baseline for assessing agencies, and can prove to be of value in creating a mechanism for assessment, identification of gaps,

and planning committee development when there are clear opportunities for improvement.

In assessing the current condition of federal government agencies, we will refer to the table shown in Figure 4. However, there are several key elements associated with the level of preparedness of federal government agencies. As noted earlier, they relate to agencies' ability to:

- Work with other federal and state agencies to coordinate planning initiatives
- Continue providing related services (public health care, unemployment benefits, natural resources, prisons, transportation, or others, as appropriate) during an event

We conducted interviews with multiple government agency representatives to effectively assess the level of maturity and identify a baseline level of preparedness. We do not claim that these results are 100 percent accurate, as there certainly would be a high level of variation depending on which agencies were selected, but they do represent a baseline for measuring other agencies on a more detailed basis.

Assessing Supply Chain Team Governance

Just about every federal agency has some type of disaster recovery plan, some governance committee, and some form of recovery plan. This was initiated largely since 9/11, but when it comes to planning, experts we interviewed agree that there are significant shortcomings in these plans, and that most of them are "skeletal" in nature. A recent issue briefing paper published by the National Association of State

Figure 4: Framework for Assessing Federal Government Preparedness (Using Pandemic Planning as an Illustrative Example)

Component	Level 5	Level 4	Level 3	Level 2	Level 1
Supply Chain Team Governance	Dedicated team with extensive, documented plans by business and function, with pilot runs and simulation analysis.	Dedicated team with extensive documented plans by business and function with pilot runs and simulation analysis.	Dedicated pandemic planning team activities under way, with some documented planning.	Ad hoc pandemic planning committee meetings.	No planning activity.
Supply Chain and IT Risk Assessment and Planning	Formal supply chain pandemic risk analysis identifying critical weaknesses in the supply chain impacted and risk mitigation plans in place. Supplier development and training deployed. Fully integrated IT plan with redundancies and work-at-home plans tested and validated.	Formal supply chain pandemic risk analysis identifying critical weaknesses in the supply chain impacted and risk mitigation plans in place. Backup plans for work-at-home policies, and IT resources to support identified and planned. Backup plans for IT system failures and server recovery plans identified.	Formal supply chain pandemic risk analysis identifying critical weaknesses in the supply chain impacted. Backup plans for work-at-home policies, and IT resources to support identified and planned	Discussions and meetings with critical suppliers on pandemic planning. Work-at-home procedures identified	No communication with suppliers on pandemic planning. No IT infrastructure plans in place.
Strategic Stockpiling Planning	Antivirals, masks, gloves, and other relevant supplies for entire workforce and critical suppliers, with detailed deployment plans.	Antivirals, masks, gloves, and other relevant supplies for entire workforce, with detailed deployment plans.	Stockpiles to cover critical workforce with informal deployment planning.	Selective stockpiling of antivirals and masks, no deployment planning.	No stockpiles created.
Supply Chain Education and Training	Defined action plans for critical workers and critical suppliers, with mitigation plans identified for employees and supplies that are impacted. Distance work and family antiviral activities identified for associates and suppliers. Trial runs carried out to identify bottlenecks and challenges in training plans with mitigation plans.	Defined action plans for critical workers, and mitigation plans identified for workers who are sick. Distance work and family anti-viral activities identified.	Mandatory training seminars providing details on pandemic precautions and policies on work restrictions in a pandemic event for critical workers.	E-mails and newsletters on pandemic precautions.	No training on pandemic precautions.

Chief Information Officers (NASCIO) suggests that the appropriate level of preparedness is simply not in place.² There are very few robust analyses that provide insights on how different federal agency services, data systems, and workforce attendance would be impacted during a full-blown emergency. For example, the H1N1 virus is now considered an anomaly in terms how an influenza pandemic typically unfolds, and in fact may prove to be one of the biggest barriers for agencies to begin preparations. Because the virus was relatively mild in nature and fortunately did not cause any debilitating problems, many political leaders and agency bureaus unfortunately may have permanently discounted the potential damage that a more serious virus might bring. The issue of governance and planning should continue to be on government policy agendas, but we fear that the damage of a mild H1N1 virus event may dissuade them from doing so in the future.

Federal agencies rely on state governments as the primary vehicle for the distribution of emergency supplies and other components of emergency responses managed by federal agencies. However, state governments also should be prepared for internal stockpiling measures required for state employees. Our interviews suggest that this level of detail has not been developed, to date, in the majority of states. Experts believe that the locus of effort should not reside with senior state officials to develop plans, but that individual agencies need to assume responsibility for specific risk planning and mitigation actions as described in this report. Legislators are not risk planners, and should not be relied on to establish detailed, unit-specific action plans. Greater interaction between federal and state supply chain and contracting agency planners is required to ensure that all state agencies are aligned with federal requirements for preparation, and should be included in any agency that is involved in these preparations.

Several leading authorities believe that a major gap in federal agency preparation exists, due to the current structure of planning. The focal point of this discussion is related to the National Incident Management System (NIMS). Michael Osterholm—director of the Center for Infectious Disease Research & Policy and director of the Minnesota Center of Excellence for Influenza Research and Surveillance—is highly critical of the NIMS

approach. He notes that NIMS is an outdated approach to responding to pandemic influenza, emphasizing that “every village, town, city, county, state, region, and even country will be in the soup about the same time with the next influenza pandemic. A pandemic will quickly exhaust available resources, replacements will not be forthcoming, and it will be many months before we enter into recovery. NIMS as we now employ it will be quickly overwhelmed. We will need to determine which authorities and responsibilities remain at the local, state, federal, and international levels, and which have a strong federal leadership role.”³

Based on these observations, we surmise that the federal government is at a Level 2, in that some progress has been made, but there is not a uniform structure or team in place at most agencies that is following a disciplined process for risk assessment, stockpiling, and workforce training and education.

Assessing Supply Chain and IT Risk Planning

There is a real diversity in the extent to which different federal agencies have prepared their supply chains for an emergency. One senior government official at DHS noted: “There are certainly gaps that need to be filled. Some have gone further than others, and have developed extensive plans with the private sector. This is critical, since 85 percent of the assets required to support a response are owned by the private sector.” Private-sector industries are essentially responsible for the continuity of water, power, health care supplies, and other critical elements. Although many have detailed plans in place, few have detailed countermeasures, and there are clearly some gaps between the public and private sectors, where planning and alignment are lacking. In general, with a lack of formal governance mechanisms, and based on interviews with state and federal officials, we believe that most states have not established impact assessments identifying critical supply chains that will be affected in an emergency.

One of the agencies that should become more involved is the Federal Trade Commission and HHS. Osterholm points out that many of the medical supplies we rely on are in fact imported from China and Asia, and that these critical transportation networks may in fact be quarantined and shut down

during a major emergency. Some of the critical medical supplies that could be threatened with shortages in an emergency include the following:

- **Test kits or reagents.** Most commercially available test kits or reagents are made outside of the United States, and there is no stockpile of these products.
- **Life saving drugs.** Due to their high cost, many hospitals do not keep a large supply of drugs.

In fact, 95 percent of all generic drugs used in the United States are made offshore, primarily in China and India. Our review of the stability of these supply chains with manufacturers is extremely alarming. Many manufacturers rely on just in time systems, and few have large stocks of generics available and stockpiled. There is clearly a need for hospitals and manufacturers to hold joint collaborative meetings to review the state of inventories and capacity in these critical supply chains. In addition, there is no national system to stockpile these drugs to ensure their production and delivery in the United States, and no national rationing plan for a serious drug shortage during an emergency.

Masks are another concern, according to Osterholm. Masks and respirators will play a major role in the case of a national medical emergency which closes borders. The production capacity for manufacturing masks and respirators is limited internationally. Much of the available U.S. product is manufactured offshore or the key raw materials originate in Asia. We will quickly exhaust limited federal, state and local stockpiles of these products, and we have no plans for how to respond when that occurs. Another issue surrounds gloves. Asian glove production capacity is the primary source of latex gloves, and production is already “stretched,” and given the importance of natural gas to such production, the cost and availability of gloves will grow as critical problems. Only limited stockpiling of gloves is occurring. Gloves, like other infection control-related products, will be in short supply very early into the next pandemic.

Federal agency information systems infrastructure is one of the most critical components of support that must be maintained during a major emergency episode. As noted earlier, NASCIO recently highlighted the importance of planning within the overall context of maintaining government agency systems.

There are many components to support IT resources, including sustaining server platforms, sources of electricity to power these platforms, cooling of server locations, and other details that are often overlooked under these circumstances. Many people fail to understand the level of support provided by an agency’s central services. Also, many states control telecommunications, including systems that support police, firemen, and first responders. Federal and state data systems provide health information that is accessed by state and local health departments, which would be critical to access in the event of a mass exodus to hospitals. If a state facility is quarantined and individuals cannot access it, there is little planning in place to develop contingency measures. In general, planning for critical federal and state agencies infrastructure is at a nascent stage.

We believe that the level of maturity for Assessment of Supply Chain and Risk Planning is at an Level 1 (ad hoc) for the majority of federal agencies. While some agencies have certainly dedicated effort towards establishing a risk assessment, and indeed some have even documented these risks, the evidence is that much work still remains to be done. Many of these risk documents are believed to be perfunctory, and have not been fully vetted with key public and private stakeholders in the supply chain. The ability of agency IT infrastructures to support a national emergency has not been stress-tested or studied in enough detail to provide insights into their ability to support a national emergency.

Assessing Strategic Stockpiling Planning

In the year 1999, the responsibility for creating a National Pharmaceutical Stockpile (NPS) was given to the Centers for Disease Control and Prevention, an agency within HHS. The purpose of creating such a system was “to provide a re-supply of large quantities of essential medicine material to states and communities during an emergency within twelve hours of the federal decision to deploy.” Effective on March 1, 2003, the NPS became the Strategic National Stockpile (SNS) managed jointly by the Department of Homeland Security and HHS.

It is further noted on the CDC’s website: “Critical to the success of this initiative is ensuring capacity is developed at federal, state & local levels to receive,

stage and dispense SNS assets.”⁴ The extent to which state governments are prepared to distribute to local communities is not fully documented. There are several key issues that determine the United State’s ability to respond to an event.

The SNS is essentially a central storage facility from which medical supplies are sent to any city in 8 hours’ time. The pre-pandemic influenza vaccine stockpile, for the H1N1 vaccine manufactured and distributed in October 2009, was recently added to the SNS. Unlike previous pandemics, the H1N1 occurred with little warning, and CDC and other government agencies attempted to initiate the development of a vaccine form which was to be distributed in October and November 2009. Unlike antivirals (e.g., Relenza and Tamiflu) and preventive supplies (e.g., masks, respirators), vaccines cannot be pre-distributed, but are best stored in a manufacturer’s temperature-controlled facilities.

HHS manages the procurement and storage of those vaccines, while CDC has been the coordinator for distribution to the states. Moreover, CDC is responsible for ensuring that the vaccines are delivered from manufacturers to the states, contacting manufacturers through HHS and working with them on supply projections. Another organization, DHS, is responsible for private organizations, telecommunications, transportation, etc. The interaction of these three organizations has occasionally resulted in miscommunication, misalignment of planning—and, for example, subsequent shortages and loss of shipments of the H1N1 vaccine in October 2009.

Vaccine manufacturers in the United States ship a significant amount of seasonal vaccine on an annual basis (approximately 100 million doses in a season).⁵ Control over the distribution of pandemic vaccines, however, falls under various levels of control, and it is not clear how these channels are managed. According to one source, CDC works with state governments to ensure that they take proper control of the situation once the federal government sends stockpile inventory to them. This interviewee suggested that “we can’t simulate what happens in a pandemic with absentee rates. We are just seeing if we can move a mock vaccine from one location to another.” This individual further notes that “they are confident they can deliver—but once they hit the state, we have no control.”

The SNS claims to be able to distribute within 12 hours medical supplies concurrently to any state in the United States and to several large cities on a broader scale. There are several challenges that may make this assumption inoperable. For instance, is there a sufficient quantity of stockpiles to cover all states concurrently? Who ultimately has the authority to decide what locations are priorities if allocation occurs? Once supplies reach each state, are there specific state timelines and methodologies for ascertaining the appropriate distribution of medical supplies to local communities? All of these decisions point to the fact that there is a need for self-supply on the part of individual enterprises, and that measures need to be considered for self-supply. This also is reflected in the comments made by a senior physician, interviewed at CDC, who commented that, for people who run private enterprises, it is “time to think about” how they might adapt if an outbreak happens on a large scale and they have to make things work with people working or studying from home. He also says that 11 million doses of antiviral drugs from a government stockpile have been sent to states with cases of the swine flu, including California, New York, and Texas. Finally, this individual expressed concern regarding a lack of funds for the public health system that, due to cuts in government budgets, could cause problems in the future—and that “investments in preparedness” is what led to this outbreak being identified in the United States as quickly as it was.

These issues clearly support the need for an improved coordination between federal and state agencies instead of a national-level stockpile, which might be best suited for tackling a terrorist attack rather than for a pandemic outbreak.

Several individuals interviewed for this report stated that alternative governance models for distribution need to be developed that can allow states to control stockpiles on a more locally distributed basis:

- “The best model would be at a state level under the governor’s supervision and in collaboration with DHS and FEMA. The model should get to the granularity of detail.” (NASCIO Issues Coordinator)
- “The Strategic National Stockpile would not be that effective for a pandemic outbreak. This is because planning has to be done on a regional/

local basis.” (Risk Manager, Large Midwest Hospital Chain)

- “SNS was originally created to counteract any event of bioterrorism, and it expanded to include pandemic attacks and natural disasters.” (Health Scientist, CDC)

In the event of a national-level outbreak, dispensing medical supplies to all the required locations from one centralized location would, in our opinion, be extremely difficult to accomplish.

Additional discussions with other agencies provided a patchwork of insights, with a great deal of confusion as to how stockpiles were to be planned for and distributed. Our own analysis of stockpiling suggests that local distribution centers would be capable of holding supplies and distributing them to a set of regional locations, based on population and geography, at some cost and by using simple inventory management principles.

Our research explored the application of a localized model to ease the pressure on the distribution and transportation networks. Such a model assumes that individual enterprises take it upon themselves to build a response capability, and collaborate with government institutions to better plan and coordinate actions to prevent massive economic and physical impacts from an episode. However, we were unable to determine exactly what form of stockpiling approach was in place at federal and state agencies today, and multiple interviews led us to believe that, if they do exist, the policies were not well communicated to impacted parties. As such, we again assigned a preparedness Level 2 to federal agencies based on our assessment of their current preparedness.

Assessing Supply Chain Education and Training

Every federal agency has some form of an emergency response website, which typically lists information on what staff should do in the event of an emergency. In many cases, these websites simply direct individuals to the local authorities. However, it appears that there are few internal training programs in place to ensure that critical federal services, including IT infrastructures, are truly prepared for a massive reduction in human resources and disruptions

Operation of the Strategic National Stockpile (SNS)

In addition to vaccines, the SNS includes the following categories of supplies that are used to combat different types of medical and threats:

- Antibiotics
- Chemical antidotes
- Antitoxins
- Life-support medications
- IV administration
- Airway maintenance supplies
- Medical/surgical items

The first line of support from the SNS is in the form of 12-hour push packages. These push packages are positioned in strategically located, secure warehouses and are ready for immediate deployment to a designated site within 12 hours of the federal decision to deploy SNS assets. While HHS manages the procurement and storage of the vaccines, CDC has the responsibility of distributing it to the states³. According to another interview, the current inventory level at the SNS is 100 million masks and 20 million doses of vaccine. The SNS is seeking eventually to have 100 million doses of vaccines.

A number of questions remain regarding stockpiling policies for the SNS:

- Are SNS warehouses located for the optimal distribution of supplies?
- Is there a specific plan for the individual states (at a granular level) to receive and effectively distribute medical supplies?
- In the event of an outbreak, what is the required level of vaccines and masks needed, by state and by region?
- Is there a plan for localized stockpiles to serve community requirements, as opposed to using centralized distribution?

It is not clear that there are effective supply chain risk planning elements associated with these questions, and that they may indeed vary by state and by region.

to federal supply chains that would accompany such an emergency.

A handful of agencies have developed strong programs to emphasize teleworking, and others have begun to prioritize which services would be the first to be shut down in an emergency situation.

However, in the words of one authority, “there is a major disconnect on what the state can do, and how the individual agencies should work together to optimize resources that are at their disposal in the event of a major emergency.”⁶ There is some movement, however, to begin education initiatives, in the form of events that bring together different agencies on a broader scale through statewide teleconferences and video conferences. We believe that most federal agencies are at Level 1 preparedness.

Recommendations

Effective response to national emergencies are a recognized part of government's responsibility. Recent incidents include oil spills, hurricanes, tornadoes, pandemics, automotive product recalls, human and animal food poisoning, and a multitude of other events. Federal agencies are urged to think not so much about how to predict the next emergency, but to look forward and address where the impact of major events will hurt the most. Once supply chain nodes are identified, mitigation planning needs to occur to ensure that a creative and cost-effective solution is identified. There is much work to do.

A number of recommendations result from our preliminary assessment conducted for this report. They include:

- **Recommendation One: Governance is a critical foundation for emergency planning.** Every major public and private institution should be required to form some sort of planning committee to initiate the assessment and identification of mitigation plans. These committees should follow clear guidelines and implement action plans that would be put into effect upon the announcement of trigger points. Although this mandate is already in place, the degree to which agencies have been audited against the criteria shown in our framework is not clear. We believe that most of these plans are at a Level 1 or Level 2, are not robust, and potentially could fall apart should an incident arise.
- **Recommendation Two: Supply chain risk assessments should be carried out to map out key stakeholders and weak nodes within the responsibility of federal government agencies.** Agencies must work closely with private industry to carry out risk assessments and strategize

on risk mitigation plans. Supply chain mapping and risk analysis tools can be applied to identify potential failure points that could impact each agency's stakeholder community. Our research indicates that current systems in place could fail if large portions of the economy move to teleworking, and there are no firm plans in place to identify critical workers. For example, the Department of Agriculture could work more closely with fertilizer producers, food retailers and producers, farming communities, and logistics providers. Similarly, the Department of Veterans Affairs could work more closely with medical distributors to better plan distribution points.

Our recommendation is that federal agencies cannot operate in a vacuum, and cannot be relied on to be the sole planning group for an emergency. Guidelines should be developed in conjunction with industry groups to better understand current practices, implement improvements in planning, and identify mechanisms for coordination and key trigger points that can generate alternative actions.

- **Recommendation Three: Stockpile planning and allocation processes should be improved.** Rather than depend on the current approach of blanketing all areas, strategic stockpile placements—in coordination with risk planning—can provide improved outcomes. Further, we believe that coordination between the federal and state distribution of national stockpiles needs to be improved. Our research suggests that state-level distribution centers with pre-positioned stockpiles could provide an improved response and deployment of multiple forms of emergency supplies as well as redundancies in service

providers. Improvements in planning and inventory management should be encouraged in all cases to improve response time.

- **Recommendation Four: Training of key individuals in conjunction with risk planning is an important component to planning.** Some of the best forms of training involve simulated exercises in work-at-home scenarios, to gauge how effective workers will be if not physically located on site during an emergency. Training should emphasize lessons learned and gaps identified for risk mitigation and planning.

There is a need for significant additional research on this topic to better understand the gaps and limitations of different industries. Our research suggests that there is especially a need for research in the requirements for supply chain planning, strategic stockpiles of hospital and medical supplies, food distribution planning, and risk maps identifying sectors that are most exposed.

There is also a clear need for joint exercises with industry and training, so that collaboration between public and private entities can be forged, with specific actions and requirements for joint activity and triggers specified and agreed on, both horizontally and vertically, in key supply chains. We hope that this report serves to initiate this activity and illustrate the importance of better understanding the deployment of supply chains in response to a national emergency.

Endnotes

1. Interview with CDC official, July 14, 2008.
2. Leatherby, Drew. 2007. Pandemic Planning and Response for State IT: Where's My Staff? NASCIO. PDF is attached.
3. Osterholm, Michael. 2009. Presentation to the Centers for Disease Control and Prevention, Pandemic influenza: Public health's Waterloo?, Atlanta, GA.
4. <http://www.bt.cdc.gov/stockpile/>.
5. <http://www.cdc.gov/h1n1flu/cdresponse.htm>.
6. Interview with CDC official, July 24, 2008.

ABOUT THE AUTHOR

Robert Handfield, Ph.D., is the Bank of America University Distinguished Professor of Supply Chain Management at North Carolina State University, and Director of the Supply Chain Resource Cooperative (SCRC; <http://scrc.ncsu.edu>). He also serves as an Adjunct Professor with the Supply Chain Management Research Group at the Manchester Business School in the United Kingdom.

The SCRC is the first major industry-university partnership to integrate student projects into the MBA classroom in an integrative fashion, and has had 15 major Fortune 500 companies participating as industry partners since 1999. Prior to this role, Handfield was an associate professor and research associate with the Global Procurement and Supply Chain Benchmarking Initiative at Michigan State University from 1992-1999.



Handfield is the Consulting Editor of the *Journal of Operations Management*, one of the leading SCM journals, and is the author of several books on SCM, the most recent being *Supply Market Intelligence*, *Supply Chain Re-Design* and *Introduction to Supply Chain Management* (Prentice Hall, 1999, 25,000 copies sold, and translated into Chinese, Japanese, and Korean). He has co-authored textbooks including *Purchasing and Supply Chain Management* 3rd revision (with Monczka) and *Operations and Supply Chain Management* (with Cecil Bozarth).

In 2009, he was nominated as an Honorary Fellow of Contract & Commercial Management by the International Association of Commercial and Contract Management. The honor is bestowed on individuals who have made exceptional contributions in the field of contracting and commercial management. Handfield is regularly quoted in and has published op ed pieces, and is quoted in blogs and global news media such as the *Wall Street Journal*, the *Financial Times*, the *San Francisco Chronicle*, *Spend Matters*, Microsoft Live, Ariba Live, Inc., *CIO*, *CFO*, the *Supply Chain Management Review*, and other media.

Handfield has consulted with over 25 Fortune 500 companies, including GlaxoSmithKline, Freightliner, Boston Scientific, Delphi, Chevron, British Petroleum, Nortel Networks, Chevron Phillips, Lyondell Chemical, Conoco Phillips, Federal Express, Milliken, and others.

He has published more than 100 articles in top management journals including *California Management Review*, *Sloan Management Review*, *IEEE Transactions on Engineering Management*, the *Journal of Product Innovation Management*, the *Journal of Operations Management*, and *Decision Sciences*.

KEY CONTACT INFORMATION

To contact the author:**Robert Handfield**

Bank of America University Distinguished Professor of Supply Chain Management
Department of Business Management
College of Management
North Carolina State University
Raleigh, NC 27695
(919) 515-4674

e-mail: robert_handfield@ncsu.edu

blog: <http://scm.ncsu.edu/blog>



For a full listing of IBM Center publications,
visit the Center's website at www.businessofgovernment.org.

Recent reports available on the website include:

Collaborating Across Boundaries

Designing and Managing Cross-Sector Collaboration: A Case Study in Reducing Traffic Congestions by John M. Bryson, Barbara C. Crosby, Melissa M. Stone, and Emily O. Saunoi-Sandgren

Contracting and Acquisition

The Challenge of Contracting for Large Complex Projects by Trevor L. Brown, Matthew Potoski, and David M. Van Slyke

Fostering Transparency and Democracy

Using Geographic Information Systems to Increase Citizen Engagement by Sukumar Ganapati

Improving Healthcare

The Role and Use of Wireless Technology in the Management and Monitoring of Chronic Diseases by Elie Geisler and Nilmini Wickramasinghe

Creating Telemedicine-Based Medical Networks for Rural and Frontier Areas by Leonard R. Graziplene

Improving Performance

Project Management in Government: An Introduction to Earned Value Management (EVM) by Young Hoon Kwak and Frank T. Anbari
Strategic Use of Analytics in Government by Thomas H. Davenport

Managing Finances

Strengthening Control and Integrity: A Checklist for Government Managers by James A. Bailey

Managing Risk in Government: An Introduction to Enterprise Risk Management (2nd Edition) by Karen Hardy

Strengthening Cybersecurity

Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers by Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, Linda Williams

Transforming the Workforce

Federated Human Resource Management in the Federal Government by James R. Thompson and Rob Seidner

Using Technology

Moving to the Cloud: An Introduction to Cloud Computing in Government by David C. Wyld

About the IBM Center for The Business of Government

The IBM Center for The Business of Government connects public management research with practice. Since 1998, we have helped public sector executives improve the effectiveness of government with practical ideas and original thinking. We sponsor independent research by top minds in academe and the nonprofit sector, and we create opportunities for dialogue on a broad range of public management topics.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value. For more information visit www.ibm.com.

For additional information, contact:

Jonathan D. Breul

Executive Director

IBM Center for The Business of Government

1301 K Street, NW

Fourth Floor, West Tower

Washington, DC 20005

(202) 515-4504, fax: (202) 515-4375

e-mail: businessofgovernment@us.ibm.com

website: www.businessofgovernment.org