Securities Industry and Financial Markets Association

Business Continuity Planning

Critical Infrastructure Guide

February 2007

The SIFMA Business Continuity Committee, Critical Infrastructure Subcommittee compiled this guide to serve as a template for firms to use in developing relationships with critical infrastructure providers in their regions and to better understand the resiliency of these providers. This Guide is published as a source of information for SIFMA member firms. The material herein is not to be construed as legal advice or opinion and should not be relied upon as an authoritative statement of applicable laws, rules and regulations.

Table of Contents

Critical Infrastructure Sub-Committee Mission Statement

Working with the SIFMA, industry regulators and other governmental agencies, the Critical Infrastructure Sub-Committee will ensure that the concerns of the financial community, especially as they relate to critical infrastructure resiliency, life safety, security, disaster preparedness, property operations, and building code modifications are properly articulated. These issues are considered paramount to successful operations and urban renewal initiatives in major municipalities throughout the nation, and integral to obtaining long-term commitments from the financial services sector.

What is Critical Infrastructure

Infrastructure includes a broad spectrum of services that incorporates public utilities, transportation systems and private sector service providers. Common infrastructures that are typically grouped include transportation, water, waste, energy,(tele)communications, emergency management and, may also include resources (personnel, land,buildings).

Infrastructure can relate individually or collectively to a system, organization or community.

When defining Critical Infrastructure one would include those parts of the infrastructure that are so vital that disabling any part of them would incapacitate the system, organization or community.

Government Initiatives

Emergency and disaster preparedness begins at home with each individual and with each individual company. The government has many initiatives for infrastructure protection and mitigation but individual businesses must take responsibility for creating and managing contingency plans for their own infrastructure or dependence on public infrastructure.

To improve the reach and effectiveness of government initiatives, firms need to take the first step in determining what is available for their business. Reach out to local and regional government officials to see if they have public-private contingency plans for protecting infrastructure. If not, the next step is to check for plans with the state government and of course, the federal government.

There are a number of ongoing public-private initiatives throughout the country that directly or indirectly support efforts to increase the protection of critical infrastructure. These initiatives are varied. They range from the major integrated program developed in New York State and New York City to the basic Emergency Support Function-Eighteen (ESF-18) created in

Florida, as well as a very area-specific plan developed for the Dallas Central Business District and titled “The Downtown Dallas Emergency Response Manual” to the King County regional plan detailed in the “Regional Disaster Plan for Public and Private Organizations in King County Washington”.

This section describes key initiatives from the Department of Homeland Security and provides examples of local, regional, state and city plans.

Federal:

--Department of Homeland Security (DHS)

In the aftermath of the terrorist attacks against America on September 11th, 2001, President George W. Bush established the Department of Homeland Security to coordinate the efforts of 22 domestic agencies in an effort to protect the nation against threats to the homeland.

The department's first priority is to protect the nation against further terrorist attacks. Component agencies analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of our nation for future emergencies.

DHS is also dedicated to protecting the rights of American citizens and enhancing public services, such as natural disaster assistance and citizenship services, by dedicating offices to these important missions.

Homeland Security Council Executive Order:
www.whitehouse.gov/news/releases/2002/03/print/20020321-9.html

DHS Border and Transportation Security agencies:

- The U.S. Customs Service (Treasury)
- The Immigration and Naturalization Service (Justice)
- The Federal Protective Service (GSA)
- The Transportation Security Administration (Transportation)
- Federal Law Enforcement Training Center (Treasury)
- Animal and Plant Health Inspection Service (Agriculture)
- Office of Domestic Preparedness (Justice)

--DHS Emergency Preparedness and Response agencies:

- The Federal Emergency Management Agency (FEMA)
    - FEMA is the independent Federal agency responsible for leading America’s efforts to prepare for, prevent, respond to, and recover from disasters. FEMA is first and foremost a coordinating agency. The Agency relies on strong partnerships to successfully carry out its mission. FEMA works with a variety of partners, including Federal agencies, States, Territories, Tribal Nations, local governments, first responders, voluntary organizations, business, industry, and individuals. While the Agency’s mission is squarely focused on protecting and preparing the Nation as a whole, primary responsibility for disaster response rests with State and local authorities. This means that FEMA does not respond to all disasters that occur in the United States. Instead, when State and local

capacity to respond is threatened or overwhelmed, a Governor may ask the President for Federal assistance. A Presidential disaster declaration directs FEMA to provide and coordinate a variety of assistance and support. FEMA's primary mechanism for doing this is the Federal Response Plan. It provides a process and structure for the systematic, coordinated, and effective delivery of Federal assistance to address any major disaster, regardless of type or cause. Through the Federal Response Plan, FEMA marshals the resources and expertise of its many partners, including Federal agencies and numerous voluntary organizations, and coordinates the overall effort with the States and communities affected by the disaster.

- Strategic National Stockpile and the National Disaster Medical System (HHS)
- Nuclear Incident Response Team (Energy)
- Domestic Emergency Support Teams (Justice)
- National Domestic Preparedness Office (FBI)

--DHS Science and Technology agencies:
- CBRN Countermeasures Programs (Energy)
- Environmental Measurements Laboratory (Energy)
- National BW Defense Analysis Center (Defense)
- Plum Island Animal Disease Center (Agriculture)

--DHS Information Analysis and Infrastructure Protection agencies:
- Critical Infrastructure Assurance Office (Commerce)
  - Coordinates the Federal Government's initiatives on critical infrastructure assurance
    - Coordinates and implements the national strategy
    - Assesses the Government's own risk exposure and dependencies on critical infrastructure
    - Raises awareness and educates public understanding and participation in critical infrastructure protection efforts
    - Coordinates legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors
  - Critical Infrastructure Sectors' Information Sharing and Analysis Centers (ISACs)
    - Agriculture
    - Food
    - Water
    - Public Health
    - Emergency Services
    - Government
    - Defense Industrial Base
    - Information and Telecommunications
    - Energy
    - Transportation
    - Banking and Finance (FSISAC)
    - Chemical Industry and Hazardous Materials

    - Postal and Shipping
- Federal Computer Incident Response Center (GSA)
- National Communications System (Defense)
- National Infrastructure Protection Center (FBI)
- Energy Security and Assurance Program (Energy)

Regional Example:

--King County, Washington

King County's "Regional Disaster Plan for Public and Private Organizations" provides a framework for inter-linking emergency response plans. By clarifying "who is going to do what", the plan coordinates public, private and non-profit organizational strategy following an emergency. The focus is exclusively on disaster response while providing a framework for future efforts to address regional mitigation, preparedness and recovery issues.

Participation in the Regional Disaster Plan is voluntary. All participants, however, are required to prepare and plan for disasters. Responsibilities include: developing an employee care plan; improving facility and equipment vulnerabilities; response plans; participation in mutual aid agreements; mechanisms for proclaiming emergencies; participation in creating Emergency Support Functions (ESFs); preparedness education; commitment for emergency support; etc.

Presently the "Basic Plan Package" consists of the Plan; the Omnibus Legal and Financial Agreement; Appendix One; Emergency Support Function (ESF) 1 – Transportation; 2 – Communications; 7 – Resource Support; and 8 – Health and Medical services.

For more information on King County's preparedness efforts, visit www.metrokc.gov/prepare.

State Examples:

--New York

---NYS Office Of Public Security (OPS)

OPS coordinate with all agencies and resources of State government on matters relating to terrorism prevention, response, and recovery. These resources include the Division of the State Police, Division of Naval and Military Affairs, State Emergency Management Office, Department of Health, Department of Environmental Conservation, Division of Criminal Justice Services, Department of State, Office of Technology, and the Department of Transportation. The Office is New York State's Primary contact with the National Office of Homeland Security. Maximum preparedness for a possible terrorist act or threat will be the result of the coordination strategy and effort.

OPS is charged with coordinating and enhancing anti-terrorist efforts in the State of New York, specifically with developing a comprehensive statewide strategy to detect, protect against, respond to, and prevent cowardly and murderous acts of terrorism.

--NY State Emergency Management Office (SEMO)
SEMO is responsible for coordinating all activities necessary to protect New York' s communities from natural, technological and manmade disasters and other emergencies that threaten the State. SEMO coordinates emergency management services for the State by providing leadership, planning, education and resources to protect lives, property and the environment.

--Major Programs:

- Citizen Corps
- Chemical Preparedness
- Disaster Recovery Assistance
- Emergency Alert System
- Emergency Communications
- Emergency Management Performance Grant
- Media & Public Information
- Emergency Stockpile Equipment
- Emergency Operations
- Legal
- Mitigation
- Planning
- Radiological Preparedness
- Training & Exercises

--NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)
CSCIC was established in September 2002 by Governor Pataki for leading and coordinating New York State's efforts regarding cyber readiness and resilience; leading and coordinating geographic information technologies, especially in emergencies, where CSCIC is the single point-of-contact; coordinating the process by which State critical infrastructure data is collected and maintained; expanding the capabilities of the State's cyber incident response team; and monitoring the State's networks for malicious cyber activities. CSCIC also coordinates closely with Office of Public Safety to ensure that the information sharing and communication required to secure New York State’s assets are maximized.

---Florida
The Emergency Support Function-Eighteen (ESF-18) position was created in Florida to aid with the coordination of communication between city and county emergency officials, and community business leadership. In most instances, the position is not sponsored by individual companies, but by business continuity organizations such as Association of Contingency Planners (ACP). Having ESF-18 for Business and Industry allows for direct communication with City and County Emergency Operation Centers in times of crisis. Businesses are kept apprised of crisis information and expected government actions that affect business operations.

While the ESF-18 position is a representative of business and has the primary responsibility of communicating with business, it is also a member of the EOC and, as such, does have certain responsibilities to that organization. The ESF-18 representative must also agree to man the EOC when necessary, participate in City/County emergency drills, keep appropriate supporting documentation for the position updated, backup other ESF's when requested, and perform any direct request by the EOC leadership.

Examples of EFS-18 can be found at www.floridadisaster.org.

--Local examples:

<u>---New York City (NYC)</u>

<u>---NYC Office of Emergency Management</u> (OEM)

OEM's mission is to provide the highest level of emergency preparedness to the citizens of New York City as they face new challenges in the 21st century. Working as inter-agency coordinators in partnership with local, state, federal and private entities, OEM seeks to provide comprehensive emergency response, hazard planning and disaster mitigation to New York City.

---Preparing for Emergencies:

- Health and Medical
- Human Services
- Recovery and Mitigation

  The Recovery and Mitigation Unit is responsible for planning associated with recovery operations, such as debris management, damage assessment, and infrastructure reconstruction. On the mitigation side, the unit performs proactive sustainability studies that seek to lesson the impact of future disasters and works with City agencies to implement measures to protect their facilities against disaster related damages.
- Geographical Information Systems
- Homeland Security

  Following the terrorist attacks of September 11th, OEM enlisted the services of a Police Department Deputy Inspector and Fire Battalion Chief who liaison with City, State and Federal agencies involved in homeland defense and ensure the coordination of the City's counter-terrorism planning efforts.

---Operations:

- Watch Command

  OEM Watch Command serves as the communication hub for the agency. Staffed 24 hours a day, 7 days a week, Watch Commanders monitor the radio and computer aided dispatch systems of the City's public safety agencies, and maintain a communications link with City, neighboring county, State, and Federal agencies, private non-profit organizations, utility providers and hospitals. Watch Commanders notify agencies of emergencies to ensure the full resources of the City are available to support response operations. In addition, Watch Commanders monitor meteorological conditions to identify weather events that may impact the City.

- Field Response
  OEM is responsible for coordinating the interagency response in the event of an emergency or disaster by responding to the scene of an emergency, assessing the situation, coordinating requests for resources and acting as a liaison between the Incident Commander and the agencies involved in the response.

- Emergency Operation Center
  The EOC – a crisis command center activated by the Mayor and managed by OEM – serves as the central coordination point for agency and resource response in a serious or potentially serious emergency. With space for 50 to 75 representatives of City, State and Federal government agencies, the EOC acts as a central clearinghouse for information sharing. The EOC Program bridges the public and private sectors by allowing private sector representatives in the City's EOC.

--Public-Private Emergency Planning Initiative (PEPI):

PEPI is an initiative designed to strengthen private sector relationships and increase the City's preparedness level. Through this program, private businesses receive help developing business continuity plans, participate in exercises and receive basic emergency management support as it relates to New York City. PEPI also offers two main components that support the private sector:

- CorpNet Information Sharing Program: OEM offers the CorpNet information service, which provides business partners with current, accurate information about emergencies to enhance awareness and aid decision-making should their businesses be affected. OEM monitors public safety radio and information networks, news media, and commercial and proprietary weather systems through its Watch Command -- Watch Command uses the OEM paging system to forward relevant messages to CorpNet subscribers. When an incident reaches a specified emergency threshold, OEM dispatches a "responder" to verify the event and facilitate interagency coordination onsite. This process enhances CorpNet's accuracy, as information comes directly from the scene via the OEM responder. Subscribers, who are typically crisis management, business continuity and security executives may also receive information regarding incidents OEM monitors, but does not necessarily respond to.

- Private Sector involvement at Emergency Operations Center (EOC): Because the EOC cannot accommodate individual companies, major business associations, which represent the City's critical industries — serve as liaisons for private sector partners. These liaisons provide members with up-to-the-minute information about emergency situations using predefined contacts and e-mail trees from their EOC workstations.

Association members can communicate with OEM through their EOC representatives via Internet or by telephone.

--Current industries/associations represented at the EOC include:

- Securities – Securities Industry Association
- Banking – New York Clearing House
- Commercial Real Estate and Building Management – Building Operators & Managers Association and Real Estate Board of New York
- Tourism – Hotel Association of New York City

For more information on New York City's public-private initiatives, visit www.nyc.gov/oem.

--Downtown Dallas, Texas

"The Downtown Dallas Emergency Response Resource Manual" is a general guideline of responsibilities for responding municipal agencies during a critical incident. To help with planning, mitigating and responding to emergencies, the manual describes possible interactions between first responders and the private sector. It also includes examples of best practices for reducing risk and increasing response and recovery capabilities.

--Subjects in the Manual include:

- Existing Emergency Management Plans
    - The City of Dallas Master Emergency Operations Plan
    - Emergency Management
    - The Dallas Building Owners and Managers Association Guidebook
    - The Emergency Management Guide for Business and Industry – American Red Cross
- Communications
- Perimeter Access Procedures – general procedures for the secured boundary around the site of a critical incident.
- Damage Assessment Criteria
- Agency Responsibilities – description of incident roles and responsibilities for municipal government and specific non-governmental agencies.
- Private Sector Guidelines – public/private partnerships
- Preparation of Recovery and Restoration Plans – recovery process advice
- Training, Drills and Exercises
- Emergency Preparedness Kits
- Identifying Building Access Levels – general access guidelines

Guidelines for Specific Critical Incidents – general response from public safety responders during emergencies

For more information on Downtown Dallas' emergency preparedness efforts, visit www.dallasalert.org.

Identifying Critical Infrastructure Utilities That Serve Your Facilities

There are several options you can use to get in touch with your utilities to establish the working relationships you need to help you through real or potential service interruptions. Your first stop should be your own facilities management and / or accounts payable offices. The facilities management staff may already have contacts you can use to open the door to a business continuity planning partnership with your service providers. A review of the utilities and telecom bills, through the accounts payable office, may also identify an assigned account representative to develop an initial relationship.

The next contact should be the local government Office of Emergency Management for your jurisdiction(s). Depending on the state in which you are located, this could be either a municipal or county function. Public sector planning standards require the development of emergency operations plans and these typically have contact information for key providers of electric, gas and water services. If your jurisdiction does not have an active emergency management program, other sources of local government referral assistance are the fire and police departments. You may also find that utility service is provided through government run water or power companies (utility authorities).

A third option is to contact trade associations specific to gas, water and power purveyors. These are usually at the state level and affiliated with national associations. You also have the option of contacting the state government agency that has regulatory authority over utility providers. Finally, the telephone directory and internet websites can be effective in providing the first point of critical infrastructure utility contact.

As a sample list, your organization should obtain contact names and phone numbers of key providers such as:

- - Electric
- - Steam Power
- - Fuel for backup generator
- - Environmental protection department
- - Water
- - Land Line telephony providers
- - Wireless Telephony providers
- - Transportation (Bus, Subway, commuter railroads, express buses)

Setting up an Initial Meeting

The best approach in making the initial contact with the utilities is to communicate directly with the provider. Unless you've gotten a specific referral from your facilities management team or a local government representative, you will probably reach somebody in the customer relations department. You may find that you are the first customer to ask questions about reliability, restoration and forming a crisis management partnership. However, you may also find that the utilities are already part of a Local Emergency Planning Committee and that mechanisms already exist to share information before, during and after emergencies occur or threaten. In any case, you should ask to speak with the person responsible for business continuity, crisis or emergency management.

You should be prepared with some non-threatening examples of the type of information you are seeking. If you present yourself as needing information to help in developing a plan, then some of the generic questions below could be used. You may also want to refer to regulatory guidelines or business continuity requirements that necessitate planning with critical infrastructure providers. Don't take an initial negative response as being final. Let your contact know it won't take much time and that you would be happy to set the initial meeting at his / her convenience and office.

following are some generic questions you might use as a guide in planning your initial conversation with a utility.

- For this area, how many distribution points do you have?
- Is it possible to run alternate supply lines to our facility (i.e.) located at _________?
- Can these alternate supply lines be routed into our facility via an alternate entry point?
- What redundancies does your supply network have built into it to avoid service interruptions?
- How do you advise your customers of service disruptions?
- Do you have contingency plans?
- What scenarios do your contingency plans cover?
- What are the recovery time objectives you intend to meet for your services?
- Does your service originate from one central source that may create a single point of failure?
- Do you have an alternate facility if your primary location is impacted by a disaster?
- Do you report any significant challenges to any external organizations?
- Do you have any partnerships / service level agreements with another service provider in order to continue providing service to your customers?
- Are there priorities to resuming operations, i.e. by service or industry?
- Is there any possibility of receiving a priority in terms of service restoration?
- Would you be willing to pass along information regarding the scope and expected duration of interruptions?

Goals of Meeting with your Critical Infrastructure Providers

The obvious goal of meeting with your critical infrastructure providers is to get an understanding of their crisis management capability. Good information will allow you to set a realistic recovery time objective for outage scenarios involving their services. This information will also let you better understand their interdependencies.

Some other goals and their benefits are:

1. Establish an ongoing relationship with your counterpart at the service provider. This can provide a different perspective on issues that affect you both and better prepare you for business interruptions. Such a relationship could be the difference between getting access to good information at time of disaster and getting only that information available to the general public.
2. Get involved in crisis management tests conducted by the service provider. These tests can be an opportunity to illustrate for your management the importance of information sharing and the value of the business continuity planning process. They can also illustrate to your internal clients the depth of your company's dependence on external resources.
3. Attempt to provide a service back to your service provider. Your organization may be able to provide important information about the critical infrastructure provider's service to your own employees when emergencies occur, e.g. what to do when there is a telecom, power or water outage.
4. Understand any vulnerability associated with the service provider and opportunities to improve your company's resiliency by mitigating the risks.
5. Understand the service provider's operating strategy and position within any larger regional or national infrastructure. When your building is down, it can be very important to be able to explain to your senior management what is going on and what are realistic expectations for service restoration.

Use of Information Obtained

After you have identified your Critical Infrastructure Providers and met with them, the question becomes "What do you do with this information?" The answer begins with goal number 4 of the previous section:

> "Understand any vulnerability associated with the service provider and opportunities to improve your company's resiliency by mitigating the risks."

The best way to understand any vulnerability to your operations is to systematically identify where the gaps between your vendor's crisis management capabilities end and your contingency program begins. Thus a "Gap Analysis" should be performed.

A Gap Analysis can be relatively simple and straightforward; Armed with the results of your vendor interviews and surveys, you can perform a gap analysis against the Best Practices for Critical Infrastructure, which follow in the next section of this manual. These Best Practices were initially developed for financial institutions, but have wide applicability to firms that *service* the financial industry. In addition, best practices for specific industries have been developed to highlight specific concerns related to that industry.

Once your Gap Analysis is complete, *risk mitigation* begins. Risk mitigation is nicely defined as follows:

> "Risk mitigation is the planning process in which you try to think of ways to prevent your identified risk from ever occurring, while at the same time coming up with a means of recovery should the risk become a reality in spite of all efforts"*.

During risk mitigation, you must weigh the chances of an identified gap actually causing serious disruption to you operations vs. the cost to mitigate it. Each firm will have a different level of tolerance for these risks; however, the best practices that follow should give you a good indication of what the leading financial firms follow.

- www.labcompliance.com

Following are suggested questionnaires that have been developed as guides for addressing various infrastructure service providers.

Transportation Questionnaire

OVERVIEW

Part of our ongoing mission is to foster relationships with state, federal and private sector organizations that provide direct and indirect support to the financial community. As an integral part of this mission we hope to achieve the following:

- Allow for open dialog with the financial community through the SIFMA
- Have representatives come and speak on their protection planning and safeguard methodologies
- Form a communication relationship
- Enlist the support of the different sectors to participate in industry business continuity and incident management testing

MTA - PLANNING MANAGEMENT

Communications

- How does communication with the OEM take place?
- Can we create a central communications network for the financial community?
- Can there be an *"Early Planning"* mechanism to allow organizations to properly plan and execute strategies for this type of event?
- Can there be an early on definition of outages in both public and private sectors for rail and ground transportation?
- During this type of event, can the MTA website be updated more frequently?

Controls

- How are your command center(s) organized?
- Are there backup console command centers in place in case the primary is impacted by a disaster?
- How are contingency plans tested and with what frequency?
- What actions would be expected from organizations?
- Given the current environment, do you feel that any significant disruption in services would expand or lessen our risk to terrorism?

ORGANIZATIONAL PLANNING

Assessment

- Have you defined business timeline impacts?
- Have you identified employee demographics?
- Have you defined criticality ratings to events?
    - Describe theses ratings and the methodology used to define them.
- Have you planned for large-scale events?
- Describe the relationship with the other city; state (NJ/NJ/CN) and private service providers and what joint efforts currently exist.
- What particular exercises are performed to simulate MTA reactions to catastrophic events?

Staffing

- Have you identified the number of employees to be accommodated?

- Have you identified those employees with quality of life issues?

Containment

- Did you make hotel arrangements?
- Have you contracted for transportation (boats, buses, car services, parking facilities, etc.)?
- Have you arranged with facilities to accommodate alternate transportation means such as bikes?
- Have you identified and categorized business processes, and established shifts?
- When applicable, have you relocated functions to regional locations?

Communication

- Identify decision team
- Identify response team
- Establish an on-watch coordinator to:
  - Gather information from the internet
  - Follow news media reports
  - Communicate with command center contacts
  - Provide regular updates to the decision team
- Request employees to identify if they have alternate arrangements
- Provide continual updates to employees

Department of Sanitation (DOS) Questionnaire

General Organization:

1. What is the DOS responsible for?
2. Where does the DOS fall within the city government hierarchy?
3. Does the reporting line described above change during an emergency?
4. How many office type-sites does the DOS occupy in the city? All five boroughs?
5. How many other types of sites does the DOS manage (dumps, garages, etc.)?
6. How many DOS employees are there?
7. What types of technology does the DOS use? Where are the DOS data centers located?
8. Does the DOS have back up data center capability? If so describe the environment.

Recovery Program:

1. Does the DOS have a business continuity/disaster recovery organization? If not who fulfills this function?
2. To whom internally does this group report(IT, Administration, Audit, etc.)?
3. Does the DOS have business continuity plans, if so, what is the status?
4. Do DOS recovery plans include external relationships with vendors, partners, clients, etc.?
5. Have plans accounted for hardware and equipment?
6. Have plans accounted for data/vital records?
7. What is the overall DOS recovery strategy for providing continued service?
8. Has a business impact analysis been conducted within the DOS? What were the results for equipment or capability loss tolerance (20%, 50%, etc.)? Data loss tolerance?
9. Has a risk assessment been prepared to identify and mitigate existing risks to the facilities and operations of the DOS? What are the primary risks that the plans cover?
10. What is the outage length the plans address?

11. Have recovery requirements and recovery time objectives been identified and consolidated to understand the organization's needs? If so what are the recovery requirements and RTO's?
12. How are DOS recovery plans stored, distributed, and maintained?
13. Does the DOS have an OEM Command Center seat?
14. Does the DOS have and maintain their own Command Center(s)?
15. Does the DOS conduct Training and Awareness exercises for its employees?
16. Does the DOS have a testing program? If so what is the current testing status?
17. Are the facilities and infrastructures included within the recovery planning scope?

18. Does the DOS have liaisons appointed to coordinate plans with the other public city organizations?
19. Does the DOS have liaisons appointed to coordinate plans with external private firms?
20. What is the planning budget for the DOS?
21. Has the DOS engaged any BCP consulting firms or planning tools?
22. What percentile of DOS employees has access to the plans? Have been trained in the use of the plans? Or are involved in plan development?

Private Industry Related:

1. If a firm were to perform a building lock down, what is the sanitation issues that they would have to consider (waste disposal / employee health)?
2. Are there general timelines that could serve as guidelines for when these issues become a health problem?
3. How are the waste/sewage street infrastructures managed and at what point generally does the ownership of that infrastructure become the responsibility of building management?
4. Generally, what types of impacts can the disruption of waste removal and sewage functions have on building occupants and the ability of private industry to operate?

Incident Response Related:

1. Does the Dept. of Sanitation have an internal problem escalation process in place?
2. At what point does the incident get escalated either to public orgs. (OEM) or to affected building managements? How are these external contacts managed?
3. Does the DOS have site evacuation plans?
4. How does the DOS propose to establish internal and external communications during an incident?
5. What type of events would cease DOS operations relating to waste removal, garbage collection, etc?
6. During a citywide declared disaster, does the DOS put its resources under the control and management of the OEM?
7. Are there other roles the Dept. of Sanitation assumes during a declared disaster or emergency?
8. Does the DOS have incident response guidelines regarding chemical or biological waste? What is it?
9. Does the DOS have incident response guidelines that deal with the inaccessibility of a percentage of both garbage dumps and waste removal equipment?
10. If the DOS in unable to operate at an acceptable level of business, what happens? Are waste removal objectives prioritized?

Steam Power/Utility Questionnaire

- What is Steam Power and is it still in used in (specify city)?
- What is the source of steam used in (specify city)?
- Could you describe the number of sources and the levels of redundancy designed in to the source feeds?
- How is steam delivered to the consumer?
- In the event of loss of a source, can other sources take over without a loss in capacity?
- Are there any other available options for sourcing steam locally?
- Could describe the dependency on other utilities (electric, water) to deliver steam to your customers?
- Could you describe the disruption caused to the steam system source and distribution following the recent events of 9/11and the 8/2003 Blackout?
- Can you discuss both recovery and contingency plans for the source steam system and distribution mechanisms in place today?
- Have any changes been made to the steam system delivery or restoration process as a result of these recent events?
- In the event of a service interruption, how do you now inform the consumer(s) of the scale, impact, cause and restoration estimates of the steam services?
- Assuming widespread interruptions, would there be any benefit to passing information to a central industry source such as a specific command center?
- What priority does the utility place on steam service restoration vs. electric or gas supplies? And could you describe the inter-relationships?
- Where can I go to determine the locational relation between my critical location and the source or distribution systems?
- What are my risks in regard to being right next to a distribution line, a block away, a ¼ mile away?
- What is the long term plans for (your City) steam usage? Are there any conversion plans on the horizon?

- What are the steam industries plans for the next 3 to 5 years in regard to upgrades to the sourcing and distribution systems?

Electric Power/Utility Questionnaire

- Describe the relationship between the regional source power grid and the local distribution systems.
- Describe the redundancies and the related recovery capacity for both the source grid and local distribution networks.
- Describe the process of restoration for source grid outages.
- Describe the process of restoration for local network distribution outages.
- How many network areas are there in (specify city)?
- Describe the inter-relationships between each network segment and the source feeds.
- Does your infrastructure meet basic standard contingency requirements for route grid design?
- What are the recovery time objectives for restoring impacted operations in any given area?
- What are the recovery time objectives for restoring impacted operations in any given network?
- Describe the restoration priorities to resuming plant and network operations.
- Describe the restoration priorities to customers – both business and residential.
- Describe the criteria for rating in terms of service restoration.
- Where does the financial services industry rank in the priority restoration scheme?
- How do you currently inform clients of a service interruption and the estimated time for restoration?
- Describe the types of service disruptions, planned or unplanned, that (specify city) could possibly experience.

- Could you provide a list of outages, type of outage and length of disruption that have affected (specify city) during the last 12 months?

- Describe and interpret the Reliability Indices used by (specify).

- During an outage, would you be willing to pass along information regarding the scope of interruptions to a central industry source, e.g. a Securities Industry Association BCP Command Center?

- Are the various local and regional power utilities cooperating in terms of providing emergency service? If so, in what way? If not, what are the concerns surrounding the lack of cooperation?

- Would you be willing to provide schematics to select individuals and/or organizations on a non-disclosure basis?

- Could you share your lessons learned from the events of 9/11 and the regional outage of 8/14/03?

- Are you familiar with the "Critical Infrastructure Assurance Guidelines for Municipal Governments" document written by the Washington Military Department Emergency Management Division? If so, would you describe where (specify city) stands in regard to the guidelines set forth in that document?

Dept. of Environmental Protection Questionnaire
(Water, Sewer, Air)

- Explain the mission, responsibilities and jurisdiction of the (specify city) DEP.
- Detail the sources of and the distribution systems for:
  - Water
  - Waste disposal
- Explain the impact to the city due to the loss of:
  - Water
  - Sewer treatment
  - Air quality
- What contingency plans are in place to deal with the above?
- What is the effect on capacity to (specify city) in the event of a loss of a source point?
- How does the DEP monitor the quality of these services?
- Explain the DEP monitoring.
- Is there a "watchdog" organization ensuring that monitoring is done to specific guidelines?
- If so, please provide the name of that organization.
- If not, what documentation is available to indicate is performed both according to schedule and according to DEP guidelines?
- Describe the safeguards in place to assure water, sewer and air quality?
- Have any changes been made to the Water, Air, and Sewer systems as a result of 9/11?
- Have you established a rating system for priorities in restoration of services?
- Assuming a service interruption, how do you inform the consumer(s) of restoration estimates?
  - During an outage, would you be willing to pass along information regarding the scope of interruptions to a central industry source, e.g. a Securities Industry Association BCP Command Center?

DEP Questionnaire for Facilities Planning/Building Management

· How many water service connections (domestic, fire) does your building have? Size? Location? Operational status?

Understanding Interconnections between domestic service lines within building?

· Does you building have a water storage tank(s)?
-- If so, where is(are) the tank(s) located? What is its capacity?
-- How long will a full tank be able to supply domestic water during a normal business day / after hours?
-- Is it a gravity feed or pressure system?
-- Does the tank provide water to the entire building or does street pressure supply a portion of the building also?

· Does you facility have the ability to accept water hook-up from a "fire hose" connection? (connection must be on the house side of the water service main valve - isolates the house from the mains in the street)

· Identify any critical functions within the facility (beyond the typical drinking, washing, sanitation, HVAC) that require water.

· Where are the buildings sewer connections?

· Do you have an internal/external notification plan for a water service disruption or sewer back up?

· If DEP walked into your building to provide notification of an emergency shutdown of the water, would the notification get to the correct people?

Fuel Oil Questionnaire

General issues

What is the capacity of the building(s) fuel tanks?

Does the generator(s) automatically start after a power outage? What is the delay? Is there a UPS system (batteries) between the utility power and the generator?

How long will the fuel tanks, at full capacity, keep critical services functioning?

What critical services will typically be on the generator and its consumption rate? Will it only be used for life safety (lights, elevator, fire pumps, etc.)? Have power consumption rates been identified to assist in prioritizing which services can be supported or remain on-line?

Do you perform Integrated Systems Testing (IST)? If so, how often and is the test with live load or simulated?

How frequently is the generator plant remediated i.e., are equipment parts changed out under a regularly scheduled replacement program? What is the longest timeframe the generators have been used in a "live" event?

What is the re-fuel requirement? At what capacity must the tank be re-filled (e.g., < 75%)?

Is the fuel "turned over" to keep it fresh (e.g. with a fuel polishing system)?

Is a dedicated support team in place for any emergency generator/Mechanical Electrical and Plant issues?

Is a sample of the fuel tested periodically by independent labs to ensure it is the proper quality (#2 low sulphur fuel)?

Security Issues

Is there remote monitoring of the fuel storage facility (for fuel levels and spill containment leaks)?

Is there a Spill Containment & Control Plan (SPCC)? If so, who approves it and when was it last reviewed?

Are there CCTV monitors/cameras in the area?

Where are the tanks located, indoors (basement, roof, etc.) or outdoors (parking lot, etc.)?

How is the fuel storage area secured and protected? Is the fuel tank protected by earth berms or concrete filled bollards for external security? Are Access Fill Valves locked up?

Are there any local building codes that limit or restrict the location of the tanks, amount of fuel that can be stored onsite and the noise limit (in decibels)?

Supplier issues

Do you have multiple suppliers under contract? Do you have priority standing with these contracts?

How many suppliers are there in the region?

Are Regional backup fuel vendors contracted for?

Is there an SLA with the supplier for delivery time and quantity?

How many trucks does your supplier(s) have?

How many clients in the same vicinity?

Do they get their fuel from multiple depots?

What is the supplier's capacity?

Do the contracts and Manifesto specify quality fuel (#2))

Can the supplier pump fuel into trucks during a power outage which impacts their operations?

Does the supplier have any arrangements for access with the various public sector agencies (e.g., emergency management, police, fire, etc.)

Medical/ Bio Terrorism Questionnaire

	Question
Disaster Recovery Questionnaire	1. Are you prepared to respond to a Medical or Bioterrorist Event?
	2. Has your firm/ municipality/ agency developed a formal plan for responding to a medical or bioterrorist event? • Are you familiar with the DRI (Disaster Recovery Institute) guidelines for what must be addressed in a DR Recovery Plan?
	3. Are you familiar with the Center for Disease Control definitions of Disease, Chemical and Bioterrorist agents? • What containment safeguards do you have in place? • What protective gear will your staff be provided to ensure they are able to function during the emergency?
	4. What medical emergency resources do you have under contract should an event occur and a triage team be required on site? • What hospitals/ medical facilities have you established relationships with which can be looked to for support in an emergency?
	5. What networking and joint planning has been done with Federal government agencies to accelerate mitigation of a crisis?
	6. If quarantining is required, what provisions have been made for space in which to quarantine impacted individuals?
	7. What tests do you perform to verify and improve your processes? • Frequency? • Controls? • Metrics?
Perimeter Security	8. What are your standards for securing and safeguarding your facility Perimeter
Please Note: The interest in HAZMAT (hazardous materials) is two fold. First, accidents can occur releasing the hazardous materials in areas where employees could be impacted. Next, if HAZMAT vehicles are hijacked, they can become weapons in the hands of terrorists.	
	9. Are you aware of the signage and package designations for hazardous materials which could be released in your vicinity? See Emergency Response Program, Identifying Hazards, US EPA
	10. Are you aware of any hazardous material (HAZMAT) development, manufacturing, reclamation or transit that is occurring within a mile radius of our proposed or existing site located at ___________________________?
	11. Are you aware of any HAZMAT storage facilities within a mile radius of the site? • What type of HAZMAT? • What controls are in place at the storage facility to ensure compliance with government regulations? • What mitigation/ containment disaster recovery plan is in place to respond to emergencies?

	12. Are you aware of any truck or railroad yards in the vicinity where HAZMAT is loaded and unloaded for transit purposes? • If so where? • How far are they from the site in question?
HAZMAT in the Area	13. Are there known issues with hazardous materials having entered the water table or soil, where the EPA has issued reported findings or is investigating? (Situations like Love Canal EPA History - Love Canal) • If so, how far is the contamination from our proposed/existing site?
	14. Are there any known issues where hazardous materials have been aerosolized and become airborne or drifted in a cloud? • What are the prevailing wind patterns? • Is the area subject to inversion layers or Fog?
	15. Are you aware of any SUPERFUND cleanups underway in the vicinity of our site? Emergency Response Program, Community Right-to-Know, US EPA
Radiological Events ——— **Preparedness and Mitigation**	16. In the event of a nuclear accident or terrorism such as a dirty bomb, do you have a stock of potassium – iodide you can distribute? http://www.nrc.gov/what-we-do/regulatory/emer-resp/emer-prep/potassium-iodide.html
	17. Are you familiar with the information provided in FEMA's site, Radiological Emergency Preparedness Program http://www.fema.gov/rrr/rep/
Medical and Bio-Terrorist Events ——— **Preparedness and Mitigation**	18. Please describe in detail your level of preparation for Medical emergencies, attributable to acts of nature, accidents or bio-terrorism • Epidemics, Infectious diseases • Poisoning due to water contamination • Poisoning or injuries due to airborne particulate matter • Exposure to chemical or bioterrorist agents • Burns due to chemical explosions, fires or other accidents • Crush injuries due to building collapse or acts of nature (e.g. tornados, earthquakes, hurricanes)
	19. Please describe how your mitigation plans are tested and what controls are in place to monitor performance and ensure continuous refinement of your processes
	20. Please describe known areas of vulnerability and your action plans to address them
	21. Please describe any actual events that have tested your processes and the lessons learned
	22. Do you have a secondary source of water should the public water supply be compromised?

Medical and Bio-Terrorist Events ——— **Preparedness and Mitigation**	23. Are you equipped with back-up emergency communications infrastructure necessary to maintain contact with partners, local fire and police, and government agencies if commercial power and the public telecommunications network is unavailable?
	24. Please describe your triage processes for handling large scale events producing high volumes of injuries or individuals needing medical intervention • Do you have established relationships with local, state and federal agencies? • Do you have documented procedures you would provide to Securities firm stakeholders in your vicinity/ jurisdiction to ensure seamless interfaces at time of event? • Do you have the infrastructure (e.g. shuttles, ambulances, EMTs, communication systems) to support triage and/or quarantine and containment?
	25. Do you have in-house resources committed to mitigating/ managing through Medical and Bio-Terrorist events?
	26. How would you fulfill your responsibilities to local clients/ stakeholders and ensure they receive necessary critical services if your facility was within the radius of the event? • What reciprocal or contingency plans do you have in place? • How do you educate your clients/ constituents on what to do if your site is shutdown?
	27. What else should we know to partner with you effectively and to ensure the safety of our employees in your vicinity?
Public Domain Information	28. Are you familiar with the PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002 http://www.epa.gov/safewater/security/security_act.pdf
	29. Are you aware of the US EPA Emergency Response Program? Have you been trained on what to do? Emergency Response Program, Recognizing Releases, US EPA

Landline Telecom Questionnaire

- What are your available circuit (landline) capacities in each major urban region in the U.S.?
- Could you describe the regional breakdowns / diagrams of your services.
- Describe the Signaling System 7 resiliency in the New York / New Jersey area.
- Describe the capacities and relationships of the Tandem switches in the New York / New Jersey area.
- Describe the recovery capability and capacity built in to the network.
- Describe your network monitoring abilities. Are all facilities proactively monitored?
- "Describe your Change Management practices as they relate to network monitoring, maintenance, equipment and software releases?"
- How are switching stations/central offices set-up for resiliency?
- How often is this resiliency tested?
- What are your lessons learned from the events of 9/11?
- Does your infrastructure meet basic standard contingency requirements for route diversity?
- Are customer network services critically reliable or does the customer need to request and pay for the elimination of single points of failure.
- How is spare capacity engineered (for example percent utilization threshold or by number of last mile customer circuits)?
- Does capacity engineering take into consideration re-directed call volumes when customers activate their disaster recovery plans to avoid choke points?
- How would you describe the industries current abilities to understand how other carriers will affect their networks during a major region outage and the ability to compensate for it?
- If your infrastructure provides route diversity, are these alternate paths solely owned by your organization, or are there reciprocal lease agreements in place with other vendors (for example Verizon dependency on ATT to deliver AIN service)?

- Would you be willing, on a non-disclosure basis, to provide schematics to select individuals and/or organizations where infrastructure is shared with other telecom providers?

- What is your recovery time objective for restoring impacted operations in any given area?

  - Describe the restoration priorities to customers – both business and residential.

  - Describe the criteria for rating in terms of service restoration.

- Is there any possibility of SIFMA participants receiving a priority in terms of service restoration?

- How do you currently inform clients of a service interruption?

- Would you be willing to pass along information regarding the scope of interruptions to a central industry source, i.e., a Securities Industry Association BCP Command Center?

- Are the various carriers cooperating in terms of providing emergency service? If so, in what way?

- For point-to-point private lines only, are any practices in place to mesh discrete customer disaster recovery plans if both side invoke?

Cell Telecom Questionnaire

- What are your available cell (channel) capacities in each major urban region in the U.S.?
- Could you describe the regional breakdowns / diagrams of your services.
- Describe the Signaling System 7 resiliency in the New York / New Jersey area.
- Describe the capacities and relationships of the Tandem switches in the New York / New Jersey area.
- Describe the recovery capability and capacity built in to the network.
- Describe your network monitoring abilities. Are all facilities proactively monitored?
- Describe any periodic maintenance that is performed on your network.
- Describe your practices for maintaining equipment up to current vendor recommended release levels.
- Describe your change control practices for implementing major infrastructure changes.
- How are switching stations/central offices set-up for resiliency and how does it get testes?
- How often is this resiliency tested?
- What are your lessons learned from the events of 9/11?
- Does your infrastructure meet basic standard contingency requirements for route diversity?
- Are customer network services critically reliable or does the customer need to request and pay for the elimination of single points of failure.
- How is spare capacity engineered (for example percent utilization threshold or by number of last mile customer circuits)?
- Does capacity engineering take into consideration re-directed call volumes when customers activate their disaster recovery plans to avoid choke points?
- How would you describe the industries current abilities to understand how other carriers will affect their networks during a major region outage and the ability to compensate for it?
- If your infrastructure provides route diversity, are these alternate paths solely owned by your organization, or are there reciprocal lease agreements in place with other vendors (for example Verizon dependency on ATT to deliver AIN service and how it works)?

- Would you be willing, on a non-disclosure basis, to provide schematics to select individuals and/or organizations where infrastructure is shared with other telecom providers?

- What is your recovery time objective for restoring impacted operations in any given area?

  - Describe the restoration priorities to customers – both business and residential.

  - Describe the criteria for rating in terms of service restoration.

- Is there any possibility of SIFMA participants receiving a priority in terms of service restoration?

- For SIFMA participants, is it possible to have a priority bandwidth set up for cell phones?

- How do you currently inform clients of a service interruption?

- Would you be willing to pass along information regarding the scope of interruptions to a central industry source, i.e., a Securities Industry Association BCP Command Center?

- Are the various carriers cooperating in terms of providing emergency service? If so, in what way?

- For Nextel only, how does the system continue to provide service if cell phones are not functional? What is the network capacity of this service (is it locally and/or regionally based)?

Cell Telecom Questionnaire
Designed for Vendor Presentations

Capacity

- What are your available cell capacities in each major urban financial market in the U.S.? This should include: Metro NY/NJ, Chicago, Philadelphia, LA and San Francisco
- Are there known “dead zones”?
- What is the range and overall roaming ability of the network?
- Describe the recovery/fail over capability and capacity built in to the network.
    - How is resiliency built in to the infrastructure
- Does capacity engineering take into consideration re-directed call volumes when customers activate their disaster recovery plans to avoid choke points?
- How can signal capacity and strength be increased during or after an event?
- For Side Band Audio: What are the radio frequencies utilized and are there distance limitations?
    - Are there any potential conflicts with other service providers or emergency communication services?

Risk Mitigation

- What are your lessons learned from the events of the August 14th, 2003 East Coast blackout as well as 9/11?
    - How are you mitigating regional risk?
- How would you describe the industries current abilities to understand how other carriers will affect their networks during a major region outage and the ability to compensate for it?
- What is your recovery time objective for restoring impacted operations in any given area?
    - Describe the restoration priorities to customers – both business and residential.
- For SIFMA participants, is it possible to have a priority bandwidth set up for cell phones (e.g., GETS)?

Diversity

- How are cell towers, switching stations, central offices set up for resiliency?

- Does your infrastructure meet basic standard contingency requirements for route diversity?

- Are customer network services critically reliable or does the customer need to request and pay for the elimination of single points of failure.

- If your infrastructure provides route diversity, are these alternate paths solely owned by your organization, or are there reciprocal lease agreements in place with other vendors?

- Would you be willing, on a non-disclosure basis, to provide schematics to select individuals and/or organizations where infrastructure is shared with other telecom providers?

- Are the various carriers cooperating in terms of providing emergency service? If so, in what way?

Crisis Management

- How do you currently inform clients of a service interruption?

- Would you be willing to pass along information regarding the scope of interruptions to a central industry source, i.e., a Securities Industry Association BCP Command Center?

Natural Gas
Preparedness Questionnaire

General Concerns:

1. How many supply vendors are parts of your supply chains?

2. Describe the process in place to assure quality of operations. Example; How often is maintenance performed on the connections at our facility? At your primary facility?

3. Describe the Service Level Agreement entered into with the suppliers for the Gas Company? With customers of the Gas Company?

4. Does the vendor have an aggregated amount of gas supply to meet demand, if a supplier event causes a disruption? What is the capacity/duration of the supply?

5. Describe method of how we would be notified of a failure or incident that could disrupt our facilities/business? Furthermore, describe the policy of on-going assessment updates and ETA notification.

6. What is your failover process, if main supply line is disrupted?

7. Do you have Business Continuity plans in place? If so, what process is in place to validate your failover/recovery capabilities?

8. How often have your business continuity plans been activated due to a "live" event or disruption?

9. How would a decrease in human capital of 40% impact your critical business function? Do you have a Pandemic Plan defining how business can continue with a 40% reduction in staff?

10. Are remote operations available on your structure/systems?

11. What regulatory bodies guide your industry? How often are reviews or audits performed?

12. Do you have any reciprocal provider arrangements in place, in the event of a disruption to your business?

Security Concerns:

1. Do all employees, including contractors, managed by vendor go through background checks? Are contractors bonded?

2. Are there remote monitoring for all storage facilities? Are CCTV monitors/cameras in use?

3. Are there other physical security capabilities in place, i.e. locks, guards, etc? Please explain.

4. Describe the process for monitoring and notification of problems associated with supply/transportation lines from providers.

Gas Services/Utility Questionnaire

- What is the source of Gas used in (specify city)?
- Could you describe the number of sources and the levels of redundancy designed in to the source feeds?
- How is gas delivered to the consumer?
- In the event of loss of a source, can other sources take over without a loss in capacity?
- Are there any other available options for sourcing gas locally?
- Could describe the dependency on other utilities (electric, water) to deliver steam to your customers?
- Could you describe the disruption caused to the gas system source and distribution following the recent events of 9/11and the 8/2003 Blackout?
- Can you discuss both recovery and contingency plans for the source gas system and distribution mechanisms in place today?
- Have any changes been made to the gas system delivery or restoration process as a result of these recent events?
- In the event of a service interruption, how do you now inform the consumer(s) of the scale, impact, cause and restoration estimates of the gas services?
- Assuming widespread interruptions, would there be any benefit to passing information to a central industry source such as a specific command center?
- What priority does the utility place on gas service restoration vs. electric or steam supplies? And could you describe the inter-relationships?
- Where can I go to determine the locational relation between my critical location and the source or distribution systems?
- What are my risks in regard to being right next to a distribution line, a block away, a ¼ mile away?
- What is the long term plans for (your City) gas usage? Are there any conversion plans on the horizon?
- What are the steam industries plans for the next 3 to 5 years in regard to upgrades to the sourcing and distribution systems?

Voice Over Internet Protocol (VoIP) Questionnaire

- Explain the makeup of the supporting IP network for VoIP service. Diagrams are useful if they have at least some level of detail. Diagrams are also useful when documenting the boundaries of responsibility between various parties.
  - How is the service delivered to the end user site? What resiliency can be designed? For example, two circuits can be configured to back each other up.
  - What resiliency is built into the carrier or internal network that transports the IP packets between sites or to the telephone network?
  - How much capacity is available on the IP network and is it enough for failover conditions? VoIP can be combined with data on the same network. If data and voice are combined, the network should handle the capacity of both and prioritize voice packets during an outage. How is the stated capacity measured/estimated?
  - How is the VoIP phone system interconnected with carrier telecommunication networks? Is their single or multiple meet-points and how is resilience achieved?
  - QOS (Quality Of Service) – Network recommendations to ensure packet priority in a configured network?

- How is the quality and availability of phone service measured? Do the monitoring tools have the capability to ascertain the quality of the phone service? Noticing and correcting packet delay, drops or jitter under good conditions can help avoid bigger problems under failover conditions. What tools are available with the product to ascertain telecommunications issues versus ip network issues.

- VoIP depends on telephony servers for call setup, phone directories, conference calling and such services. The servers may be provided by either a third party or internally. Among the servers, what resiliency is available and what services depend on single points of failure?

- Are there any dependencies for an individual's phone service on their PC such as call center software? If so, how does the individual recover from a PC failure?

- How may an individual transfer their phone service to another phone, softphone (phone emulation software on a PC), or an alternate location? What components of failover are manual and automatic? How much time is needed for recovering an individual service? In times of crisis when many individuals may need assistance, is the process simple enough to not over burden a central department? Has the vendor addressed (documented) the specific steps of their failover procedure when entering a DR situation?

- In case of site failure, how is the service restored to an alternate location? What parts of the process are in control of the company and which steps depend on external parties such as a carrier?

- Describe the security measures deployed to assure voice conversations are not emulated, recorded or denied? This is important when depending on third party IP networks. When working with third parties, understand who is responsible for security of the various components.

- If personal individual phone management tools exist for end users such as voice mail or call forwarding, consider the security of the tool. For example, if the management tool is on the web, what rules are in place for choosing/expiring passwords, and encryption of traffic?

- Who is responsible for notifying and upgrading software associated with phones, servers and routers? Sometimes upgrades are needed quickly to patch vulnerabilities. How easily can the software/firmware be pushed out to the phones and solution servers and are there any limits to the number of concurrent phones updated. Can the updates be automated and scheduled in the system to self deploy after-hours. What upgrades if any are covered at no cost. What is the frequency of patch availability?

- For components dependent on a third party or carrier, ask where your requests would sit in terms of priority to others during a time of an outage impacting multiple companies. Can processes be automated or put in the control of the customer to reduce dependencies on the third party? Can SIFMA membership give you higher priority?

- What is the notification process in case of outage? Can automated processes send alerts to a list of contacts? Ask for a list of contact numbers and escalation points from the carrier.

- How is 911 services handled in the VoIP network especially when an individual's service may move between offices, to home or a hotel room while traveling.

- Does the provider of the service pass along information regarding the scope of interruptions to a central industry source, i.e., a Securities Industry Association BCP Command Center? What provider reports are available to the customer to review capacity utilization.

General Service Provider BCP/DR Questionnaire:

Objective:
To learn about and understand the business continuity and IT disaster recovery plans of select service providers used by SIFMA member firms. This information is being requested by the SIFMA as part of the securities industry's response to business continuity planning / disaster recovery (BCP/DR) inquiries about industry readiness. This effort is being coordinated through the SIFMA in order to minimize the amount of surveys initiated by individual securities firms with service providers used by many firms.

Scope:
The SIFMA intends to distribute this survey to select service providers used by many SIFMA member firms. It is anticipated some service providers will opt not to complete this survey. In these instances, the SIFMA will likely extend an invitation to those service provider organizations to address key questions outlined in the survey by giving a presentation to members of the SIFMA BCP Steering Committee, its subcommittees or their SIFMA member customers.

The following types of service providers will be included in the survey and extended an invitation to present to the SIFMA BCP Steering Committee, its subcommittees or their SIFMA member customers.

Market Data Service Providers
Telecommunications Service Providers
Back-Office Securities Processing Service Providers
Correspondent Clearing Service Providers
Global Custody Service Providers

Results will be shared with the SIFMA BCP Steering Committee only. However the survey can also serve a template for each service providers to share this info with their customers if they see fit.

General Service Provider BCP/DR Questionnaire:

A	**Business Continuity Strategy**	
A1	In the event of a disaster or significant disruption, does your organization have documented plans for business continuity and IT disaster recovery?	Yes ________ or No ________
A2	If you answered, "Yes" to Question (A1), what type of failure scenarios or outages do you plan for?	____ ____(Please attach an additional sheet if you need___ _____more room to answer this question)_________
A3	If you answered, "Yes" to Question (A1), what duration of time is assumed for each type of failure scenario or outage you plan for?	___________________________(Please specify # and hours, days, weeks, months, etc. for each type)
A4	What types of business functions do you consider critical?	____ ____(Please attach an additional sheet if you need___ _____more room to answer this question)_________
A5	If you answered "Yes" to Question (A1), does the plan establish critical business functions with recovery priorities?	Yes ________ or No ________
A5	If you answered "Yes" to Question (A5), what is the expected recovery time for your critical business functions?	0 – 4 hours _____ 4 – 8 hours _____ Within one day _____ 1 – 2 days _____ More than 2 days _____ Other (please specify) _____ N/A _____
A7	If you answered, "Yes" to Question (A1), does the plan account for interdependencies both internal and external to your organization?	Yes ________ or No ________
A8	If you answered, "Yes" to Question (A1), does the plan cover some, most, or all locations from which you provide your services?	Some _______________ Most _______________ All _______________ Other (please specify) _________________________ N/A _______________

A9	If you answered, "Yes" to Question (A1), what percentage of "business as usual" servicing capability is the plan designed to address?	1 – 10% _____ 11 – 20% _____ 21 – 30% _____ 31 – 50% _____ 51 – 75% _____ 76 – 99% _____ 100% _____
A10	Do you have a dedicated team of professionals focused on business continuity and/or IT disaster recovery?	Yes ________ or No ________
A11	If you answered "No" to Question (A10), do you use an external BCP/DR service provider to handle your planning needs?	Yes ________ or No ________
A12	Do you use an external BCP/DR service provider to handle your **hardware** recovery needs?	Yes ________ or No ________
A13	Do you use an external BCP/DR service provider to handle your **software** recovery needs?	Yes ________ or No ________
A14	Do you use an external BCP/DR service provider to handle your **telecom** recovery needs?	Yes ________ or No ________
A15	Do you use an external BCP/DR service provider to handle your **work area** recovery needs?	Yes ________ or No ________
A16	Is your main IT facility or data center located in the same building or office complex occupied by your main business or operations staff?	Yes ________ or No ________
A17	Please provide an illustration or schematic of how your organization's primary, secondary, and/or tertiary servicing centers are setup to provide redundant services to customers.	____ ____(Please attach an additional sheet if you need___ _____more room to answer this question)_________
B	**Crisis Communication**	
B1	Do you have a documented crisis management process within your organization?	Yes ________ or No ________
B2	If you answered "Yes" to Question (B1), does this process cover internal and external communications during a crisis event?	Yes ________ or No ________

B3	How do you notify your clients of an outage?	____ ____(Please attach an additional sheet if you need___ _____more room to answer this question)_________
B4	Do you provide your customers with detailed contact information in the event of an outage or emergency?	Yes ________ or No ________
B5	Please describe how you notify your team of an incident and direct them through the recovery.	____ ____(Please attach an additional sheet if you need___ _____more room to answer this question)_________

C	**Back Up Facilities**	
C1	Does your organization have an alternate site location for data center recovery purposes?	Yes ________ or No ________
C2	If you answered, "Yes" to Question (C1), what is the approx. distance between your production (primary) site and alternate (secondary) site for data center recovery purposes?	____ (Please specify # and miles/kms, city blocks, etc.)
C3	Does your organization have an alternate site location for work area recovery purposes?	Yes ________ or No ________
C4	If you answered "Yes" to Question (C3), what is the approx. distance between your production (primary) site and alternate (secondary) site for work area recovery purposes?	____ (Please specify # and miles/kms, city blocks, etc.)
C5	Do you use an external BCP/DR service provider for your data center recovery needs?	Yes ________ or No ________
C6	Do you use an external BCP/DR service provider for your work area recovery needs?	Yes ________ or No ________
C7	If you answered "Yes" to Question (C6), is your contract with your BCP/DR service provider honored on a first-come/first-served basis?	Yes ________ or No ________

C8	What recovery strategy does your organization use for mainframe systems?	Active/Active _______ Active/Back-up _______ Vendor Supplied _______ Other _______ N/A _______
C9	What type of recovery strategy does your organization use for distributed systems?	Active/Active _______ Active/Back-up _______ Vendor Supplied _______ Other _______ N/A _______
C10	Is the processing capacity of your back-up facility equal to that of your primary facility?	Yes ________ or No ________
C11	If you answered "No" to Question (C10), what is the capacity ratio of your back up to your primary facility?	1 – 10% _____ 11 – 20% _____ 21 – 30% _____ 31 – 50% _____ 51 – 75% _____ 76 – 99% _____ 100% _____ N/A _____
C12	Is it feasible to run your primary "data center" or technology center from your back-up facility for an extended period? (e.g. at least one month)	Yes ________ or No ________
C13	Is it feasible to run your primary "people" or work area from your back-up facility for an extended period? (e.g. at least one month)	Yes ________ or No ________
D	**Testing**	
D1	If you answered "Yes" to Question (A1), is the plan periodically tested?	Yes ________ or No ________
D2	If you answered "Yes" to Question (D1), how frequently is the plan tested?	Annually _____ Semi-annually _____ Other (please specify) __________________________
D3	Do you have BCP test dates scheduled over the next 12-18 months?	Yes ________ or No ________
D4	If you answered "Yes" to Question (D3), please list those dates (for industry planning purposes)	_______ _______ _______ _______ _______

D5	If you answered "Yes" to Question (D1), do you involve IT staff, business unit or operations staff or both in your internal BCP/DR tests?	IT staff only _____ Business Unit or Operations Staff only _____ Both IT and Business Unit or Operations Staff______
D6	If you answered "Yes" to Question (D1), do you also involve customers in your external BCP/DR tests?	Yes ________ or No ________
D7	If you answered "Yes" to Question (D6), what is the percentage of customer participation?	1 – 10% _____ 11 – 20% _____ 21 – 30% _____ 31 – 50% _____ 51 – 75% _____ 76 – 99% _____ 100% _____ N/A _____
D8	If you answered "Yes" to Question (D1), do internal or external auditors review your BCP/DR tests?	Yes ________ or No ________
D9	If you answered "Yes" to Question (D1) what components of your systems and infrastructure are tested?	Applications ______ Middleware ______ Databases ______ Data networks ______ (internal and external) Voice networks ______ (internal and external) Desktop ______ Facilities ______ Voice equipment ______
E	**September 11th**	
E1	Did your organization invoke its business continuity or IT disaster recovery plan(s) as a result of the September 11 tragedy?	Yes ________ or No ________
E2	Has your organization enhanced its business continuity planning initiative, or is in the process of enhancing its plans in light of September 11?	Yes ________ or No ________
F	**Industry BCP Support**	
F1	Please provide primary and alternate contact information for industry level communication during an emergency.	____ ____(Please attach an additional sheet if you need___ _____more room to answer this question)_________

F2	Would your organization be willing to disseminate information regarding the scope of interruptions experienced within your organization to a central industry group such as the Securities Industry Association's BCP Command Center or FIF Recovery Site?	Yes ________ or No ________
F3	Would your organization be willing to address BCP strategy and best practices with a group of your customers as part of an organized industry effort?	Yes ________ or No ________

GENERAL BEST PRACTICES FOR ALL INFRASTRUCTURE PROVIDERS

The following are the recommended guidelines / best practices that should be observed by each firm's business continuity program and business continuity plans.
(These are right from the Best Practices Guideline at www. SIFMA .com)

I. General Concepts for an Infrastructure Provider's Business Continuity Program

A. Existence of Plans

Each firm should have in place a Business Continuity (BC) program that ensures:

The development, implementation, testing and maintenance of business continuity and emergency response plans that enable the business to protect its assets and meet its business recovery objectives.

Below are Prevention and mitigation activities that reduce the likelihood and impact of a disruption.

As an ongoing employee awareness program;

Each firm should have a Business Continuity policy document which provides the framework for its Business Continuity program and the development of business continuity and emergency response plans.

Business continuity plans should be documented and readily accessible to those who need access.

Each firm should have an Executive and corporate group responsible for overseeing the business continuity program.

Business managers should be responsible for the review, implementation, funding and sign-off of business continuity plans and associated exercise results.

Recovery exercises for critical business functions should be conducted no less than annually and as is warranted by changes in the business and/or information system(s) environment.

Plans should be reviewed and updated no less than annually and as warranted by changes in the business and/or information system(s) environment.

B. Recovery Strategies

Each firm should develop recovery strategies that would enable them to continue their most critical operating, service and technology functions in order to:

- Meet defined recovery objectives
- Meet the service level commitment to customers
- Meet fiduciary requirements
- Minimize financial, legal and / or regulatory exposure

A firm's strategy should be based upon an event impacting an extended geographic zone and having a significant impact on the firm and its resources.

C. Recovery Resources

Each firm should ensure that required resources are available to meet its recovery objectives.

The firm should have the capability to communicate with employees using multiple methods of communication (i.e. phone, pager, cellular phone, e-mail, internet, etc).

The firm should have pre-defined business continuity teams, detailing management structure and roles and responsibilities.

Essential business staff should be trained and fully capable of performing business functions at the recovery location.

Recovery facilities should not be located in the same geographical zone as the primary business facility and should be supported by separate telecommunication and utility infrastructure.

The accessibility, availability and capability of recovery facilities should support the firm's requirements and recovery objectives.

Firms should consider geographic diversity of critical staff and critical production applications, data, or data centers supporting them.

BC plans should include internal and external business partners (operations, tech support, clients, vendors, regulators, exchanges, etc.), ensuring that acceptable levels of operational connectivity can be resumed within recovery objectives.

Firms should be familiar with business partner BC plans (both internal and external) and understand any associated risk.

Business units should ensure that redundant copies of vital records are stored in a secured and geographically diverse location and are available for use during an emergency within stated recovery objectives.

II. General Best Practices for an Infrastructure Provider's Business Continuity Program

A valuable resource of Best Practices that can be applied to any provider is the following website.

> **www.NRIC.org – The Network Reliability and Interoperability Council**

While the Council is focused on the reliability of telephony and data transmission, it also supplies numerous examples of best practices that can be adapted or adopted by any industry. Some of those best practices are paraphrased as follows:

> Service Providers … should establish and maintain an interface with local, state, and federal government agencies to ensure effective support is available upon request as part of disaster recovery.
>
> Provide diverse power feeds … for any components identified as ""critical"" single points of failure in transport and operations of the network…
>
> Maintain adequate fuel on-site and have a well-defined re-supply plan. Improve fuel systems reliability by providing redundant pumps for day tanks and a manual-priming pump. Wherever possible, use dual-source.
>
> Schedule System Backups - All Service Providers should establish policies and procedures that outline how critical network element databases, (e.g., router configurations, digital cross connect system databases, switching system images), will be backed up onto a storage medium (e.g. tape, optical diskettes) on a scheduled basis. These policies and procedures should address, at a minimum, the following:
>
> - Database backup schedule and verification procedures
> - Storage medium standards
> - Storage medium labeling
> - On site and off site storage
> - Maintenance and certification
> - Handling and disposal
>
> The implementation of this practice will mitigate the impact of data corruption or some other loss of a critical network database.
>
> Develop crisis management exercises - Service Providers should, at a minimum, have a communications structure in place for timely notification of affected parties in the event of disasters or emergencies.
>
> Service Providers should establish agreements with landlords for both regular and emergency power.
>
> Service Providers … should consider using a disaster recovery support model with escalation procedures that provide a clear escalation path to executive levels both internally and externally.

In preparation for predicted natural events, e.g., ice, snow, flood, hurricane, Service Providers … should consider placing standby generators on line and verify proper operation of all subsystems.

Service Providers … should consider, where feasible, utilizing multiple communication carriers to provide diverse connectivity between service nodes reducing single points of failure.

Service Providers… should consider, during their response to major disasters, editing the support "hotline"-calling calling tree by adding a specific entry for disaster events.

Service Providers … should consider the development of a vital records program to protect vital records that may be critical to restoration efforts.

Service Providers … should identify key individuals within their organizations that are critical to disaster recovery efforts. Planning should consider maximizing the availability of these individuals.

Service Providers … should consider utilizing multiple alternative communication devices and service providers for critical service personnel during emergencies.

Service Providers … should develop company specific protective measures that correlate with the threat levels identified in the Homeland Security Advisory System

Service Providers … should consider establishing a designated Emergency Operations Center. This center should contain tools to coordinate and restore its services including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.

Lessons Learned

Post August 14, 2003 Blackout Update

Project Objective:

To review published post-blackout reports to determine what issues, if any, may be relevant to individual financial institutions for BCP planning purposes and to assist in any corporate risk mitigation practice going forward.

The following information was derived from multiple sources relating to the East Coast Blackout of August 14, 2003.

As requested, data was extracted from the following sources:

- "Enhancing New York City's Emergency Preparedness" – prepared by New York City Emergency Response Task Force dated October 28, 2003.
- "The Digital Power Group" prepared by Peter Huber and Mark Mills August 2003. Web: http://www.digitalpowergroup.com/
- "Financial and Banking Information and Infrastructure Committee" October 2003

Background:

The East Coast experienced an electrical blackout that began in the late afternoon of August 14, 2003. The blackout shut down power service for approximately 50 million people from New York to Canada to the North and from the East Coast all the way to Detroit. New York City experienced outages of 8 million people, which were larger than the 1965 and 1977 power outages.

The 2003 blackout affected more individuals then in previous blackouts because of the vast array of technologies supporting required infrastructures. This blackout went far beyond the loss of modern conveniences: people were stopped dead in their tracks; public safety was jeopardized on the street with no traffic lights; people stuck in elevators; normal voice communications were not working as required; and the technologies needed to keep things moving were in most cases shut down. Public core infrastructures (computers, communications, transportation, safety…) require power to maintain an expected level of service required by people to maintain normal lives. In most cases these infrastructures were compromised during the blackout.

Impact and Issues:

New York City experienced problems with the mobilization of some crisis command centers and response due to:

- Lack of consistent recovery response plans – not being properly drilled
- Emergency units working in a silo-based manner lacking communications between other critical areas.
- Employee movement / staffing were hampered by; getting staff mobilized and providing people with proper credentials to move in-out of the city with supplies. .
- Non-availability of public sector employees during the blackout was paramount to the recovery effort taking longer then expected.
- The city needs to define activities for non-emergency staff to support tasks for specialized workers such as electricians and plumbers. People who work in non-emergency response agencies could have been used to help in the recovery efforts.

Summary of Emergency Response Issues:

The public as well as the private sector experienced similar based problems related to communications, infrastructure recovery and the overall logistical impacts of dealing with this unprecedented event. More strategic planning and simulation drills are necessary to for public and private sectors to insure recovery of their environments making them more prepared for future events. The City in general should strengthen their command center structure, notification capabilities to the public, communications infrastructure, power infrastructure, recovery plans and to perform more drills allowing staff to become more familiar with the recovery concerns.

Business Continuity Concerns

- The City experienced a shortage of power and fuel to run their generators during the blackout.
- Generators failed to operate or had mechanical problems when they were under a load
- Slow recovery of Steam Pressure was a major delay in the resumption of a small population of businesses in the city. Steam service took several days to be back online causing some of the 1800 customers to have shut downs in their operation.
- Most agencies did not have enough emergency supplies on had to support the blackout. Items such as food, water, batteries, flashlights and cash on hand to make purchases.
- Having well established communication channels with small businesses in the city. Information was not flowing to people and businesses in a concise or timely manner. Having a good public address system with backup power is essential for all buildings and small businesses in the city.
- It is essential that Firms utilize redundant central communication offices to support their business data and voice capabilities. Know your communication provider and understand their recovery capabilities.
- Cellular networks will overload during emergency situations. Develop additional communication capabilities to reach out to staff during a disaster.

- Understand your power requirements and recovery capabilities within your organization. The Power Grid or portions of it may fail again in the future. Firms should have stand alone power sources to maintain their critical environments. This is a mandatory requirement and much more necessary as we continue with the electronic age. Firms should conduct a power survey and develop backup to support all essential infrastructure components.
- Understand transportation and the failures that may occur and how they can affect your recovery planning strategies. Firms need to have well defined plans on how to move staff during recovery operations.
- Having well defined health and safety programs in your organization. Understand the critical health requirements of your current staff and plan for contingencies to support individuals who requires special medical attention.
- Develop in your organization a skills database to be used during a crisis. Firms can capitalize on skills of other employees at time of event.
- Ensure Firms have building evacuation plans and that they are exercised on a regular basis.
- Understand your local city requirements for crisis escalation within the public sector (mayor's office, police, fire, health…)

Useful Websites For BCP Practitioners

Value	Description	Web-Link
	US Government Links	
1	DHS Disaster Help	http://www.disasterhelp.gov/
2	Emergency Planning and Prevention	http://www.dhs.gov/dhspublic/display?theme=14
2	EPA Environmental Emergencies	http://www.epa.gov/ebtpages/emergencies.html
1	Federal Emergency Management Association	http://www.fema.gov/
1	FEMA: A Citizen's Guide to Preparedness	http://www.fema.gov/areyouready/
2	National Weather Satellite pictures	http://www.osei.noaa.gov/
2	New York State Emergency Management	http://www.nysemo.state.ny.us/
2	NGDC-Natural Hazards Databases	http://www.ngdc.noaa.gov/seg/hazard/
1	Office of Homeland Security	http://www.dhs.gov/dhspublic/
1	Ready.Gov: Useful Sites	http://www.ready.gov/useful_links.html
	Severe Weather	
	NWS Severe Weather Awareness	http://www.nws.noaa.gov/om/svrawar/svrwx.htm