

CHSR

**THE CENTER FOR
HOMELAND SECURITY & RESILIENCE**

**Ensuring
Systemic Resiliency
to Manage *Catastrophic Risk***

by J. Michael Barrett

Director, Center for Homeland Security & Resilience

26 September 2015

Contents

I. Background

II. Philosophical Approach

III. Ensuring Systemic Resilience

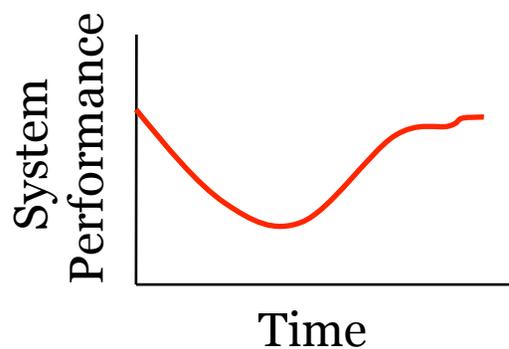
IV. Conclusions

I. Background:

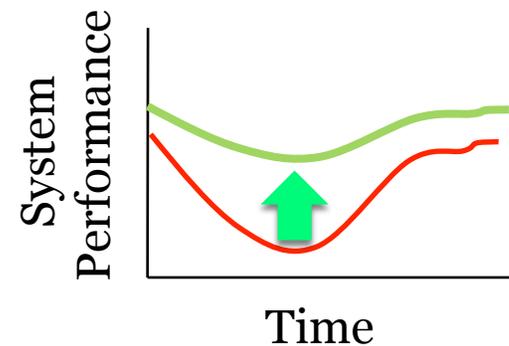
What is Systemic Resiliency?

Resilience: “An ability to recover from or adjust easily to misfortune or change.”
- Webster’s

The objective of Systemic Resiliency is to continue operations at an acceptable level during and after an event and to resume pre-event operations levels as soon as possible:



Vs.



In other words...

“Control how far you fall and how fast you recover.”

I. Background:

Examples of Systemic Resilience Solutions

ENERGY: The electric grid continues to operate at an acceptable level because, pre-event, investments were made in standardization of parts and configurations to enable interchangeable parts and quick replacement after disruption



COMMUNICATIONS: Acceptable levels of communication for responders, businesses and the sick and injured are ensured by rapid deployment of portable communications networks located aboard tethered dirigibles

TRANSPORTATION: Goods continue to flow using temporary, portable bridges whose footings and access ramps are pre-installed before the event, servicing traffic flow until the construction of a permanent bridge is completed



I. Background:

What is Catastrophic Risk?

According to DHS, “A catastrophic incident... results in **extraordinary levels of mass casualties, damage, or disruption** severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic incident could result in **sustained nationwide impacts** over a prolonged period of time; almost **immediately exceeds resources** normally available...”

I. Background:

What is Catastrophic Risk?

Different Agencies and actors have ***vastly different*** ideas of ‘**Catastrophic Risk**’:

Catastrophic can often be confused with ‘**mass casualty**’, which can mean **as few as 4-6 injured**, or whatever would overwhelm the local response capacity

I. Background:

What is Catastrophic Risk?

et... a RAND study, “*Considering the Effects of a Catastrophic Terrorist Attack*”, offers the following impacts of a “catastrophic” nuclear attack in Los Angeles:

10,000 people might die instantly from the blast itself or quickly thereafter from radiation poisoning.

10,000 more might be exposed to hazardous levels of radioactive water and sediment from the port, requiring emergency medical treatment.

completely destroy the entire infrastructure and all ships in the Port of Long Beach and the adjoining Port of Los Angeles.

1,000,000 people might try to evacuate the Los Angeles region.

gasoline supplies might run critically short

economic impact ... could exceed \$1 trillion, driven by outlay for medical care, insurance claims, workers’ compensation, evacuation, and construction. The \$100 billion to \$100 billion for 9/11 puts this figure into perspective.

I. Background:

Insights from the field

Most risk models are ***asset-based*** and ***probabilistic***, being derived from security/risk management models originally designed for ***asset-specific*** security

However, **systemic risk** and **cascading impacts** from the failure of **interdependent systems** belies the assets-based approach – because the **system is > the sum of the individual assets**

- Massive catastrophic events often result from non-linear, unpredictable changes, driving the need for ***systemic resilience***
- No alchemy of **estimation**, **historical analysis**, and **complex simulations** can divine a **fully correct number** for assigned risk
- Lacking precision, **actuarial-based risk calculations ignore** unlikely but potentially catastrophic events – and **misallocate resources**

I. Background:

Insights from the field

As a result, we are ***not good*** at fully preparing for ***truly catastrophic events***

- Low likelihood, high consequence issues have few supporters

A better approach is to work the issue backwards, defining what is necessary post-event and ensuring there is resiliency at that level

Resiliency is not about the assets themselves, it's about the systems' ability to meet minimally acceptable thresholds (MATs) of their primary critical functions (PCFs)

II. Philosophical Approach: *The 'Governance Gap'*

Federal Government is ultimately responsible for the **security of the nation as a whole** – *and they are the ONLY entity with the authority to address this risk* **because of the nature of the system that includes massive cascading effects**

Protecting all potential targets is neither feasible (too expensive) nor guaranteed to sustain the system (because each system needs the others in order to function)

Therefore, in practice, many/most DHS and other Federal efforts **support state/local and private sector owner/operator efforts** to protect **concrete assets** – not the system as a whole

As with fielding a national military for national security, the Federal Government can address the 'Governance Gap' that exists when a system's downstream risks are otherwise not addressed.

II. Philosophical Approach: *Thesis Statement*

“For truly Catastrophic Events, the most important national imperative is to ensure that major lifeline critical infrastructure sectors continue to operate and to bounce back as quickly and well as possible.”

the thesis is correct, then:

- Who Leads?
- What do they Do, and How?
- Who Pays?

The proper **Federal** focus is on ***continued functioning of the systems*** throughout our nation. This, in turn, requires a “System of Systems” approach, as follows:

Resiliency for Complex Adaptive Systems (RCAS)

can **complement** traditional **asset-based risk models** with **resiliency models**” aimed at **minimizing the cascading impact** of a catastrophic event

- Focus is on **ensuring** that the **Critical Infrastructure (CI) systems** continue to **operate** at a **minimally acceptable level**

requires mapping out the **interconnectedness** and **cascading effects** of losing any given systems upon the rest of the systems.

Then, determine **minimally acceptable throughputs** for specific systems and where **bottlenecks** occur during a given disruption

NOTE: this approach relies **less on complex math** and **more on expert elicitation** from on infrastructure personnel. This helps approximate real-world complexity of the major lifeline systems – **Food, Water, Power, Transpo, and Comm**

III. Ensuring Systemic Resilience: *The RCAS Approach*

Concept

Post-event **consequences** are deemed **acceptable**

Focus is **regional**

Emphasize **food, water, power, transpo, & comms**

Process

- Develop a manageable number of reasonable **catastrophic scenarios**
- Determine **acceptable levels** of CI operations
- Assess the **consequences** of the scenarios against a regional set of lifeline CI systems.

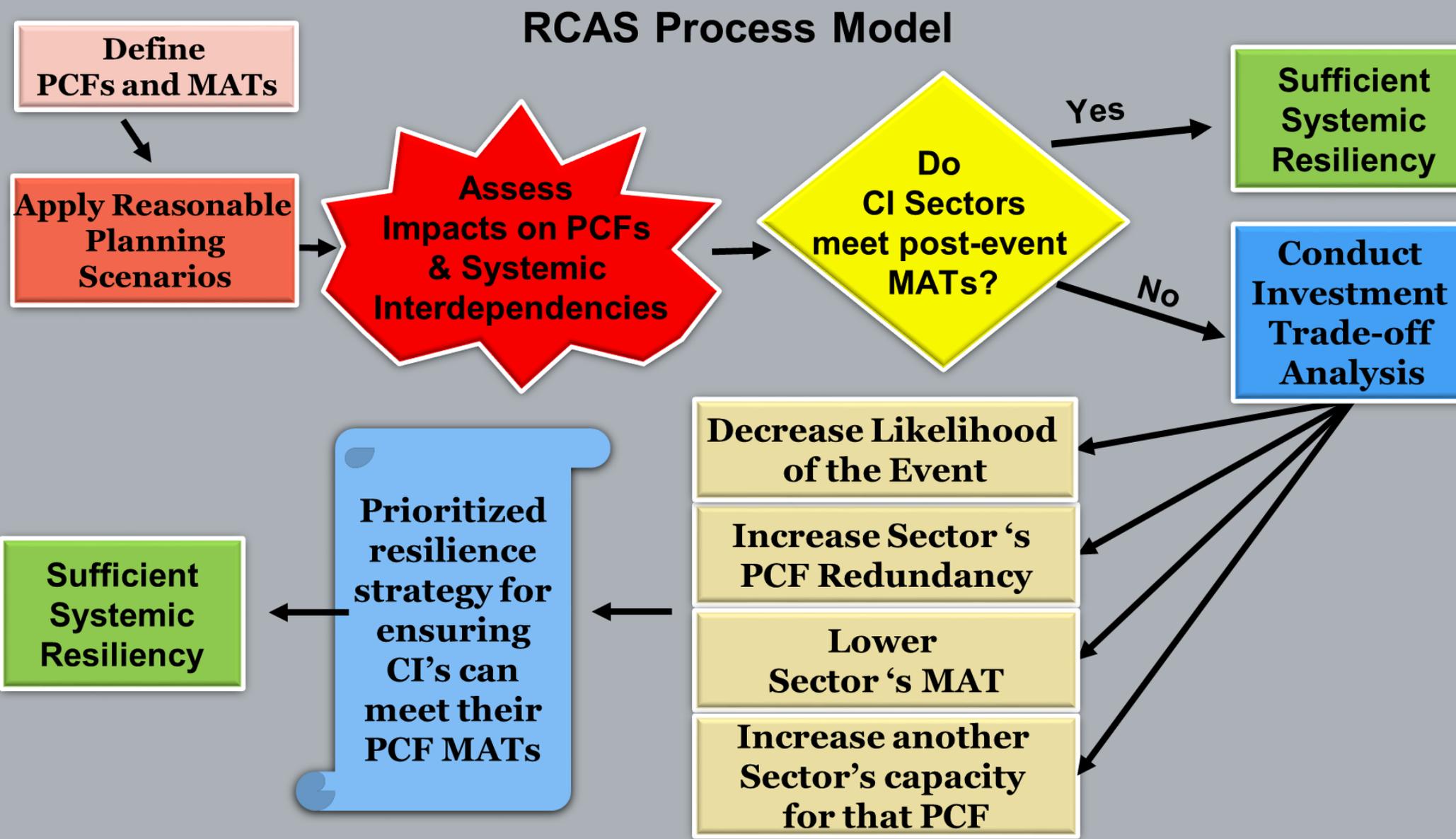
Starting Point

- ID plausible illustrative scenarios
- ID primary critical functions (PCF) per CI
- Define minimum acceptable threshold (MAT)

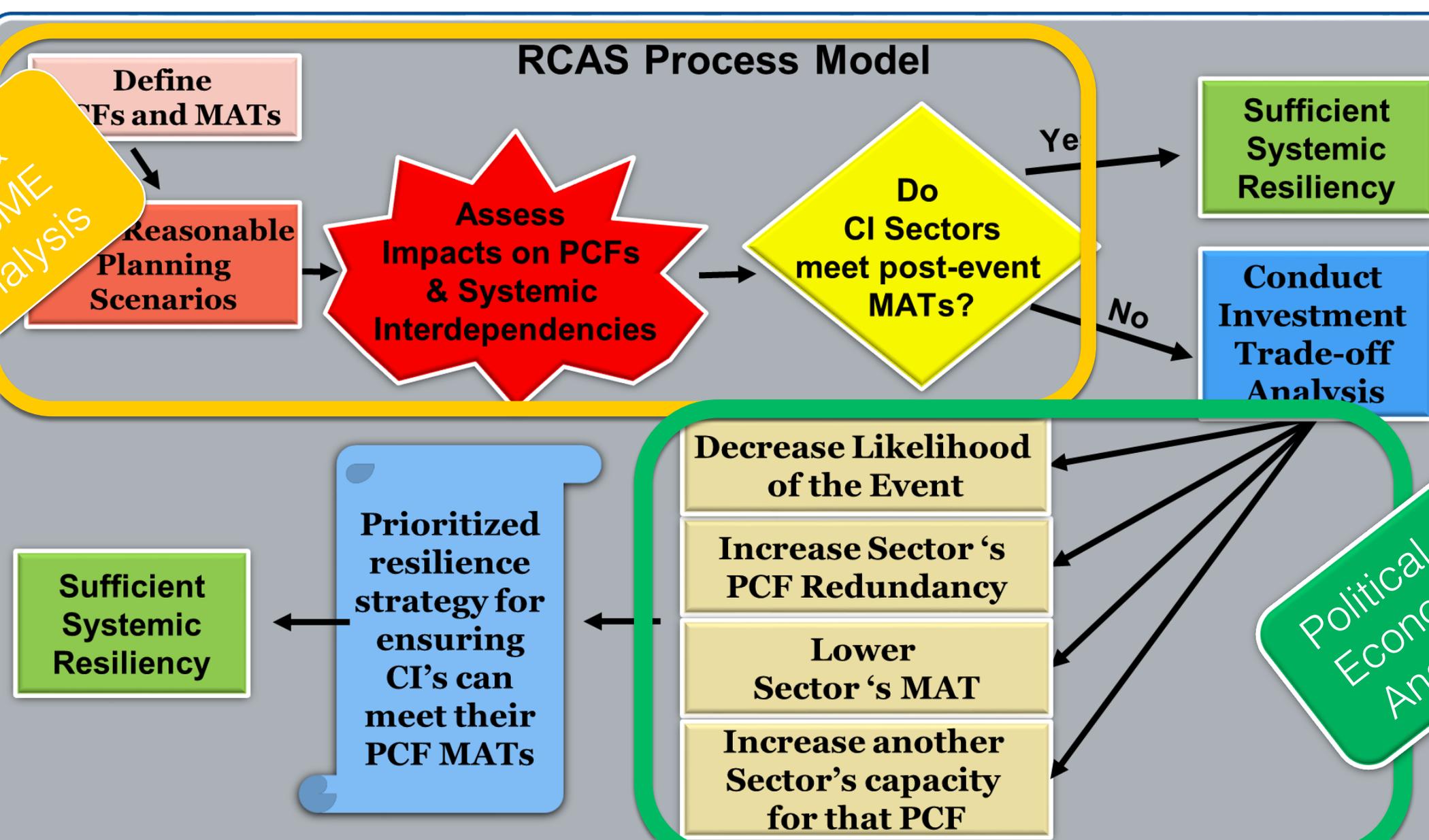
**NOTIONAL* Minimally Acceptable Thresholds (MATs)*

SECTOR	MAT, During Event	MAT, Immediate Aftermath	MAT, Long-Term
Agriculture & Food	75% of normal capacity	85% of normal capacity	95% of normal capacity
Banking & Finance	99%	99%	99%
Chemicals	80%	90%	95%
Energy	70%	80%	90%
Transportation	75%	80%	90%
Water	85%	90%	95%

III. Ensuring Systemic Resilience: *The RCAS Process Model*



III. Ensuring Systemic Resilience: *The RCAS Process Model*



III. Ensuring Systemic Resilience:

3 Key Factors in Systemic Resilience

Ability

The degree to which a specific infrastructure or system plays a role in supporting the overall prevention, preparedness, mitigation, response and recovery with regard to a hazard. The infrastructures and systems they support often play important roles in mitigating the impact of hazards before, during, and after they take place, and capturing their relative role in supporting operational continuity in the face of specific hazards.

Ability

The degree to which a given hazard impacts a particular infrastructure or other system. By creating representative disaster scenarios based on expert analysis and informed by historical events, various critical infrastructure systems experts can be surveyed to assess the impacts of these hazards on the systems. This analysis produces a tiered list of the hazards that cause the greatest impact for each of the specific infrastructures and systems.

Interdependency

The degree to which it supports other systems, for individual critical infrastructure systems that support each other (for example, electricity is required to pump water, and both are required for normal operational continuity), and proper functioning often requires the systems to function together in tandem. Assessing these critical infrastructure systems individually to capture their importance in supporting each other, and therefore their role in continuity of operations as a whole, is a crucial task in achieving systemic resilience.

III. Measuring & Modeling Resilience: *Sample RCAS Investment Alternatives*

Installing
redundant power,
telecoms, other
networks

Developing and
storing temporary
power/telecoms/
etc. networks

Training and
exercises

Cross-training
personnel

Relocation
and repositioning of
equipment and
personnel

Redundant
equipment,
infrastructure,
multiple vendors

Emergency
command and
control structures /
resilient
communications

Flexible emergency
business operation
policies

Use of multiple
vendors

Waiving certain
regulations

Re-routing /
relocating key
functions

Mutual aid p
sharing reso

III. Ensuring Systemic Resilience: *Driving Smarter Investments!*

1. Decreasing the likelihood of the event

- Prevention, such as increased radiation scanning

2. Increasing sector's Redundancy

- Redundancy and Reserves, such as increasing the overall power generation capacity or investing in modular/interchangeable designs

3. Lowering the sector's MAT

- Reset, such as public information campaign to reduce psychological impacts of an event, enabling a lowered MAT

4. Increasing another sector's capacity

- Substitutes, such as increasing the ability to import food through the transportation sector inherently lowers the MAT for agriculture & food

IV. Conclusions:

The Governance Gap

old model for managing risk was to draw out **discrete, singular risks** to protect against the **most likely** and **the worst** of them by protecting **asset level**.

ay's networks are **too large, change too fast**, and cover **too many complex interdependencies** to use such a linear approach.

neither possible nor sufficient to **strengthen the weakest points** or **spread resources thinly** across every possible point of attack or failure

ead, we must determine what is critical to **ensuring the system is viable and durable** enough to continue to operate at acceptable levels and take measures to implement solutions that address current gaps

... But ONLY the Federal Government can fill this gap!

IV. Conclusions:

Federal Roles & Responsibilities

Federal entities should:

Continue to support State/Local and Private Sector efforts by coordinating best practices and standardization

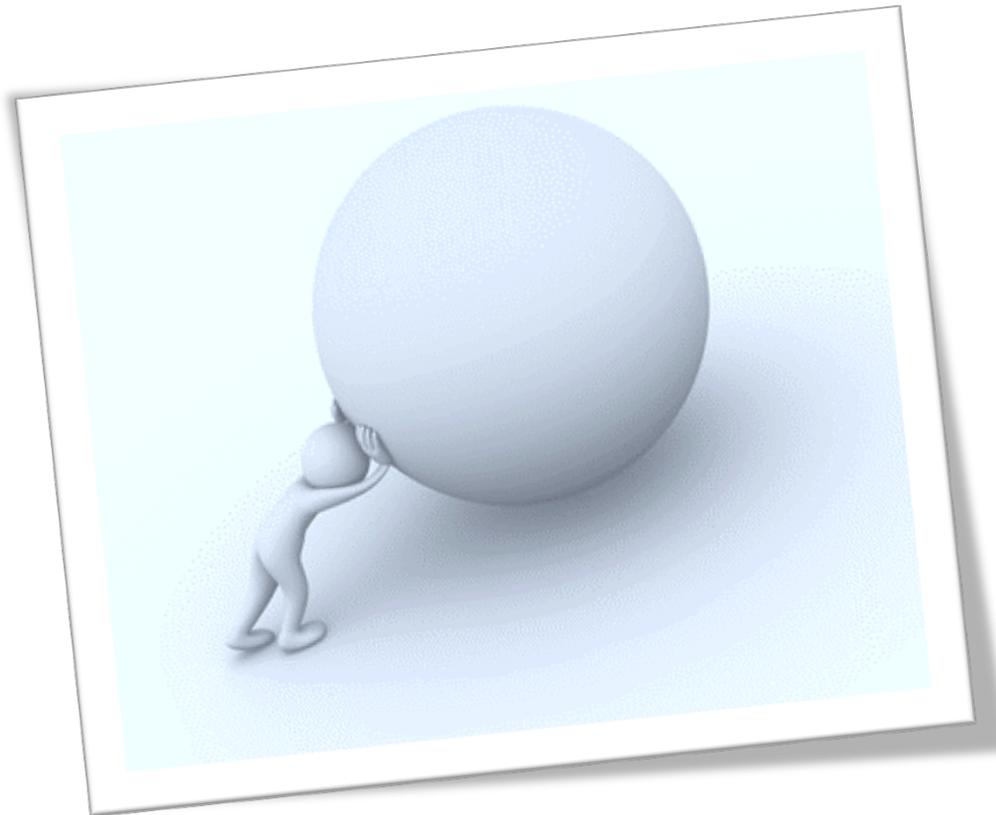
Severity of impact in state/local case determines Fed involvement

Main Fed involvement should focus on limiting spread of the impact (where applicable)

BUT also must address the problem top-down, looking first at existential threats and “systems of systems” analysis to ensure COOP/COG and survivability of truly strategic CI, i.e., **Food, Water, Comms, Power & Transportation**

Look at breakpoints in capability of systems where impairment would be catastrophic

Is Resilience Modeling for Catastrophic Events worth it?



THE CENTER FOR
HOMELAND SECURITY & RESILIENCE

**If you knew 10,000 or 100,000 or more
could be impacted,
what wouldn't you do to get ready?"**

QUESTIONS?

**For more
information:**

Mike Barrett

(703) 899-0066

mbarrett@security-resilience

www.security-resilience.org

BACK-UP SLIDES

Roles & Responsibilities: State/Local & Private Sector

State / Local and Private Sector should:

Identify and protect individual assets

Continue asset-based security and reasonable redundancy, excess capacity, and use of alternate systems that meet the reasonable business imperative of the entity.

Coordinate with the Federal government on facilitating COG and strategic survivability as well as take lead on asset level risk management efforts.

Prepare to lead local and regional response/recovery efforts

A Systems-Based Critical Functions Model

Determining "*how much resilience is enough?*" using a Systems-Based Critical Functions model:

Define each CI sector's Primary Critical Function (PCF)

Define Minimally Acceptable Operational Capacities (MATs) for each sector's PCF;

Evaluate each sector's relative current resiliency for meeting its PCF MATs

- Assess the consequences of illustrative event scenarios acting upon PCF's of the CI sectors;
- Measure current gaps between the consequences of the HLS threat and the PCF MAOCs;

Remedy the resiliency gaps by investing to ensure the CI sectors can meet the MATs of their PCFs.

RCAS Process Model

Define
and MATs

Reasonable
Planning
Scenarios

Assess
Impacts on PCFs
& Systemic
Interdependencies

Do
CI Sectors
meet post-event
MATs?

Sufficient
Systemic
Resiliency

Conduct
Investment
Trade-off
Analysis

- Decrease Likelihood of the Event
- Increase Sector's PCF Redundancy
- Lower Sector's MAT
- Increase another Sector's capacity for that PCF

Prioritized
resilience
strategy for
ensuring
CI's can
meet their
PCF MATs

Sufficient
Systemic
Resiliency

