SECTOR BLACK SKY PLAYBOOK

Draft/Sector Steering Committee Reviewed, July, 2017.

ABSTRACT

Yedidya Sinclair

V 2.5

Table of Contents

Role of the EPRO Sector Black Sky Playbook

This Playbook is designed to provide an evolving framework of recommended guidelines to manage risks of long duration, multi-region power outages associated with emerging "Black Sky" hazards.

This Playbook will be consistently updated and reviewed using the EPRO Sector Steering Committee process through consultation with Finance Sector professionals and managers. This playbook contains the latest consolidated school of thought on the unique challenges posed by wide area, long duration outages. It provides guidelines to help individual Finance Sector entities strengthen their internal resilience measures, develop focused operational plans and identify external support needed to address these severe hazard scenarios.

Sector Background

The United States Financial Sector is a critical driver of the world economy. With assets estimated to be in excess of $48 trillion, this large and diverse sector accounts for more than 8 percent of the United States gross domestic product (GDP). The Financial Sector is primarily owned and operated by the private sector whose institutions are extensively regulated by federal and, in many cases, state government.

The Finance Sector is characterized by deep mutual interdependencies with other key infrastructure sectors. It is critically dependent on electrical power, voice and digital communications and urban transportation networks. The financial sector is highly automated and digitized. Other infrastructure sectors are, in turn, critically dependent on the financial sector, most acutely on the payments functions performed by the sector. As well as enabling the exchange of all sorts of goods and services, payment mechanisms enable the pervasive signaling of demand and need across our society, a function vital to the efficient and effective allocation of goods and services.

After 9/11, the U.S. government took the lead in promoting emergency and resilience planning in the financial sector. In October 2001, the US government established **FBBIIC** (Financial and Banking Information Infrastructure Committee) a working group comprising all US federal government regulators and agencies involved in the Finance Sector. The East Coast power outage of August 2003, when some financial institutions and markets closed for a few hours, lent further urgency to the sector's emergency and resilience planning.

The Finance Sector's emergency and resilience planning is detailed, pervasive and sophisticated. There are extensive coordination mechanisms between government and the private sector. Major financial firms and institutions have their systems and records backed up at alternate sites, far from their main offices. Many also have alternate personnel teams who are trained to take over the firm's key functions at the alternate business sites in an emergency. Banks and institutions of medium size and above have their own emergency generators and fuel supplies (though it is unclear how long the fuel supplies would last). The US government has a program to enable emergency communications facilities for financial firms. This program operates through the DHS' Government Emergency Telecommunications (GETS) and Wireless Priority Service (WPS). The GETS program offers priority, government channel cell phone access to high priority institutions, when the normal cell phone networks are overloaded. However, the

program does not assist in a situation where cell phone networks have failed altogether, such as could be the case following a Black Sky event.

The sector's resilience planning is heavily focused on cyber defense. However, there are few references to Black Sky events in the sector's planning documents. Consequently, it is unclear whether the resilience measures that the sector has in place would be adequate to deal with a lengthy and extensive power outage affecting all key infrastructure sectors. Impacts resulting from the April 2017 power outage in San Francisco caused by a circuit breaker failure suggest that these measures may well not be adequate. Approximately 500,000 people were affected. Wells Fargo closed 13 bank branches and four office buildings, while the New York Stock Exchange said its ARCA options trading floor in San Francisco was briefly unavailable. Employees in Goldman Sachs' financial district office were sent home. Approximately 25% of the traffic lights in San Francisco were affected and traffic was a disaster all day with pedestrians at much higher risk than normal. This was the impact from the failure of one circuit breaker in one substation.

Sector Black Sky Environment

A Black Sky level power outage would likely have the following broad impacts on the financial industry:

Physical Operations: power failure would likely cause the closure of major financial firms and institutions' main bases of operations. In addition, cascading impacts of power failure on urban traffic and transportation systems would probably prevent financial sector employees being able to travel to and remain at their places of business and customers from accessing the facilities. Since lower paid employees would not be able to come to the population centers, the banks serving in-person customers would probably not function

Financial Operations: cash could not be withdrawn, checks could not be cashed, and debit and credit card networks (including ATMs) would be down. Continuity of operations procedures (required of all but the smallest depository institutions,) would begin, including maintaining critical personnel and data storage (with daily backups) located at least 20 miles from a bank's headquarters.[1] Data backups would come into effect. The severity of impact would depend on the extent of the outage and also on the effectiveness of financial institutions' emergency generators and the duration of their fuel supplies.

Communications: A Black Sky event would seriously impact normal communications networks. Financial firms are heavily dependent on communications for all operations and also for recovery activities. Financial institutions maintain multiple and redundant communications paths (landlines, cell phones, wireless, satellite, broadband etc.) to enhance resilience. They also have priority access to government emergency communications programs including the DHS's Government Emergency Telecommunications (GETS) and Wireless Priority Service (WPS). Depending on the severity of the event, some of these channels might be operational or, conceivably, they could all fail.

[1] N. Eric Weiss Banking and Financial Infrastructure Continuity, Congressional Research Service, 2009

Sector Model Overview

.

The financial services sector is complex and diverse, ranging from the largest institutions with assets greater than one trillion dollars to the smallest community banks and credit unions. Financial institutions provide a broad array of and services. These products can be classified as follows,

(1) Deposit, Consumer Credit and Payment System Products; Depository institutions of all types (banks, thrifts, and credit unions) provide wholesale and retail payments services, such as wire transfers, checking accounts, and credit and debit cards. These institutions use and/or operate the payments infrastructure, which includes electronic large value transfer systems, Automated Clearinghouses (ACH), and automated teller machines (ATM). (more than $10 trillion in assets);

(2) Credit and Liquidity Products; Financial institutions, such as depository institutions, finance and lending firms, securities firms, and Government Sponsored Enterprises (GSE) meet customers' long- and short-term credit needs. Some provide credit directly to the end customer; others provide wholesale liquidity to those financial services firms that provide these services on a retail basis. (more than $14 trillion in assets);

(3) Investment Products; These products include debt securities (such as bonds and bond mutual funds) and equities (such as stocks or stock mutual funds), and derivatives (such as options and futures). Certain securities including U.S. Treasuries and equities of some multinational companies—are traded around the globe 24 hours a day. (More than $18 trillion in assets);

(4) Risk Transfer Products; Products for the transfer of financial risks, such as the financial loss due to theft or the destruction of physical or electronic property resulting from a fire, cyber-attack, or other loss event, or the loss of income due to a death or disability. Providing institutions include insurance companies, futures firms, and forward market participants offering financial products for customers to transfer various types of financial risks. (more than $6 trillion in assets)

The financial world is global; the US Finance Sector is inextricably connected to financial markets world-wide. Serious disruption of the US financial sector could have major international repercussions upon both the financial sector and the real economy.

New York City, the center of the US financial sector, vies with London for the position of world's leading financial hub. The City of London is home to a massive, diversified and global financial service sector, including exchanges, banks, brokers, investment managers, pension funds, hedge funds private equity funds and insurance companies.

Sector Model Graphic

To be developed

Sector Black Sky Strategic Mission Statement

The Finance Sector should perform the following functions in a Black Sky event:

- Maintaining a core payments mechanism: the financial sector should ensure that a basic means of making payments survives throughout a Black Sky event. It is critical that a capacity to make payments and carry out transactions is maintained to facilitate the restoration of others sectors and to provide a way of signaling where restoration needs are most critical. While government can be expected to take a large role in the restoration, the scale of complexity of recovery from Black Sky is such that it is very doubtful if it can be managed entirely by government-led command and control processes. It is our assumption that the continuation of some very basic market exchange processes will facilitate the recovery.
- Maintaining financial sector critical operations, such as data centers and critical services, including large value payment processing, clearing and settlement of transactions, and supporting systems such as funding and reconciliation services.
- Maintaining channels of communications within the financial sector and between the financial and other interdependent sectors.
- Rapid restoration of financial sector critical operations and services.

Sector Black Sky Strategic Mission Priorities Matrix

Because of its greatly increased dependence on digitization, the Financial Sector is particularly vulnerable to a long-term, widespread power outage. In a Black Sky event, the Finance Sector's mission should be to maintain minimal levels of service These services are vital to resuming, maintaining and operating other critical infrastructures and to enabling a basic level of commerce that will assist the other recovery of the other infrastructure sectors. These minimal service priorities include maintaining a core payments system, sustaining finance sector critical operations and maintaining channels of communications within the Finance Sector and between the sector and other key infrastructure sectors.

Phase	Priority	Mission
Throughout	Critical	Maintain a core payments system, whether through ordinary operations or a predetermined emergency liquidity facility
Throughout	High	Maintain financial sector critical operations, such as data centers and critical services, including clearing and settlement of transactions, through operation of normal and/or backup operations centers.
Thoughout	High	Maintain channels of communications with the financial sector and between the financial and other interdependent sectors.
Later Stage	Critical	Rapid restoration of financial sector critical operations and services.

Black Sky Decisions Overview

Following a Black Sky event, initial decisions that would need to be made concerning the functioning of systems and operations in the Financial Sector and within its large firms and other key actors. An important early decision would be whether the principal places of business of large companies are still operational or whether operations need to be transferred to the backup locations outside large areas that most large firms have prepared. This decision would depend on the status of power availability, communications and transportation at firm's principal, urban business locations.

Another important early decision is whether it would be necessary to activate some Emergency Liquidity Facility that may have to be set up to facilitate critical transactions and payments that are necessary to help the recovery of other sectors. This would depend on an assessment of whether normal payments methods are still operating.

Furthermore, decisions would need to be made about which communications channels, if any, are still viable after a Black Sky event and which should be used to maintain essential communications within the sector and beyond – whether this is the government enabled emergency communications facility that is open to key Finance Sector players or some general cross-sector emergency communications platform such as BSX that EIS Council is working to establish.

Beyond the initial stages, available, there will be important decisions to be made about the reallocation of emergency generators and fuel supplies that are maintaining essential operations.

Black Sky Decisions Matrix

Phase	Priority	Decision
Early	Critical	Do financial firms' operations need to be moved to backup business locations?
Early	Critical	Are employees able to come to offices in primary locations? Backup locations?
Early	Critical	Do emergency communications channels need to be activated?
Early	Critical	Do emergency liquidity facilities or other emergency payments mechanisms need to be activated?
Middle-Late	Critical	Do emergency generators need to be replaced, repaired or refueled?

Sector Black Sky Situational Awareness Overview

Some of the key situational awareness elements that will need to be established are the status and functioning of financial institutions' primary places of business, including the status of electrical power supplies, the ability of employees to travel to primary/secondary places of work the status of normal and backup communications networks, including landlines, cellphones, internet, satellite phone networks and emergency government communications networks; also the status of Financial Sector operations, including normal payment and clearing mechanisms, operation of ATMs and status of data storage systems. In addition, it will be important to gain situational awareness on the status and functioning of backup places of business and support facilities, especially backup power generators.

Priority Information Requirements Matrix

Information	Source	Priority	Confidence Level
Status and functioning of Finance Sector primary business sites.	Finance Sector staff	Very high	High
Status and functioning of normal and backup communications channels	Finance Sector staff	Very high	High
Status of Finance Sector operations, including payments and clearing mechanisms etc,	Finance Sector staff	Very high	High
Status of backup financial sector operations, places of	Finance Sector staff	Very high	Medium

business and power generators			

Sector Initial Actions

Essential, initial actions will include:

- Checking on safety of staff; ensuring that they can return to work when their physical facilities are not operating or are not accessible. Notifying employees in case work locations are shifted to backup locations.
- Financial institutions monitoring, executing pre-established crisis management procedures, and coordinating responses.
- Implementing business recovery plans for recovering equipment, applications, vital records and regulatory reports, transferring if necessary to relocation sites, and activating recovery teams and tasks — needed to reestablish essential business operations
- Implementing systems and data recovery, focusing on restoring the financial institutions' core infrastructure, including networking, applications and other shared technologies to ensure the continuation of critical business systems; activating backup data systems.

Sector Initial Actions Matrix

Priority	Initial Action	Desired/Required Outcome
Critical	Checking on safety of staff and their families; ensuring their availability for work	Staff and their families are safe, and key staff are available for recovery ops
Critical	Financial institutions executing pre-established crisis management procedures, and coordinating responses with other government and private institutions	Crisis management procedures are viable and are implemented successfully
Critical	Implementing business recovery plans for recovering equipment, applications, vital records and regulatory reports, transferring if necessary to relocation sites, and activating recovery teams and tasks	Business recovery plans and recovery tasks and teams implemented successfully
Critical	Implementing systems and data recovery focusing on restoring the financial institutions' core infrastructure, including networking, applications and other shared technologies to ensure the continuation of critical business systems; activating backup data systems.	Successful implementation of systems and data recovery to enable continuation of financial institutions critical systems.

Internal Sector Requirements

Some of the key internal sector requirements for Black Sky resilience that enable the sector to carry out its mission are:

- Detailed, pre-established crisis management procedures and business recovery plans for equipment and vital records, and systems and data recovery plans
- Personnel skilled and trained in implementing crisis management, business recovery and systems/data recovery
- Adequately equipped backup operations locations accessible to trained staff and equipped with adequate emergency power generators and fuel supplies; backup storage for key records and data
- Communications system sufficiently resilient to withstand a Black sky event for intra-sector communication, cross-sector communication with government and interdependent sectors, and international communication with other financial sector bodies.

Internal Sector Requirements Matrix

Phase	Priority	Requirement
Pre-event	Critical	Detailed, pre-established crisis management procedures, business recovery plans for equipment and vital records, and systems and data recovery plans
Pre-event and during event	Critical	Available personnel who are skilled and trained in implementing crisis management, business recovery and systems/data recovery, including skills specific to EMP and major cyber events.
Pre-event and during event	Critical	Adequately equipped backup operations locations accessible to trained staff and equipped with adequate emergency power generators and fuel supplies; backup storage for key records and data
Throughout event	Critical	Communications system sufficiently resilient to withstand a Black sky event for intra-sector communication, cross-sector communication with government and interdependent sectors, and international communication with other financial sector bodies.

External and Cross Sector Dependencies Overview

The cross-sector interdependencies of the financial sector include those that are required to support continued sector operations and include consideration of people, equipment and facilities and security.

The cross-sector interdependencies that support people include food, water, medicine and physical security. Transportation is also critical for recovery workers from the Finance Sector to be able to reach operations locations.

Interdependencies that support equipment and facilities include, primarily, dependency on backup power that is necessary to maintain Finance Sector operations communications and data transfer and storage. In a prolonged outage, this will require refueling of emergency generators by the oil distribution sector and repair of generators. Water and waste-water treatment that keep offices and workplace viable is another critical interdependency.

For Finance Sector operations, the key interdependency is telecommunications, which are critical for all financial sector operations - payments, account balancing, transfers, data storage and transfer etc.; They are also critical for complex recovery operations. Intra-sector communications will need to be complemented by a viable cross-sector communications networks that is resilient to a Black Sky level power outage.

External and Cross Sector Requirements Matrix (V2.5/V3)

Requirement Area	Priority	Requirement
Manpower	High	Finance Sector staff need to be available to work on maintaining operations and recovery at primary or backup workplaces
Transportation	High	Road transportation, especially within cities, and commuter rail to cities are necessary to enable minimal necessary staffing at key financial institutions, during a Black Sky event.
Backup Power	Critical	Electrical power is needed for operation of Finance Sector IT, communications, operations and data storage and transfer as well as for functioning physical work places; Oil distribution is required to refuel emergency generators that are needed to keep power-dependent, critical Finance Sector operations and services running
Security	High	Public security is necessary for recovery work to be done
Communications (Physical)	Critical	Telecommunications, including internationally, are critical for all Finance Sector operations - payments, account balancing, transfers, data storage and transfer etc; They are also critical for complex recovery operations
Water	Critical	Water and waste water are required for functioning and viability of Finance Sector work places
Food	Critical	Disruptions in production, distribution and retailing of food and medicine will rapidly impact ability of Finance Sector staff to continue working

Add additional lines as need within each area as needed. In future versions there will likely be an Annex to further define these requirements.

Sector Specialized Resource Requirements Overview

The Finance Sector requires a number of key resources to maintain and restore operations after a Black Sky event. The key resource is fuel to continue operations of backup emergency generators for Finance Sector facilities. Spare parts to repair broken generators will also be needed. Technically trained staff who are capable of restoring data and communications systems will also be a key requirement.

Sector Commodity Specific List Matrix

Phase	Commodity	Estimated Quantity	Potential Source
From mid stage	Fuel for emergency generators	TBD	
From mid-stage	Spare parts for generator repair	TBD	
Throughout	Technically trained staff to restore systems	TBD	

Sector Black Sky Communications Overview

The ability to communicate after a Black Sky event is critical to the Finance Sector. The East Coast power outage of August 2003 lasted only 24-48 hours but brought serious communications disruption to the Finance Sector. In some cases, the blackout affected entire telecommunication networks that had insufficient backup power at some central office switches. In other cases, some firms found that their backup electrical generators did not support their internal telephone systems, rendering their digital telephones inoperable, while their analog-line telephones (which receive power over their land lines and bypass internal telecommunication switching systems) continued to function. In addition, mobile phones soon became inoperable due to message congestion, insufficient backup power at transmission and relay sites, and the inability of individuals to recharge their mobile phones' batteries. A longer term outage today when the Finance Sector is even more dependent on communications could be catastrophic.

Financial firms should identify those responsible for communicating with staff and external stakeholders in a long-term outage. This group should be able to communicate with personnel located at isolated sites, dispersed across multiple locations, or otherwise away from the primary business location; contact information for relevant domestic financial authorities and financial industry participants should be available to facilitate an assessment of the condition of the financial system and to coordinate recovery efforts.

Failures in primary communication systems should be expected. Many financial firms and institutions have developed systems and maintain contact information for key personnel that facilitate multiple methods of communicating (e.g., digital and analog land line phones, mobile phones, satellite phones, text messaging, websites, hand-held wireless devices); major financial firms also have access to government priority emergency communications networks. It is quite possible that in a Black Sky event, most or all of these channels would be down and alternative, resilient communications networks would be needed.

The EPRO BSX communications project is developing the architecture for such a communications system that would withstand an EMP burst or cyberattack and satisfy the Finance Sector's need for emergency communications that would provide situational awareness and command and control following a Black

Sky event, that is, a communications environment without cellular or satellite means, for periods in excess of a month without Grid-furnished power.

Given the deepening interdependencies of financial systems across national boundaries, financial authorities also need to adopt communication protocols that address situations where cross border communication may be necessary.

Sector Communications Matrix

Phase	Communications Requirement	Coordinated Cross Sector Element
Initial	Finance Sector institutions will require working voice and electronic communications with their staff to gain situational awareness in the state of their personnel operations and facilities	Internal to sector
Throughout	Working voice and electronic communications with other Finance Sector institutions, government and international sector partners to maintain a basic level of Finance Sector operations; includes communications with oil distributors for refueling emergency generators	Cross-sector, especially with government
Recovery	Working voice and electronic communications with and between systems and equipment restoration workers in the Finance Sector and power restoration people outside the sector	Cross-sector.

Sector Black Sky Assessment Tool (s) Overview

Sector Black Sky Planning Requirements

Emergency planning in the Finance Sector is quite advanced. Associations such as FSCCC (Financial Services Coordination and Communication Center) and FS-ISAC (Financial Services Information Sharing and Analysis Center, described above, have develop networks of emergency communication, crisis communication between government and financial firms and sharing of threat alerts and intelligence. However, the overwhelming majority of emergency preparation in the Finance Sector today focuses on preparation and response to cyber-attacks on financial institutions and networks.

The FSCCCs' All-Hazards Crisis Response Playbook, currently in development, groups best practices under five headings:

1. Finance Sector (FS) crisis communication;

2. FS Crisis Response Coordination;
3. Government Crisis Response Coordination;
4. Associations, Regional and Multi-Sector Crisis Coordination; and
5. Sector Contingency Plans and Event Closure.

Within the Finance Sector, Goldman Sachs is known to have good emergency and business continuity planning. (The firm's headquarters in New York City was, notoriously, one of the very few mid-town Manhattan skyscrapers to remain illuminated throughout Hurricane Sandy in 2012.) Its plans (a summary of which is publicly available) include emergency generators at all its sites, fully equipped alternate operations sites away from urban areas, and fully trained alternate staff ready to continue operations at alternate sites in emergencies, as well as multiple backups of key data and systems. According to a November 10th 2012 report on business disaster planning in The Economist, "Goldman Sachs has long been a leader in disaster planning because it understands that the situations in which it might not be able to function are exactly the sort of events when very large changes in the value of its investments could occur." The firm's resilience and emergency planning approximate to current best practices in the sector.

However, based on publicly available Finance Sector emergency plans there appears to be have been little consideration and preparation in the sector for "Black Sky" level prolonged, widespread power outages that could last for a month or more. Preparing for Black Sky events in the Finance Sector would require at least three substantial additional areas of planning.

1. Emergency Generation and Refueling: although significant Finance Sector firms and organizations have emergency generators, it is questionable how many, if any, have addressed the logistics of repairing, refueling or replacing generators that would be required in a Black Sky level outage of a month or more.
2. Resilient Emergency Communications: well-prepared financial firms and institutions have built in multiple channels of communication to their emergency planning, including cellphone, landlines, broadband, satellite phones etc. However, it is far from clear how they would function if most or all ordinary communications channels were brought down, as could well happen in a Black Sky event.
3. Emergency Liquidity Facility: Planning for a Black Sky event requires consideration of how to maintain some basic mechanisms of payment and exchange when normal payment, transfer and ATM facilities may have broken down. Such an emergency payment mechanism will be important for facilitating the recovery activities of other sectors.

Sector Best Practices Matrix (On-going)

Area of Operations	Recommendation	Expected Improvement
Planning	All significant financial institutions should develop their business continuity plans to match the level set by current leaders in the field. The plans should be regularly tested and exercised, including cross-sector exercises.	Institutions with less developed business continuity plans adopt current best practices.

Planning and Operations	Financial institutions should develop plans for emergency generation that include provisions for refueling, repair and replacement of generators (e.g. through putting in place agreements with diesel and equipment suppliers)	Institutions would be equipped with emergency generation that can run for at least a month after a massive, prolonged power outage.
Planning and Operations	Planning for use of an appropriate emergency communication system for internal and external communication and data. This is necessary for both internal operational plans and coordination with external sectors. The planned Emergency Communication (BSX) System architecture under development by EIS Council could serve as a basis for these plans	Finance Sector institutions would have a Black Sky resilient communications system for use in the event that normal communications channels to not work after a Black Sky event.
Planning and Operations	Financial institutions together with government agencies plan how a basic mechanism for ensuring that payments and transfers can continue in a Black Sky event even if normal payment and transfer channels fail	Essential business transactions, especially those necessary for recovery activities, can continue.

Integrated and/or Shared Planning Actions

To be completed

Planning Actions Matrix

Response Area	Shared Planning Requirement/Interface Point	Cross-Sector(s) ID

Sector Black Sky Resilience Considerations Overview

There are a number actions and investments the Finance Sector should take to improve resilience against a Black Sky Event.

A Black Sky event will be widespread enough that outside assistance may not be available. In a coordinated cyber-attack or other Black Sky event, outside agencies may be reluctant or unable to provide assistance because of the possibility they will soon be attacked. The Finance Sector will need to ensure that there are sufficient numbers of trained staff to respond.

A Black Sky event will very probably disrupt communications systems. The EPRO BSX communications project is developing the architecture for a communications system that would withstand an EMP burst or cyberattack and satisfy the Finance Sector's need for emergency communications that would provide situational awareness and command and control after a Black Sky event.

Resilience Initiatives Matrix

Initiative Title	Initiative Description/Cost	Expect Outcome
Emergency staff training	Training to ensure sufficient numbers of qualified staff to maintain and recover systems in a Black Sky event	Adequate emergency staffing at principal and alternate operations locations
Emergency Communications BSX	Develop a resilient communication system that will provide voice, and possibly some data, transmission in the event of failure of telephone, internet, cell phone and satellite communications	Provide the minimally acceptable ability to maintain post Black Sky event financial sector operations as well as situational awareness and control

Sector Black Sky Regulatory Impacts and Issues Overview

Sector Regulatory Matrix

Area of Operations	Issue	Recommended Solution/Resolution

Sector Black Sky Essential Critical Infrastructure (MC) Overview

[This will necessarily focus on the digital platform and how to maintain it throughout Black Sky recovery]

Sector Critical Infrastructure Matrix

Element	Function

Sector Black Sky Specialized Skill Training Requirements Overview

[cyber restoration will be a vital skill and the number of experts will be short]

Sector Specialized Skill Training Requirements Matrix

Phase	Position/Skill	Training/Certification Requirement
	cyber	
	Generator operators	
	Generator mechanics	
	IT network engineers	

Annex A – Assessments (On-going)

Sector Overall Resilience Assessment (V2)

[FDIC the Federal Deposit Insurance Corporation conducts capacity assessments, but only for 'financial' hazards; it would be worthwhile to encourage them is to consider Black Sky assessments.]

Annex B – Regulatory Issues Detail Statements (On-Going)

Issue Statement 1

- Statement
- Decision Authority
- Required Documentation – To justify/document decision
- Resiliency Investment statement
- Plan Requirements
- Training Requirements
- Liability Statement/3rd Party Protection Issue
- Explicit requested legislative changes/Insurance/Assurance/3rd Party Indemnification

Annex C – Communications Requirements (V2/2.5/3/4)

Communications Requirement 1

- Internal/Planned Format/Path
- External/Planned Format/Path
- Explicit Model
    - Who
    - What
    - When
    - Strategies (back up)
    - Bandwidth requirement (actual and notional)
    - Format
    - Priority