SANDIA REPORT
SAND2013-4664
Unlimited Release
Printed May 2013

The Future of Infrastructure Security:
A workshop held at Sandia National Laboratories

Pablo Garcia
Interdependency and Consequence Effects Department

Jessica Glicken Turnley
Policy and Decision Analytics Department

Lori K. Parrott
Policy and Decision Support Analytics Department

Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185-1138

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation,
a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's
National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online order:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2013-4664
Unlimited Release
Printed May 2013

The Future of Infrastructure Security:
A workshop held at Sandia National Laboratories

Pablo Garcia
Interdependency and Consequence Effects Department

Jessica Glicken Turnley
Policy and Decision Analytics Department

Lori K. Parrott
Policy and Decision Support Analytics Department

Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185-1138

Abstract

Sandia National Laboratories hosted a workshop on the future of infrastructure security on February 27-28, 2013, in Albuquerque, NM. The 17 participants came from backgrounds as diverse as federal policy, the insurance industry, infrastructure management, and technology development. The purpose of the workshop was to surface key issues, identify directions forward, and lay groundwork for cross-sectoral and cross-disciplinary collaborations. The workshop addressed issues such as the problem space (what is included in 'infrastructure' problems?), the general types of threats to infrastructure (such as acute or chronic, system-inherent or exogenously imposed) and definitions of 'secure and resilient' infrastructures. The workshop concluded with a consideration of stakeholders and players in the infrastructure world, and identification of specific activities that could be undertaken by the Department of Homeland Security (DHS) and other players.

ACKNOWLEDGMENTS

We would like to acknowledge Mercy Berman, Richard Sweeney, Jennifer Hutchison, Dan Horschel, Steve Conrad, Charles Rath, and Theresa Brown for their assistance with this workshop. In addition, Jessica Glicken Turnley provided expert tutelage and facilitation of our planning process and the workshop, as well as the drafting of this report.

CONTENTS

FIGURES

NOMENCLATURE

DHS	Department of Homeland Security
IPCC	Intergovernmental Panel on Climate Change

EXECUTIVE SUMMARY

Sandia National Laboratories hosted a workshop on the future of infrastructure security on February 27-28, 2013, in Albuquerque, NM. The 17 participants came from diverse backgrounds, representing federal policy makers, the insurance industry, infrastructure managers, technology developers, academe, the finance sector, and others. The purpose of the workshop was to surface key issues, identify directions forward, and lay groundwork for cross-sectoral and cross-disciplinary collaborations.

All comments were made in a non-attribution environment. The workshop was held on-site at Sandia National Laboratories, and facilitated by Jessica Glicken Turnley of Galisteo Consulting Group, Inc.

The workshop discussion began by addressing the problem space – defining what is included in 'infrastructure' problems. The focus then moved to the general types of threats to infrastructure (such as acute or chronic, system-inherent or exogenously imposed) and then turned to a definition of success factors. What is meant by 'secure and resilient' infrastructures? How would we know if we were successful? The workshop concluded with a small group exercise addressing defined questions about the range of stakeholders and players in the infrastructure world, and identification of specific activities that could be undertaken by the Department of Homeland Security (DHS) and other players.

Participants discussed infrastructures as a distribution system, which includes hard assets and systems and networks of various types, designed to distribute a service that fulfills some social function. The discussion underscored the public good generated by infrastructure systems and the associated responsibility of the government to manage infrastructures to ensure delivery of that good. Equity issues come into play when considering the allocation of services, as do the deliberate use of infrastructures to foster large social agendas. Participants noted that in addition to preserving, restoring, and improving functions and structures, a resilient infrastructure system might curtail certain functions and structures as they outlived their social usefulness. The goal, they suggested, was a state of *acceptable functionality*, not a restoration of the *status quo ante* or maintenance of the *status quo*. As society changed, so would the definition of 'acceptable.'

There appeared to be consensus that the infrastructure system in the US should be defined with a baseline of service provision for which the government should be responsible. The workshop clearly recognized the public good provided by infrastructure systems and the difficult questions of equities and allocation that were raised. The construction of new infrastructure systems can be used to exercise large social and political agendas as their planning, construction and existence can significantly change population footprints. Rebuilding to the *status quo ante* after an acute event can perpetuate existing social patterns that can be either good or bad. Infrastructure systems can be a powerful mechanism of social change.

The intersection between this public good and the private ownership of many of the hard assets stimulated some interesting discussion on the assumption of risk management (which is distinct from the allocation problem) and raised very important questions of governance. In addition to the public-private relationship, the multi-jurisdictional footprint of many infrastructure systems requires a hard look at many governance issues. The workshop discussion recognized the contribution of local communities to the resilience question as well as the impact of the American geopolitical position on both the security and resilience of infrastructure systems.

This strong social component led to agreement that the problem of the future of infrastructures is not primarily a technical issue but is also a people issue.

Participants identified change factors that could impact infrastructures of the following types: changes in social expectations of infrastructure systems, changes in stresses on infrastructure performance, and changes in the nature of the infrastructure systems themselves. Threats included aspects of our culture, aspects of the system we do not understand, demographic changes, and threats largely out of our control such as weather. Participants made an initial and recognizably incomplete effort at defining players in this complex world. They developed suggestions for innovative public-private partnerships, and suggested some new areas for research in both the technical and social domains.

The workshop raised but did not resolve several questions related to different aspects of infrastructures.

- What are we trying to achieve with policies and activities around infrastructures? Are we trying to maintain a certain quality of life (perhaps phrased as maintain the status quo), open new markets, shift population footprints…? Are we clear and explicit on these goals?
- What will the next generation economy and society look like? How can we learn enough so we can build to tomorrow, not just today?
- How much is enough? And where should it be? Who decides who gets what? Who manages these equities and how?
- How do we determine what ‘acceptable’ functionality looks like?
- How is responsibility for developing, repairing, maintaining and protecting infrastructures allocated to and (not) accepted by the individual citizen, local communities, governments, and the private sector?
- How should the multi-jurisdictional nature of many infrastructure sub-systems be managed?

1 INTRODUCTION AND BACKGROUND

Sandia National Laboratories hosted a workshop on the future of infrastructure security on February 27-28, 2013, in Albuquerque, NM. (See Appendix A for letter of invitation.) Participants came from diverse backgrounds, representing federal policy makers, the insurance industry, infrastructure managers, technology developers, academe, the finance sector, and others. The purpose of the workshop was to surface key issues, identify directions forward, and lay groundwork for cross-sectoral and cross-disciplinary collaborations.

There were 17 participants at the workshop: a list of participants can be found in Appendix B. Per agreement with the participants, all comments were made in a non-attribution environment.[1] The workshop was held on-site at Sandia National Laboratories, and facilitated by Jessica Glicken Turnley of Galisteo Consulting Group, Inc.

The workshop engaged participants through a variety of formats which allowed individuals with different participatory styles to engage fully. As participants entered the workshop room, they were directed to large pieces of paper topped by questions on the walls. Participants were encouraged to write comments, thoughts, ideas, comments on comments and the like during the course of the workshop. All writing on the paper was anonymous. In addition to this written brainstorm, the workshop used more traditional techniques of facilitated large group discussions, and small breakout groups focused on specific topics. There also was plenty of time during breaks for participants to exchange thoughts and ideas.

The evening opening session for the workshop began with context-setting remarks from the hosts, and introductions and contributions from all participants. (An agenda for the workshop can be found in Appendix C.) This was followed by a small group/plenary session exercise designed to orient participants to the topic and desired time-frame for the problem space, and stimulate out-of-the-box thinking. The program for the second day moved from a definition of the problem to a focus on the threat and other factors of change to a discussion of success. The workshop ended with suggestions for possible paths forward.

2 SETTING THE CONTEXT

Pablo Garcia, Program Manager of Resilient Infrastructure Systems at Sandia and attached to the National Infrastructure Simulation and Analysis Center at the labs, and Ms. Durkovich, the Assistant Secretary for Infrastructure Protection in DHS, set the context for the workshop with their opening remarks. They pointed out that those concerned with protecting the nation's infrastructures need to look at far more than the types of malevolent adversaries that perpetrated the 9/11 attacks and stimulated the creation of DHS. Natural hazards with devastating consequences such as Superstorm Sandy and other extreme weather events, the natural processes of aging, fiscal constraints, and strategic national security risks also challenge the viability of the nation's systems of infrastructures in some way. The long life cycle of an infrastructure system (some of current infrastructure systems like the interstate highway system are over 50 years old; others such as some water systems are over 150 years old) force a long planning horizon – perhaps as long as 100+ years. Consequently, response and management regimes cannot be

[1] Although there were women as well as men attending the workshop, when we refer to participants in the report we always use the male pronoun. This is for convenience sake only, and is not to infer that the female participants were silent.

solely a governmental responsibility.[2] Input, engagement and action from a wide variety of sectors (government, private, non-profit, etc.) are needed to craft a holistic response to any of these change factors. Hence the breadth of perspectives represented at the workshop is critical to crafting viable approaches.

The workshop began with introductions. As participants introduced themselves, they were asked to present the group with a one-sentence thought related to infrastructure. Pre-workshop instructions described the one sentence as an odd fact, a future prediction, an observation, a question – or anything else related to infrastructures the participant thought might be of interest to others at the workshop.

The list below gives those one-liners. They are presented in no order. As participants often volunteered more than one sentence, some of the one-liners below are synopses or précis of longer statements.

- Valid solutions must be robust to uncertainty
- Infrastructure issues are a govern*ance*, not a govern*ment*, problem
- While we often think of climate change and terrorism as the biggest concerns, perhaps the most significant risk to infrastructures is austerity
- We need to figure out how to manage the inevitable increase in foreign capitalization of our infrastructures
- As Yogi Berra said… "The future ain't what it used to be!"
- A significant 'grey swan' event will affect food and agriculture sometime over the next 25 years
- The solution often is to skip over the current problem
- From 2002-20012, fatalities from pipeline accidents have roughly equaled those from commercial airline accidents
- When do small events aggregate or grow to a point where they are consequential enough to become the concern of a government agency such as DHS?
- Our focus needs to be on the infrastructure as it will be 100 years in the future
- Given the inter-jurisdictional nature of infrastructures, how do we optimize governance across multiple entities?
- Each infrastructure will 'get smart' at a different rate; how do we manage the different rates of development?
- Infrastructures are not engineering artifacts but agents of change

[2] This position – that critical infrastructure security and resilience is a "shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure" – and other policy dimensions are articulated in Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

- How do we learn lessons from the entities (e.g. localities, municipalities, countries organizations) that are ahead of the game?
- Decentralization will change the resiliency problems faced by infrastructures
- ‘Infrastructure’ is a public good
- How important is an understanding of the psychology (attitude of the users) to an expectation of infrastructure resiliency?

After this introductory exchange, participants self-selected into three small groups for a discussion exercise. The purpose of the exercise was to use the introductory remarks and the contributions by participants as stimulants for thinking about hypothetical problems. This would orient participants to the topic and desired time-frame for the problem space, and encourage out-of-the-box thinking.

The assignment was as follows:

> The year is 2025. [CHANGE FACTOR] has been at play. What is the impact on the system of infrastructures and what are the implications for changes (if any) in governance approaches to that system?
>
> We do not expect you to come up with a complete and elegantly formed answer, but rather to explore some of the unexpected pathways this change factor might open or close.

Each group was given the following four change factors. They could select one to discuss in depth, or treat some or all of them.

- Everyone has a smart phone with full 24/7 access to the internet and a complete suite of applications.
- The United States (federal, state, local governments) has put virtually no money into refurbishing and upgrading the interstate highway system and local streets.
- Because of security threats we believe are originating outside the country, we have beefed up security on all modes of public transportation including trains and busses as well as air travel, resulting in long lines and significant extra travel time on all modes of transportation. Security has also been increased at our borders (including passport control at airports, cargo inspections at sea ports and land crossings) resulting in crossing delays of many hours or even days.
- The population footprint of the United States has changed significantly. Internal migration has resulted in significant population increases along the East and West coasts, creating megacities. At the same time, many more retirement and recreation communities have been built in rural areas near large expanses of wilderness, while the farming communities of the Midwest are depopulated.

All of the groups addressed the impacts of the changes in population footprint, although in slightly different ways. One of the groups briefly addressed all the questions; the other two focused primarily on the megacities problem.

The impact of concentrations of people on infrastructure performance and development stimulated much of the discussion. Such concentrations would have a ripple effect, perhaps leading to different technologies and configurations for (e.g.) food production such as the development of vertically stacked fields close to consumption centers. There also was talk about ‘tipping points,’ i.e., when government support of certain infrastructures might be abandoned or (conversely) assumed. Participants were interested in what such a tipping point would look like. What would stimulate it? Would it be a bottoms-up phenomenon or would governments decide that they no longer would support a certain lifestyle? And if access to infrastructures really is a public good, how do equities affect these types of discussions? There was talk about the attractive power of infrastructures, the recognition that the presence of an infrastructure system (such as healthcare or electricity) is itself an agent for change. There were comments about the opportunity to use that attractive power in a mindful and considered manner.

The distinction between governance and government was made several times. The recognition both of the interconnectedness of infrastructures and (perhaps more emphatically) the recognition that infrastructure systems cross jurisdictional boundaries stimulated discussion of regional solutions and the need for interagency and intergovernmental cooperation. Although market-based solutions were proposed to some of the problems around infrastructure scarcity, it was recognized that these could raise questions of equity and equality… which again brought the discussion back to one of governance and the nature of the public good infrastructures provide.

3 THE PROBLEM SPACE

The discussion of the problem space began by recognizing the difference between problems related to in-place or aging infrastructures, new or proposed infrastructures, and re-built or renewed infrastructures. New systems, for example, can stimulate social change, which can have cascading effects on the initiating infrastructure as well as on others and on other social systems. Rebuilding to the *status quo ante* can perpetuate existing social patterns which can be either good or bad. These and similar points emphasized the discussion to the recurring theme of the public good and associated equity issues.

Participants did address the question of the boundary of an infrastructure ‘system.’ Does an infrastructure consist only of its physical assets? Of the assets and the people who consume the infrastructure service? What about the regulators and governors?

As a way to direct the discussion, one participant suggested the following definition: Infrastructures are the assets, systems, and networks which produce functions necessary for our economy and way of life. One participant suggested that rather than think of ‘assets, systems and networks’ as an infrastructure problem, think of it as a distribution problem. Critical elements are a good or service that needs to get somewhere, and whatever it is that gets that good or service where it needs to go. The infrastructure problem thus becomes a true network problem where the key is to leverage the betweenness[3] of critical nodes. He gave an example of a small rural community where the ‘node’ with the greatest betweeness was the Catholic church (the building). Once that was understood, distribution problems within the community could leverage that structure as well as the social network that caused the structure to be built (the Catholic church as an institution). This is a strong re-framing of the problem. It suggests that

[3] ‘Betweenness’ is a term from network analysis that measures the degree to which one actor in a social network (or node in a physical network) connects other, non-adjacent actors (or nodes). Actors or nodes with high betweeness connect large numbers of other actors or nodes that otherwise would have no connections, and so play critical and unique roles in network functions.

using the hard and soft assets of the Church (buildings, social connections) may be the most efficient distribution mechanism. Does this, then, make the Church part of the infrastructure? Or just the church building?

The comments quickly turned to the question of ‘criticality’ – which infrastructures are critical? How ‘much’ of each system is critical? And who decides? The recognition that at least some portion of infrastructures and the services they provide are public goods (and hence critical?) while the remaining portion is market-driven highlights the inherent tension in discussions about infrastructures in this country, as many of the assets which provide that public good are privately owned. Most participants agreed that there should be some collective (government) responsibility for the ‘critical’ portion of service or goods delivery, with the market driving the rest. However, this raised the question of how to determine an economic value for an infrastructure and the service it provides. As many of the costs of the ‘critical’ portion are externalized because of the public good component, it is difficult if not impossible to do a full market valuation. (One participant suggested looking at how the environmental field is using a concept of ecosystem services to ‘value’ ecosystem functions. He suggested that a similar method might be utilized for infrastructure services.)

The public good discussion caused some participants to warn against the ‘disease of the peak’ – planning systems around peak use or demand, whether that peak be defined in time or space. Should an electricity delivery system be designed against Superstorm Sandy or against less stressful but more common storms? This raised the question of how one plans for events that are outliers today but may not be in the future. Superstorms like Sandy may become the norm, not the exception – how do we recognize and plan for that type of a future? It also raised the question of the responsibility of the citizen. How much inconvenience should an individual bear (is it acceptable for the power to be off for 24 hours but not for 48?) – and what is the associated responsibility of the collectivity to mitigate or prevent inconvenience?

The question of criticality and the notion of the ‘disease of the peak’ turned the discussion directly to the problem of allocation and equity. As one participant pointed out, risk management is not the same thing as allocation. Allocation involves the recognition and management of equities. In a world of scarce resources, how do we allocate scarce capacity in an equitable fashion? And if we plan with a scarcity mentality, will we be able to design a system that serves the economy of the future?

Participants explored several other important political questions. What does equity mean, in this context? When the economy changes, how do we change investment equations while still appropriately managing the equity issues? Furthermore, when discussing public investment in infrastructure, we need to be cognizant that the federal government can execute different types of financing instruments than can state and local governments because of its ability to manage the money supply. As a consequence, its investment planning will look different. And as planning models shift from large, centrally financed, capital-intensive systems to more distributed and locally financed systems; this distinction could become quite significant.

This brought the discussion back to the social utility of infrastructures. What do we as a society want to achieve with them? They can be used to open new markets or foster geographic expansion (think of the interstate highway system in the US in the 1950s and 1960s), to contribute to national defense (like some parts of the cyber network), to support economic development (roads, sanitation, fiber optics, telecommunications into rural or new urban neighborhoods), or for other social purposes. Although participants raised the question, there was no consensus in the room regarding a large social agenda or direction that should be stimulated by infrastructure development.[4]

This underscored the social dimension of the definition of infrastructures and addressed our collective expectations of these infrastructures. One participant noted that in this country in addition to expectations about service delivery, we also have certain aesthetic expectations (think of cell phone towers disguised as trees) and environmental requirements (pollution regulations for power generation, for example, or concerns about harm to birds from wind farms) of our infrastructures. Others pointed out that we in the US are at a point in our economic development where we have the luxury to worry about things like aesthetic standards. In developing economies, the expectation often is purely functional.

One participant summed up the discussion with the statement that "the problem is not the technology, it's the people." Several agreed with him, and no one challenged him.

To summarize: infrastructures are a distribution system, which includes hard assets and systems and networks of various types, designed to distribute a service which fulfills some social function. Some participants wanted to limit the infrastructure definition to the distribution system, focusing particularly on the hard assets. However, the discussion about the future of infrastructures identified the public good generated by infrastructure systems and the associated responsibility of the government to manage infrastructures to ensure delivery of that good. The strong social component led to agreement that the problem of the future of infrastructures is not primarily a technical issue but also is a people issue. Equity issues come into play when considering the allocation of services, as do the deliberate use of infrastructures to foster large social agendas. As a result, there appeared to be consensus that the infrastructure system in the US should be defined with a baseline of service provision for which the government should be responsible to recognize and manage the public good component. Any services above that baseline should be driven by the market with pricing mechanisms allocating demand.

4 FACTORS DRIVING CHANGE

The discussion then turned to change. What were factors that could drive changes in the ways in which we approach infrastructures? Participant responses addressed changes in social expectations of infrastructure systems, changes in stress factors, and changes in the nature of the infrastructure systems themselves. We present a list of changes offered. The list is in no particular order. Note that some factors appear in more than one section.

4.1 Factors Driving Changes in Expectations of Infrastructure Systems

- Political will
- Generational changes with associated changes in expectations of government
- The state of the economy

[4] Ed. Note: not only was there not consensus among participants, they really did not discuss any large political agendas, whether they agreed with them or not – just recognized the role infrastructures can play in their execution.

- The global geopolitical environment, particularly changes in the US position in it
- Re-definition of national security, broadening it to focus on protection of a way of life
- Migration and associated changes in population footprints
- More awareness of and attention to the problems of infrastructures
- Population growth and other demographic changes (aging, etc.)
- Newly built infrastructures providing access to services in places that previously didn't have them, or access to new types of services
- Intellectual property theft
- Privacy-related concerns
- The changing relationships between a global network of corporations and sovereign states

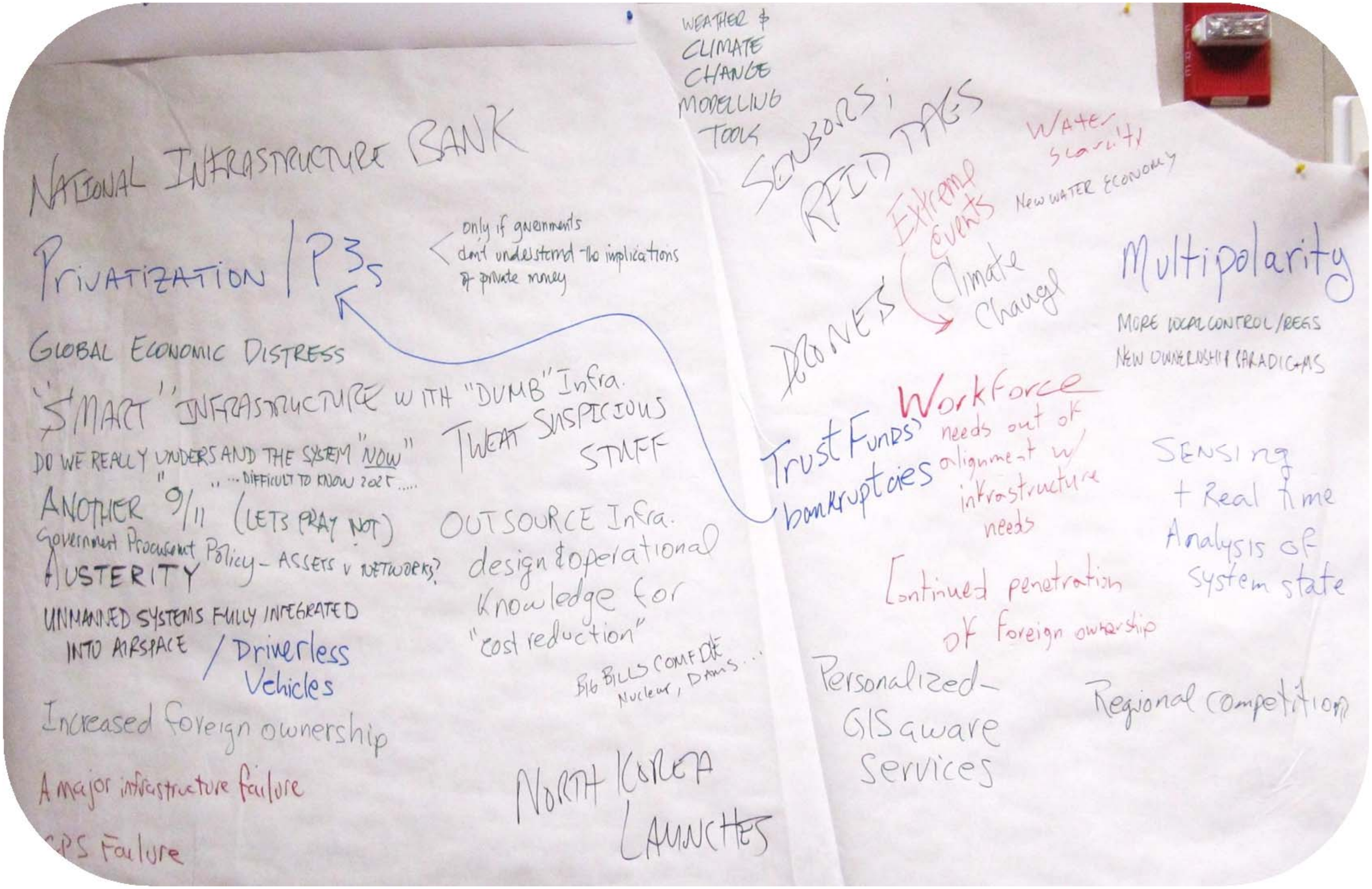
4.2 Factors That Will Stress Infrastructure Performance

- Climate change
- Acute events (weather, meteorites, other) becoming more frequent and increasingly severe
- Population growth and other demographic changes (aging, etc.)
- Newly built infrastructures
- Aging

4.3 Changes in the Nature of the Systems

- Changes in technology – both the rate of change of technology and new technologies, including GPS, those related to transparency and visibility, and self-monitoring systems,
- Increasing interdependencies among infrastructure systems
- The increasing complexity of the supply chain
- The increasing complexity of ownership/management
- Increasing regulatory complexity
- Newly built infrastructures
- The increase in larger, more centralized systems

Identification of change factors was one of the topics of the written brainstorm. To honor the connections between and comments about contributions to the brainstorm, rather than reproduce the list from the paper on the wall here, we provide a picture of the brainstorm page in Figure 1.



NATIONAL INFRASTRUCTURE BANK

PRIVATIZATION | P3S

only if governments don't understand the implications of private money

GLOBAL ECONOMIC DISTRESS

"SMART" INFRASTRUCTURE WITH "DUMB" Infra.

DO WE REALLY UNDERSAND THE SYSTEM "NOW"
" " ... DIFFICULT TO KNOW 2025 .....

ANOTHER 9/11 (LETS PRAY NOT)

Government Procurement Policy – ASSETS v NETWORKS?

AUSTERITY

UNMANNED SYSTEMS FULLY INTEGRATED INTO AIRSPACE / Driverless Vehicles

Increased foreign ownership

A major infrastructure failure

GPS Failure

TWEAT SUSPICIOUS STUFF

OUTSOURCE Infra. design & operational Knowledge for "cost reduction"

BIG BILLS COME DUE Nuclear, DAMS...

NORTH KOREA LAUNCHES

WEATHER & CLIMATE CHANGE MODELLING TOOLS

SENSORS; RFID TAGS

DRONES

Extreme events (Climate Change

Water scarcity

NEW WATER ECONOMY

Multipolarity

MORE LOCAL CONTROL/REGS

NEW OWNERSHIP PARADIGMS

Trust Funds' bankruptcies

Workforce needs out of alignment w/ infrastructure needs

SENSING + Real time Analysis of System state

Continued penetration of foreign ownership

Personalized – GIS aware Services

Regional competition

Figure 1: Written Brainstorm - Change Factors

Participants then briefly discussed the change factors that have made infrastructures an issue of concern today when they were not two decades ago. Clearly in recent years our infrastructure systems have been used against us: the transportation infrastructure on 9/11 and cyber-attacks are two examples, although there are others. Our recognition of the increasing interdependencies of infrastructure systems also suggests increasing vulnerabilities and possible required changes in governance and management systems. And finally, there has been increasing centralization and automation of the design and operation of infrastructure systems – but not of the authorities governing them (for example, there are 47 federal entities involved in energy policy decision making). The cross-jurisdictional nature of many infrastructure systems raises important issues of governance.

Participants were clear that we as a society could respond to infrastructure change in one of three ways:

- We could re-build to old standards and patterns – reinstate or try to maintain the status quo
- We could build to new standards and configurations – use infrastructure development as a means to help achieve social goals
- We could do nothing

This again pointed to the critical role infrastructure development can have in shaping a society, and the concomitant social responsibility put upon those who must allocate resources to infrastructure security.

To summarize: Change factors can be of the following types: changes in social expectations of infrastructure systems, changes in stresses on infrastructure performance, and changes in the nature of the infrastructure systems themselves. There has been increasing attention paid to infrastructures in the last two decades because of changes in the nature of the system itself. We are aware of the increased interdependencies among the parts of the system and of the increased complexity of the system itself, partially made visible by the cross-jurisdictional nature of many of its component systems. Since infrastructures have been used against us in very visible fashions recently (think 9/11 and cyber-attacks for example), we are recognizing the critical roles infrastructures play in defining and maintaining our way of life and the associated necessity of protecting them.

5 THREATS

The next question posed to participants was that of threats. Participants offered the following list, again in no particular order. They are roughly divided among socio-cultural threats, i.e. resulting from American cultural propensities or consequences of our way of life; threats over which we have little control; threats arising from our inability to understand or manage some aspect of the system; and demographic changes.

5.1 Socio-cultural – Aspects of the American Landscape or Consequences of Our Way of Life

- Neglect
- Societal tolerance or intolerance for the infrastructure (think of the changing attitudes towards nuclear power)
- Societal memory (as memory of extreme events fades, for example, we may be more reluctant to include them in the risk equation)
- Hubris
- An effective short-term response capability which may mask a lack of attention to long-term problems
- Short-term planning regimes based on short-term political and economic agendas addressing problems with long time horizons
- The need to exploit resources in extreme environments as resources become scarcer
- Limited availability of natural resources (scarce resources)
- Growth of information and misinformation ("I read it on the internet so it must be true…")

5.2 Factors Generally out of Our Control

- Extreme weather events and natural disasters
- Meteorites
- New types of terrorism; evolving, adaptive threats

5.3 Threats Resulting from our Inability to Understand or Manage the System

- The change in risk positions driven by increased centralization and the associated lack of redundancy
- A lack of understanding of the depth of our reliance on technologies such as GPS for infrastructure functioning
- Changes in the US global position in the energy markets that may make us more (or less) vulnerable
- The change in the US geopolitical position (are we still the world's superpower?)
- Emergence of another market player (e.g., Google)

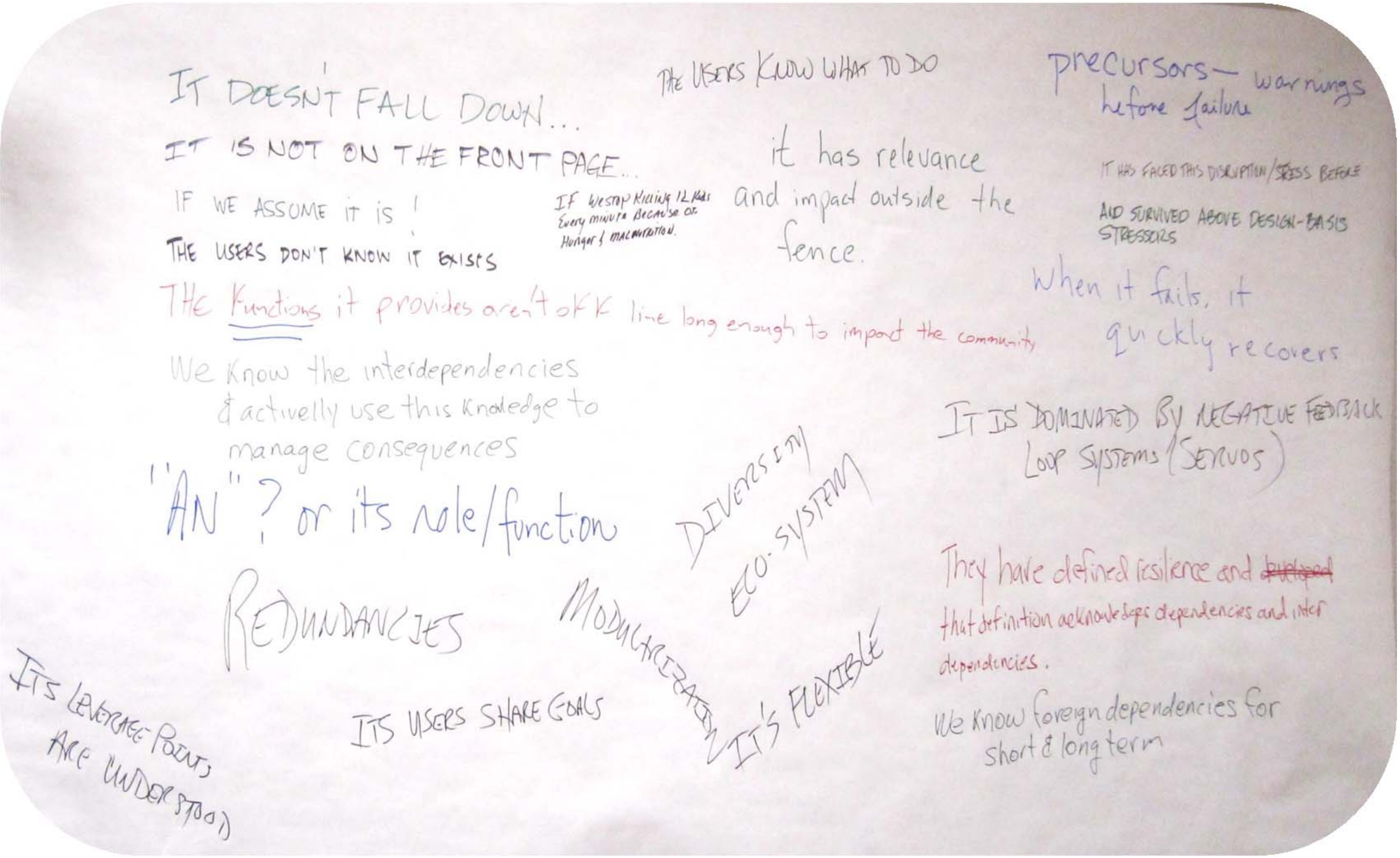
5.4 Demographic Changes

- Age of the workforce that operates the infrastructure – the need to have a workforce that can operate today's infrastructure and be prepared for tomorrow's

- Changes in population makeup due to immigration and migration; changes in infrastructure use based on cultural practices
- Societal ignorance and general inability to make informed decisions

6 SUCCESS: SECURE AND RESILIENT INFRASTRUCTURES

The discussion had now moved from a definition of the problem space to factors causing change in that space to active threats to it. Participants now turned their attention to a definition of success. If our infrastructure system was secure and resilient, what would it look like? This was the topic of the second written brainstorm which is shown in Figure 2.



IT DOESN'T FALL DOWN...

IT IS NOT ON THE FRONT PAGE...

IF WE ASSUME IT IS!

THE USERS DON'T KNOW IT EXISTS

IF We STOP KILLING 12 KIDS
Every MINUTE BECAUSE OF
Hunger & MALNUTRITION.

THE USERS KNOW WHAT TO DO

it has relevance
and impact outside the
fence.

precursors — warnings
before failure

IT HAS FACED THIS DISRUPTION/STRESS BEFORE

AND SURVIVED ABOVE DESIGN-BASIS
STRESSORS

THE Functions it provides aren't oKK line long enough to impact the community

When it fails, it
quickly recovers

We Know the interdependencies
& activelly use this Knowledge to
manage consequences

"AN"? or its role/function

IT IS DOMINATED BY NEGATIVE FEEDBACK
LOOP SYSTEMS (SERVOS)

DIVERSITY IN
ECO-SYSTEM

REDUNDANCIES

MODULARIZATION

IT'S FLEXIBLE

They have defined resilience and ~~developed~~
that definition acknowledges dependencies and inter
dependencies.

We Know foreign dependencies for
short & long term

ITS LEVERAGE POINTS
ARE UNDERSTOOD

ITS USERS SHARE GOALS

Figure 2: Written Brainstorm - Infrastructure Resilience

It quickly became clear that participants believed that it is important to distinguish between robustness and resiliency. Robustness was defined as the ability to adapt to a changing environment faster than the rate of change of the environment. For resiliency, the group turned to a definition proposed by the Intergovernmental Panel on Climate Change (IPCC) to guide the discussion. The IPCC defined resiliency as:

> The ability of a system and its parts to anticipate, absorb, recover and accommodate change in a timely and efficient manner to preserve, restore and improve functions and structures.

The group suggested that 'anticipate' and 'absorb' were aspects of robustness, and focused their resiliency discussion on 'recover and accommodate.' The group also pointed out that the magnitude and duration of the deviation from targeted performance standards would need to be considered in a consideration of the resilience of a particular system. One of the participants asked that the concept of anti-fragility[5] be considered – was an infrastructure system that drew strength from disorder possible? Finally, the group recognized that resilience could and should be considered for both single systems and for the system of infrastructures as a whole.

Participants also noted that in addition to preserving, restoring and improving functions and structures, a resilient infrastructure system might curtail certain functions and structures as they outlived their social usefulness. The goal, they suggested , was a state of *acceptable functionality*, not a restoration of the *status quo ante* or a maintenance of the *status quo*. As society changed, so would the definition of 'acceptable.'

One of the participants pointed out that the resilience of the communities served by the infrastructures is an important part of the infrastructure resilience calculation. He suggested that for any given infrastructure failure, the infrastructure will be more resilient if it resides in a community with a great deal of social capital. Another participant added that an important part of that social capital is the strength of the media in the affected region. This would include both social media and traditional media, as both are factors in organizing a timely response. Others agreed, but pointed out that social capital will play in the restoration of infrastructures to the *status quo ante* but not in their improvement. System failure should be seen as an opportunity to change, add, or upgrade. However, as that sort of system change challenges established equities, it is often a difficult step to take.

This, of course, returned the discussion to the question of equities and the social good, and the governance structure and the processes that support them. As one participant pointed out, resilience is only useful if it enhances social welfare. But how social welfare is defined, and whose social welfare must be considered is a political question. Furthermore, there is a paucity of useful tools and methods to calculate the social costs and benefits (particularly around issues like privacy and civil liberties) associated with major changes to social structures and processes.

The group discussed the lack of tools to determine responsibility for infrastructure resilience. Any tool or method would need to consider impacts on three dimensions:

[5] Taleb, Nassim Nicholas. 2012. *Antifragile: things that gain from disorder*. Random House Incorporated.

- The governance space, moving from the responsibility of the individual to the responsibility of the federal government;
- The geospatial extent of the infrastructure failure, moving from local to global and introducing the multi-jurisdictional question; and
- The temporal dimension, considering the acute or chronic nature of the failure.

Any assignment of responsibility would need to consider all three dimensions. Any viable planning or management approach would be at some intersection of all three.

One of the participants pointed out that resilience (and the responsibility for developing and maintaining resilience) also is a design specification. It differs for specified resilience and generalized resilience. For specified resilience, the system is designed to a disturbance whose character generally is known and whose impact is localized. For generalized resilience, the system must be designed to a set of unknowns – the character and the impact are unknown. Resilient infrastructure systems must be resilient according to both types of specifications.

Measurements of resilience were a bit trickier than the definition. Participants noted that both security and resilience focused on acute insults; it was more difficult both to identify and measure chronic or long-term change, partially because of the increased uncertainty as timeframes became longer. That said, participants identified the following as possible metrics for resilience:

- Know what is Unacceptable (e.g., power loss for more than 24 hours? Road closures for more than 4 hours?)
- Measure social capital and local resourcefulness. Tools and methods are lacking here, however.
- Know where benefits exceed costs. Again, tools and methods for measuring or assessing social benefits and costs are lacking
- Assess what individuals and communities have done to set up substitute methods for acquiring functionality (think of the p*osse comitatus* or local militia activity on the southwestern US border where communities feel the Border Patrol is ineffective, or individuals with generators in their garages for use in case of power failures)
- Measure precursors. Do not wait for catastrophic failure
- Measure what we *do* have (e.g. hospital beds)

And this led to a (recognizably incomplete) list of tools and methods that need to be developed:

- Big data analytics and predictive algorithms to utilize the large quantities of data now collected through sensors and monitoring technologies
- Social modeling tools to address questions around the interaction of policy, threats and change factors
- Advanced stakeholder inclusion processes to better understand local and national expectations of infrastructures

- Better measures of social capital and local resourcefulness
- Infrastructure evolution modeling including aging factors and acute insults.

Finally, the group addressed the question of security. They quickly came to agreement that there are certain threats against which we specifically want to protect. If the system and its parts are so protected, they are secure.

To summarize: This portion of the discussion focused on definitions. Resilience needs to be distinguished from robustness, and both are different than security.

- Robustness is the ability to adapt to a changing environment faster than the rate of change of the environment.
- Resilience is the ability of the system to return to an acceptable level of functionality (note that this does not necessarily mean restoring an infrastructure to the *status quo ante*).
- Secure is the state of being protected against certain types of threats.

Metrics for resilience are difficult to establish. Resilience often lies not in the performance of the hard assets but in the communities served by the infrastructure systems. Tools and methods for assessing relevant social metrics are lacking, as are data analytics to leverage the flood of data we are now receiving from sensors and other monitoring technologies.

7 PATHS FORWARD

For the final session of the workshop, participants broke into small groups to discuss possible paths forward. They were asked to specifically address the following questions:

- Who are the players in the infrastructure arena? What are their respective roles and interactions?
- What are some novel ideas for public/private partnerships?
- What are some possible research directions?
- How do we assure that the private sector adhere to adequate cyber security standards?

7.1 Identifying the Players

When the groups re-convened, they began by delineating the universe of players. Figure 3 illustrates the players identified by the group, organized into a stakeholder map.[6] Note that the figure includes ONLY those players identified during the workshop.

[6] Glicken, Jessica. "Effective public involvement in public decisions." Science Communication 20.3 (1999): 298-327.

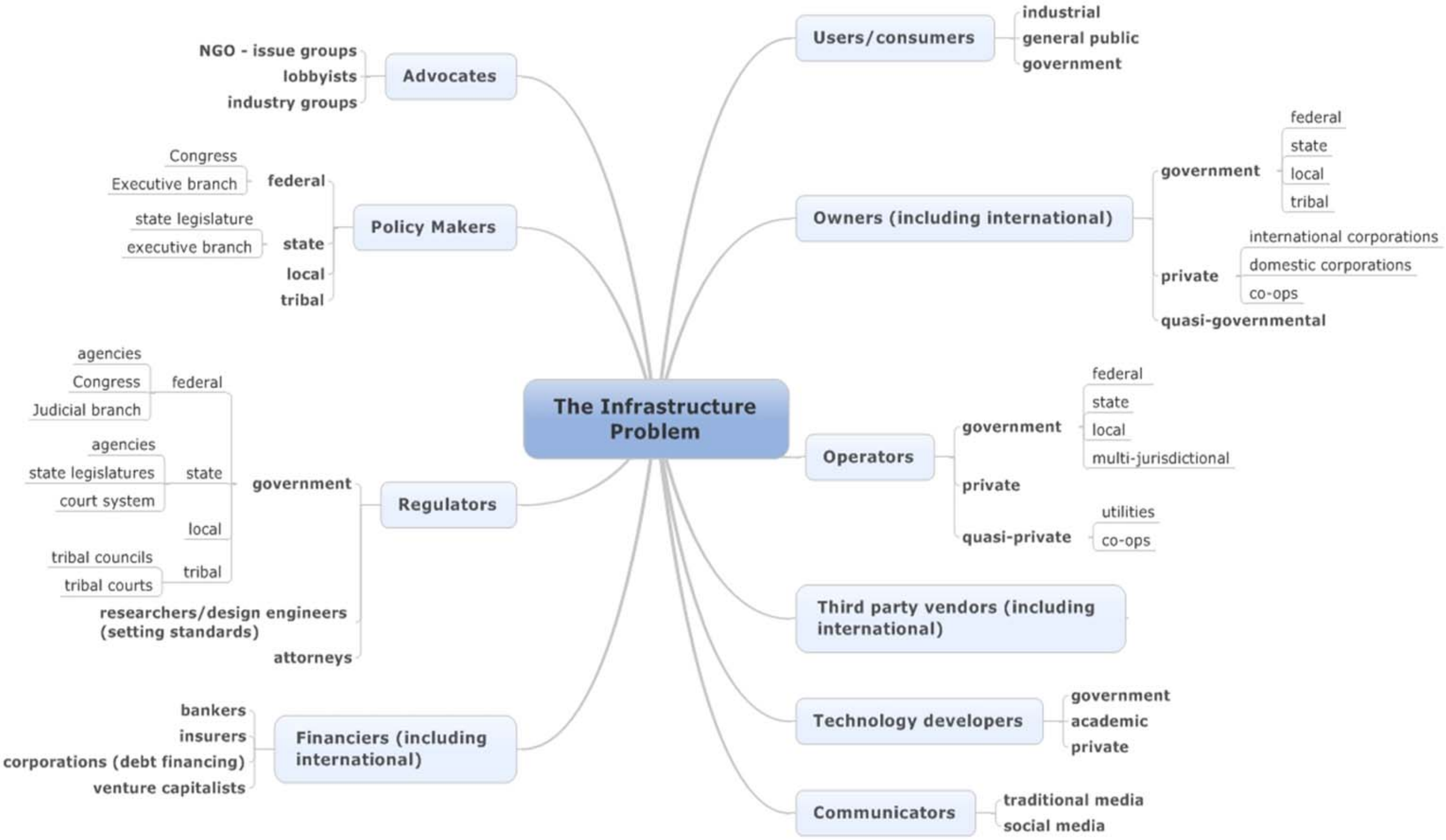


Figure 3: Mapping of Players Identified During Workshop

7.2 Public-private Partnerships

Participants contributed ideas for public-private partnerships around the infrastructure problem.

- The grand challenge model – the government offers a prize for solving a problem. DARPA has used this model with some success
- As a funder of infrastructure development – as the government provides funds to infrastructure projects, it can provide incentives for development in certain directions. (As an example, the government in effect used procurement policies in the 1960s to stimulate the development of computational technologies.)
- The development and promulgation of a broad Infrastructure Policy Act
- Development of multi-jurisdictional regions for planning purposes – inclusion of players other than government (think of the move of environmental planning from a jurisdictional to a watershed mode as a model- the Chesapeake Bay is an example).
- Bottoms-up funding through regional, multi-jurisdictional approaches to infrastructure planning
- An approach similar to the crop insurance program – the private sector takes the construction risk while the public sector takes the market risk through insurance vehicles
- Changes in the way in which our national accounting systems manage infrastructures – what if they were part of a capital budget rather than an operating budget?
- The use of private funds to build infrastructure components which are then sold to the government which operates them
- The use of the government as a 'data aggregator' to collect and manage the large, cross-sector and cross-organizational data sets that will be necessary to understand how the system of infrastructures works. (It was suggested that government assumption of this role would help avoid anti-trust issues.)
- Development of government-sponsored industry/trade groups focused on resiliency at the national level – they can act as an interface between a government with a declared intention to regulate and the requirements of market-driven industries

7.3 Research and Development Opportunities

Participants suggested a formal exercise in which a group rigorously addressed the list of threats, looking for R&D opportunities to counter them. This could be supplemented by an inventory of best practices which could stimulate additional research ideas.[7]

[7] Editor's Note: The 2013 ASCE Report Card for America's Infrastructure (http://www.infrastructurereportcard.org/a/#p/home) was released shortly after this workshop was held. Several participants referred to it (and its pending release) during the workshop and its utility as a source document for defining the current state of various types of infrastructure systems in the United States.

There also was discussion of the difficulty of transferring research from a research environment to full deployment. This is not unique to the infrastructure problem and, strictly speaking, is not a research opportunity. In fact, participants suggested that it has been addressed with varying degrees of success in other sectors by innovation or development hubs which co-locate academe, national labs, industry, and regulators – in other words, through public-private partnerships of various types.[8]

7.4 Private Sector Adherence to Cyber Security Standards.

There was not much discussion of this topic. However, one group did suggest a completely new approach to the internet to counter the cyber security problem. Rather than add fixes to an existing system, they suggested developing 'internet 2.0' – a system in which security was inherent to the design.

8 WRAP-UP

The workshop underscored the value that the diverse perspectives brought to the problem of the security and resiliency of infrastructures. The wide range of sectoral representation, skills and expertise, and the international components at the table gave a breadth and depth to the discussion it otherwise would not have had.

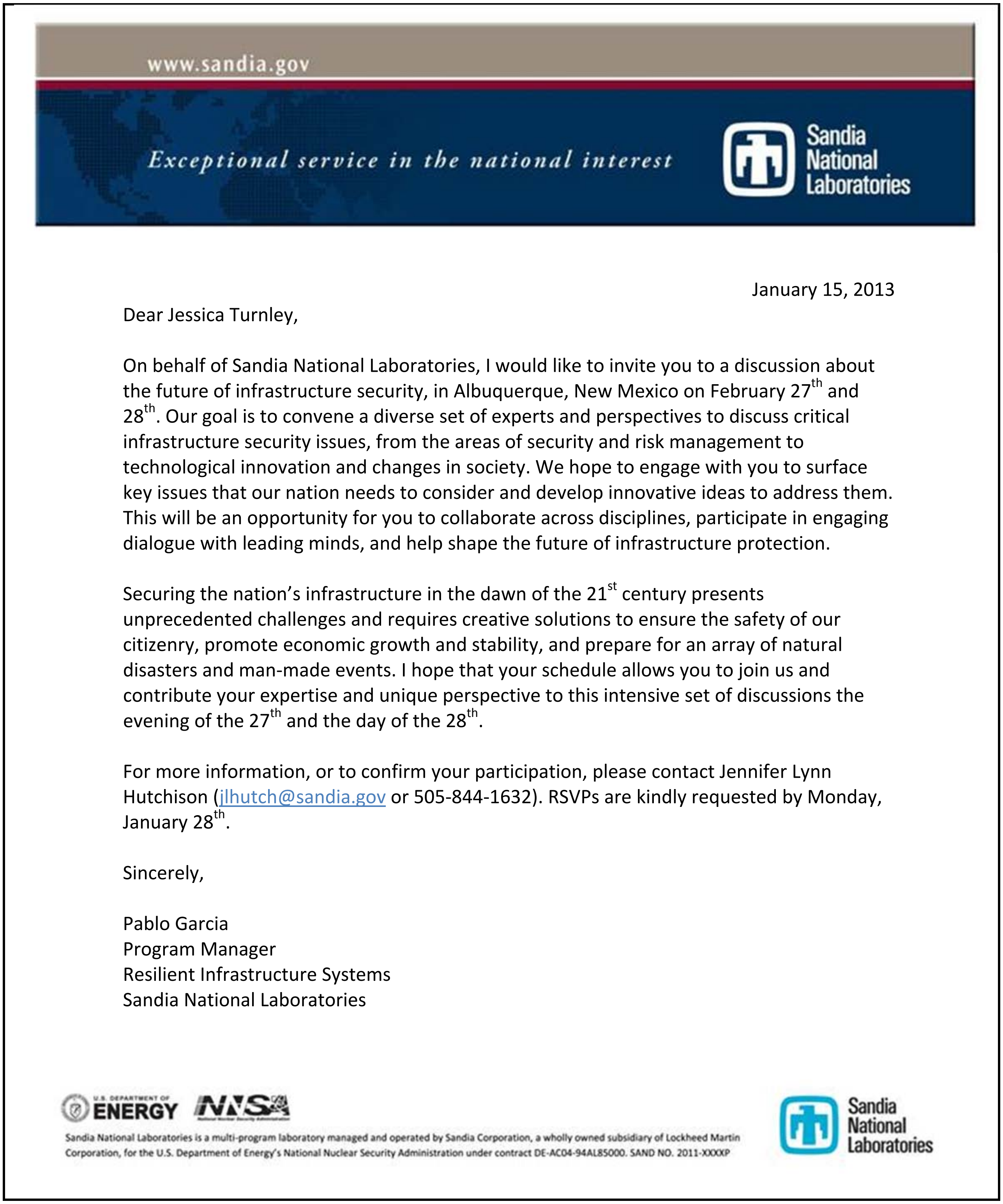
Conversations around definitions of the system, change factors, players in the game, and other topics yielded many more questions than they did answers.

- What are we trying to achieve with policies and activities around infrastructures? Are we trying to maintain a certain quality of life (perhaps phrased as maintain the status quo), open new markets, shift population footprints…? Are we clear and explicit on these goals?
- What will the next generation economy and society look like? How can we learn enough so we can build to tomorrow, not just today?
- How much is enough? And where should it be? Who decides who gets what? Who manages these equities and how?
- How do we determine what 'acceptable' functionality looks like?
- How is responsibility for developing, repairing, maintaining and protecting infrastructures allocated to and (not) accepted by the individual citizen, local communities, governments and the private sector?
- How should the multi-jurisdictional nature of many infrastructure sub-systems be managed?

[8] Ed.note: It is worth noting that the problem as it was stated and the solution proposed stem from two different paradigms of the relationships among research and deployment. The problem posits a linear progression from basic idea to social use, while the solution suggests a high degree of interaction and engagement among researcher, engineer, and end user. For a discussion of these paradigms and the ways in which they have influenced U.S. research policy, see Tsao, J. Y., Boyack, K. W., Coltrin, M. E., Turnley, J. G., & Gauster, W. B. (2008). Galileo's stream: A framework for understanding knowledge production. *Research Policy*, *37*(2), 330-352.

Participants agreed that the problem is not just a technology problem. Management of infrastructure systems must include management of much more than just hard assets, and must address political and social issues as well as questions of science and technology. The workshop clearly recognized the public good provided by infrastructure systems and the difficult questions of equities and allocation that rose. This also challenges and requires definition of the appropriate role of government and some broad social agreement on ‘essential service levels’ and on identification of critical services. Most infrastructure-related decisions require social trade-offs. Funding is often tax-driven, and public budgets usually are treated as a zero-sum exercise. Funding infrastructure construction may be perceived to come at the expense of other programs. The intersection between the perceived public good and the private ownership of many of the hard assets stimulated some interesting discussion on the assumption of risk and raised very important questions of governance and of economic direction – failure of certain infrastructure systems can have significant economic consequences. Workshop discussion also recognized the contribution of local communities to the resilience question as well as the impact of the American geopolitical position on both the security and resilience of infrastructure systems.

APPENDIX A: LETTER OF INVITATION



www.sandia.gov

Exceptional service in the national interest

Sandia National Laboratories

January 15, 2013

Dear Jessica Turnley,

On behalf of Sandia National Laboratories, I would like to invite you to a discussion about the future of infrastructure security, in Albuquerque, New Mexico on February 27th and 28th. Our goal is to convene a diverse set of experts and perspectives to discuss critical infrastructure security issues, from the areas of security and risk management to technological innovation and changes in society. We hope to engage with you to surface key issues that our nation needs to consider and develop innovative ideas to address them. This will be an opportunity for you to collaborate across disciplines, participate in engaging dialogue with leading minds, and help shape the future of infrastructure protection.

Securing the nation's infrastructure in the dawn of the 21st century presents unprecedented challenges and requires creative solutions to ensure the safety of our citizenry, promote economic growth and stability, and prepare for an array of natural disasters and man-made events. I hope that your schedule allows you to join us and contribute your expertise and unique perspective to this intensive set of discussions the evening of the 27th and the day of the 28th.

For more information, or to confirm your participation, please contact Jennifer Lynn Hutchison (jlhutch@sandia.gov or 505-844-1632). RSVPs are kindly requested by Monday, January 28th.

Sincerely,

Pablo Garcia
Program Manager
Resilient Infrastructure Systems
Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY NNSA

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Sandia National Laboratories

APPENDIX B: LIST OF PARTICIPANTS

Caitlin Durkovich
Assistant Secretary for Infrastructure Protection
National Protection and Programs Directorate
U.S. Department of Homeland Security

Garry Bowditch
Chief Executive Officer SMART Infrastructure Facility

Theresa J. Brown
Distinguished Member of Technical Staff
Sandia National Laboratories

Dick Bratcher
Senior Principal Consultant
DNV KEMA Energy & Sustainability

Todd E. Combs
Deputy Director of the Decision and Information Sciences Division (DIS) at Argonne National Laboratory

Sarah Ellis Peed
Deputy Director for Strategy within the Department of Homeland Security's Office of Infrastructure Protection (IP)

John Freisinger
President and CEO of Technology Ventures Corporation

Pablo Garcia
Sr. Manager, Interdependency and Consequence Effects Group, Program Manager for Resilient Infrastructure Systems, Sandia National Laboratories

Charles Hookham
Vice President and Director of Power Projects for HDR Engineers

Bob Kolasky
Director of Strategy and Policy for the DHS Office of Infrastructure Protection

Christopher Koliba
Associate Professor in the Community Development and Applied Economics Department at the University of Vermont (UVM) and the Director of the Master of Public Administration (MPA) Program

Kevin E. Lansey
Professor in the Department of Civil Engineering and Engineering Mechanics and an adjunct faculty in the Department of Hydrology and Water Resources at the University of Arizona

Monisha Merchant
Senior Advisor for Business Affairs for U.S. Senator Michael Bennet (D-CO)

Donald Quinn O'Sullivan
Program Director Global Security – Emerging Threats
Los Alamos National Lab

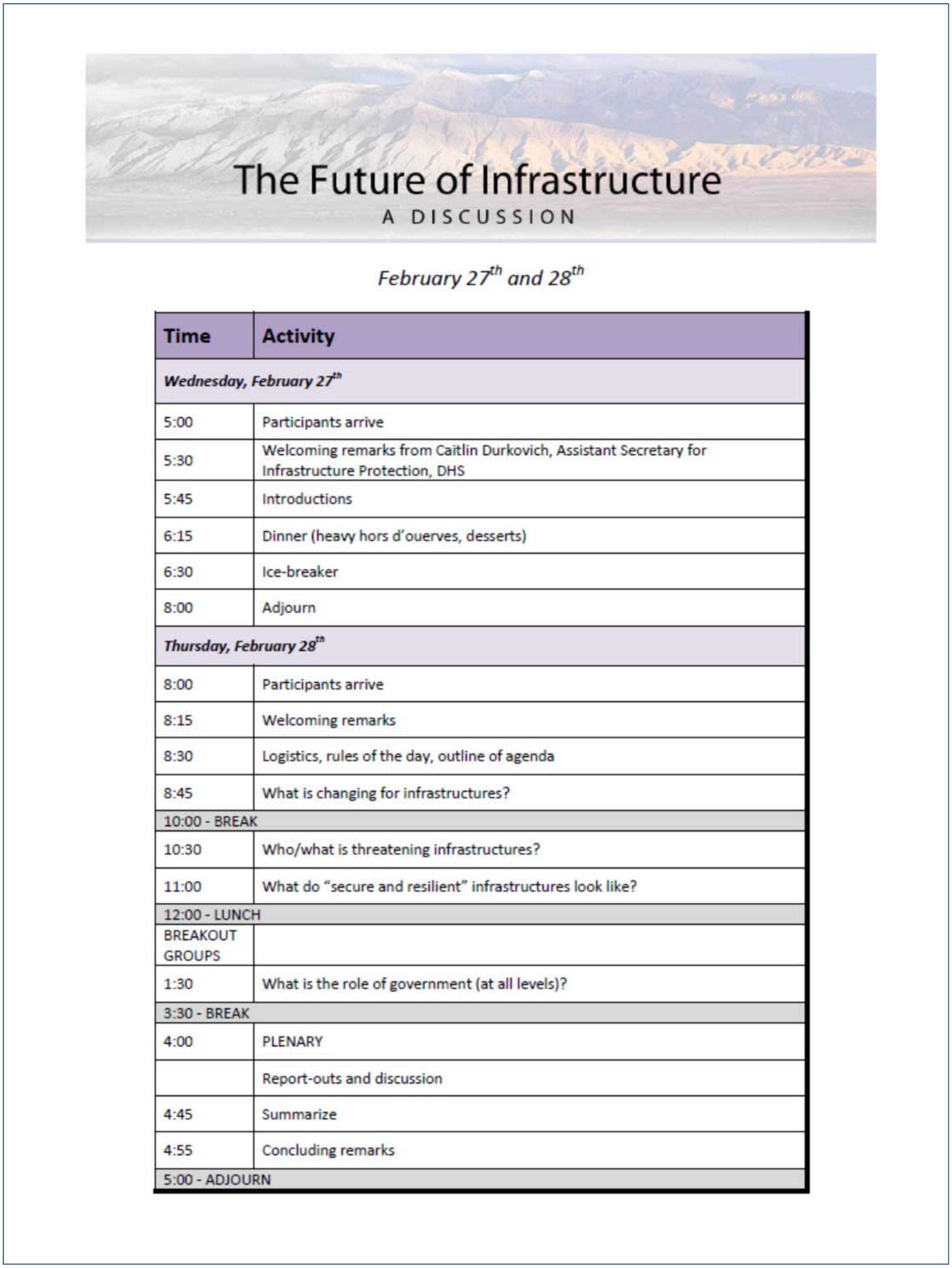
Michael J. Radzicki
Associate Professor of Economics at Worcester Polytechnic Institute

Richard L. Shanks
National Managing Director
Aon Risk Solutions – Food System, Agribusiness & Beverage Group

Stephen Van Beek
Executive Director of Policy and Strategy for LeighFisher

Facilitator: Jessica Glicken Turnley
President
Galisteo Consulting Group, Inc.

APPENDIX C: AGENDA



The Future of Infrastructure

A DISCUSSION

February 27th and 28th

Time	Activity
Wednesday, February 27th	
5:00	Participants arrive
5:30	Welcoming remarks from Caitlin Durkovich, Assistant Secretary for Infrastructure Protection, DHS
5:45	Introductions
6:15	Dinner (heavy hors d'ouerves, desserts)
6:30	Ice-breaker
8:00	Adjourn
Thursday, February 28th	
8:00	Participants arrive
8:15	Welcoming remarks
8:30	Logistics, rules of the day, outline of agenda
8:45	What is changing for infrastructures?
10:00 - BREAK	
10:30	Who/what is threatening infrastructures?
11:00	What do "secure and resilient" infrastructures look like?
12:00 - LUNCH	
BREAKOUT GROUPS	
1:30	What is the role of government (at all levels)?
3:30 - BREAK	
4:00	PLENARY
	Report-outs and discussion
4:45	Summarize
4:55	Concluding remarks
5:00 - ADJOURN	

DISTRIBUTION

4 Garry Bowditch
Chief Executive Officer SMART Infrastructure Facility
University of Wollongong
Wollongong NSW 2522
AUSTRALIA

4 Dick Bratcher
Senior Principal Consultant
DNV KEMA Energy & Sustainability
155 Grand Ave. Suite 500
Oakland, CA 94612

4 Todd E. Combs, Ph.D.
Deputy Director of the Decision and Information Sciences Division
Argonne National Laboratory
Argonne, IL 60439

4 Caitlin Durkovich
Assistant Secretary for Infrastructure Protection
MGMT/OCAO/Mailstop 0075
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0075

4 Sarah Ellis Peed
Deputy Director for Strategy for the DHS Office of Infrastructure Protection
MGMT/OCAO/Mailstop 0075
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0075

4 John Freisinger
President and CEO of Technology Ventures Corporation
1155 University Blvd. SE
Albuquerque, NM 87106

4 Charles Hookham
Vice President and Director of Power Projects for HDR Engineers
5405 Data Court
Anne Arbor, MI 48108-8949

4 Robert Kolasky
Director of Strategy and Policy for the DHS Office of Infrastructure Protection
MGMT/OCAO/Mailstop 0075
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0075

4 Christopher Koliba, Ph.D.
Director, Master of Public Administration Program Associate Professor, Community Development & Applied Economics University of Vermont
103 Morrill Hall
Burlington, VT 05405

4 Kevin E. Lansey, Ph.D.
Professor in the Department Head
Dept. of Civil Engineering and Engineering Mechanics
The University of Arizona
Tucson, AZ 85721

4 Monisha Merchant
Senior Advisor for Business Affairs for U.S. Senator Michael Bennet
1127 Sherman Street, Ste. 150
Denver, CO 80203

4 Donald Quinn O'Sullivan
Program Director Global Security – Emerging Threats
Los Alamos National Laboratory
P.O. Box 1663
Los Alamos, NM 87545

4 Michael J. Radzicki, Ph.D.
Associate Professor of Economics
Department of Social Science & Policy Studies
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609-2280

4 Richard L. Shanks, ARM | National Managing Director
4801 Main Street, Suite 350
Kansas City, Missouri 64112

4 Stephen D. Van Beek, Ph.D.
Executive Director, Policy and Strategy
11730 Plaza America Drive, Suite 310
Reston, Virginia 20190

4 Lawrence Livermore National Laboratory
Attn: N. Dunipace (1)
P.O. Box 808, MS L-795
Livermore, CA 94551-0808

1	MS0701	Marianne Walck	06900
1	MS1138	Mercy Berman	07931
1	MS1138	Theresa Brown	06924
1	MS1138	Stephen Conrad	06921
1	MS1138	Pablo Garcia	06920
1	MS1138	Daniel Horschel	06925
1	MS1138	Jennifer Hutchison	06920
1	MS1138	Lori Parrott	06924
1	MS1138	Charles Rath	06921
1	MS1138	Richard Sweeney	10662
1	MS9001	J. Stephen Rottler	08000
1	MS9151	Leonard Napolitano	08900

1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories