National Institute of
BUILDING SCIENCES

A Business Process Engineering Approach to Managing Security and Resilience of Lifeline Infrastructures

An Authoritative Source of Innovative Solutions for the Built Environment

July 2015

A Business Process Engineering Approach to Managing Security and Resilience of Lifeline Infrastructures

Submitted in Partial Fulfillment of Contract No. HSHQDC-14-C-00089

Submitted to

Mr. Robert Kolasky

Deputy Assistant Secretary

Mr. Brian Scully

Ms. Lisa N. Barr

Office of Strategy, Policy & Budget

Office of Infrastructure Protection

U.S. Department of Homeland Security

By the

National Institute of Building Sciences

Jerry P. Brashear, PhD, Paula L. Scalingi, PhD, and Ryan M. Colker, JD

July 2015

About the National Institute of Building Sciences

The National Institute of Building Sciences, authorized by public law 93-383 in 1974, is a nonprofit, nongovernmental organization that brings together representatives of government, the professions, industry, labor and consumer interests to identify and resolve building process and facility performance problems. The Institute serves as an authoritative source of advice for both the private and public sectors with respect to the use of building science and technology.

ACKNOWLEDGEMENTS

This report is submitted as the final report under Contract Number Contract No. HSHQDC-14-C-00089 between the U.S. Department of Homeland Security and the National Institute of Building Sciences.

The Contracting Officer is Mr. Haben Woldemichael and the Contract Specialist is Mr. Colin Bornmann. Mr. Brian Scully and Ms. Lisa Barr oversaw the contract for the DHS/Office of Infrastructure Protection/Office of Strategy and Policy (IP/S&P), Mr. Robert Kolasky, Deputy Assistant Secretary of Infrastructure Protection.

Mr. Earle Kennett was the original Project Director for the Institute and was succeeded by Mr. Ryan Colker, JD, on Mr. Kennett's retirement. Dr. Jerry Brashear managed the project with expert advice and active participation by Dr. Paula Scalingi.

Information and insights into the conditions, constraints and objectives for the use of risk analysis by lifeline infrastructures, local governments and region partnerships was been generously provided by a large number of the leaders and staff of such organizations, who were guaranteed total anonymity.

In addition, many federal officials contributed valuable presentations and experience with federally sponsored risk and vulnerability assessment tools. Their names and organizations are provided in Annex 2 of Appendix D.

Dr. Brashear expresses his gratitude to the Institute, the Department and IP/S&P for their guidance and to his colleagues for their contributions, while taking full responsibility for the content of this report.

As full disclosure, Dr. Brashear has been professionally involved with several projects that have relevance to the present work. He wrote the final update of the Risk Analysis and Management for Critical Infrastructure Protection (RAMCAP^{TM}) and several related reports while with the American Society of Petroleum Engineers, where led the work to adapt the generic RAMCAP methodology to the water sector. He also served as secretary of the standards committee for ANSI/AWWA J100-10, *Risk and Resilience Management of Water and Wastewater Systems* and adapted the J100-10 methodology for a regional developmental feasibility study conducted for DHS Science and Technology Directorate in the Nashville metropolitan region. As revealed in the project study and this report, this methodology compares well with other federally sponsored risk analysis tools for lifeline critical infrastructures. The criteria leading to that conclusion are drawn directly from the risk disciplines and associated literature. While this research was conducted impartially under the auspices of the Institute, Dr. Brashear admits (upon conclusion of the project) some satisfaction that this tool comes closest to the ideal model described in this report.

Jerry P. Brashear, Ph.D.
July 2015

This page left blank.

Table of Contents

List of Figures

List of Tables

A Business Process Engineering Approach to Managing Security and Resilience of Lifeline Infrastructures and Regions

Jerry Brashear, PhD, Paula Scalingi, PhD, and Ryan Colker, JD

Executive Summary

Presidential Policy Directive/PPD-21 – Critical Infrastructure Security and Resilience (PPD-21); the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013): the *Office of Infrastructure Protection Strategic Plan: 2012-2016: Collaborate*; and their predecessor documents all emphasize the central role of individual critical infrastructure (CI) systems and state and local governments in advancing the national goals of critical infrastructure security and resilience (CISR) at the regional scale. The decisions made by these entities largely determine the levels of security and resilience U.S. communities will enjoy. Of particular concern are the populous multi-jurisdictional regions that account for the majority of the U.S. Gross Domestic Product with extensive supporting interdependent infrastructures.

NIPP 2013 and its *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach* describe a risk analysis framework for identifying and understanding the most important risks an infrastructure or regional community faces, evaluating options for improving CISR, and assessing their performance over time.

The National Institute of Building Sciences project team undertook the present project to operationalize the NIPP 2013 framework into a conventional business process, a CISR Risk Management Process (CISR-RMP). The project employs a business process engineering approach to extend that framework into a workable, scalable, repeatable, defensible and practical process that infrastructures, especially interdependent lifelines (energy, water/wastewater, transportation and communications), local government agencies, and regional public-private partnerships can use to collaboratively rationalize the allocation of scarce and constrained resources for security and resilience. Three investigations informed the design specifications for such a process:

1. Review of federal policy and strategy documents to determine the specific objectives, scope and policy requirements for the process;
2. Decomposition of one of these requirements, defensibility, into a set of technical specifications based on the standards of the risk disciplines (economics, operations research, finance, etc.) and conducting a cursory review of 24 federally sponsored methods and tools designed for lifeline CIs; and
3. Interviews with infrastructure and local government analysts and decision-makers, typical of those who would use a CISR-RMP, to learn their interests, preferences and constraints.

From these and additional research on existing federal and other public and private-sector risk-related capabilities, an integrated set of design specifications was developed and used to guide the design of a CISR-RMP, which can be used by diverse organizations and constituencies (key stakeholders) at three interacting levels of application necessary for addressing regional risk:

1. Individual CI and emergency response enterprises, public and private, whose analyses and decisions, necessarily internally oriented, establish the current actual levels of CISR in each region;
2. Regional public-private coalitions or partnerships that facilitate cross-CI cooperation, facilitate analysis of dependencies and interdependencies, and conduct regional analyses from the public's orientation; and
3. State and/or federal government agencies that set policy and guidance; develop tools and techniques; provide direct support, including training, technical assistance and quality assurance; and aggregate risk, resilience, benefits and costs to state, multi-state regions and national totals for accountability and support to CISR policy and program decision-making at these levels.

The CISR-RMP operationalizes the NIPP 2013 risk framework by enabling five key sets of actions based on collaborative decision-making at all three stakeholder constituency levels:

1. *Set goals and objectives:* define the enterprise and regional purposes in CISR and the threats to be considered;
2. *Identify infrastructure:* determine the truly critical assets, systems and subsystems in specific CIs and regions and the threats that could most endanger them;
3. *Assess and analyze risk:* estimate the baseline risk and resilience levels of each threat-asset combination, accounting for protective and mitigating measures currently in place;
4. *Implement risk management:* design options to reduce risk and/or increase resilience; valuing them relative to their costs; allocate scarce resources to those that maximize net benefits within constraints; and implementing the options chosen; and
5. *Measure effectiveness:* monitor implementation and estimate the amount by which actual risk and resilience were changed by the options, based on exercises, relevant actual cases (in any comparable location), professional and trade literature and a re-visit of the estimates of the baseline and option valuation.

The design balances two conflicting purposes: the "ideal"—to make the process fully effective in allocating resources for the greatest benefit (which makes it defensible in terms of risk analysis methodology)—and the "pragmatic"—to make the process simple enough to be applied, understood, integrated into existing management processes and used routinely by staffs and management of CIs, local governments and regional coalitions. The project team achieved this balance by adopting common U.S. Department of Homeland Security (DHS) definitions of risk and resilience; relying on a threat-asset scenario approach, with point estimates of key risk terms; conducting cross-CI interdependency analysis; and using constrained net-benefit decision-making as the resource-allocation decision criterion. Certain desirable features of a state-of-the-art risk management process (e.g., full uncertainty and correlations with Monte Carlo simulations, real-options, portfolio optimization, etc.), while inherent in any contemporary, ideal design, were seen as too complex for the present, so are deferred for a time when user sophistication calls for them.

The project concluded with a "roadmap" to operationalize the risk management process by simultaneously closing the most critical component gaps and developing a novel way of initiating CISR-RMP implementation in the field, both in preparation for possible full-scale developmental pilot testing. Closing the gap would consist of intensively searching for proven tools and methods that meet the specifications of the CISR-RMP. Where nothing suitable and effective is found, the specifications for new development would be spelled out.

As with the process design itself, the implementation approach is a balancing of the "ideal"—all users apply the CISR-RMP in the same manner to support comparisons, interdependencies analysis and aggregation—and the "pragmatic"—users adapt their *existing* management processes to incorporate the CISR-RMP functionality into their routine management processes. Unlike the usual "top down, outside-in" federally sponsored, local/regional security and risk programs, a CISR-RMP team would engage prospective users in an organic, "bottom-up, inside out" business process engineering approach, recognizing that user organizations are "going concerns" with unique and valuable knowledge, processes, models (both digital and mental) and relationships in place and then building upon them, moving toward the CISR-RMP as the "ideal." Integral to success in this is developing a stakeholder-validated implementation strategy in the initial stage of the process: the users must be "in charge" by being called upon to make specific process implementation decisions necessary to implement the CISR-RMP.

At present, the knowledge base for designing such an implementation approach is inadequate. Too little is known beyond the brief, non-random survey in the present project about the objectives, attitudes, constraints and conflicts involved in applying and using these tools to define an effective implementation strategy. The organic implementation approach would receive initial validation and substantially deeper understanding through a series of case studies of actual use of the leading tools by lifeline infrastructures, local government agencies and, possibly, regional organizations. Based on their actual experience, the tools used (and, hence, the CISR-RMP that would employ them) would be user-validated and the organic implementation approach would be refined for possible testing in field developmental pilot tests. A major emphasis in each case study would be describing not only the currently used risk management process of the subject organization, but also its related processes that might contribute information to a future risk process. The related processes might include asset management, continuity planning, capital development planning and budgeting, and operational planning and budgeting.

Once the major gaps are narrowed and the organic implementation approach is better defined, it is recommended that two or three regional pilot projects be conducted in regions where multi-stakeholder CISR-focused partnerships or other collaborative mechanisms are already in place. The purpose of these pilot tests would be both to test the collaborative organic implementation approach and to evaluate the feasibility and effectiveness of the CISR-RMP. The results from these pilots will be used to enhance the CISR-RMP framework and its implementation approach. In the initial phase, the project team would work with users to review the users' existing risk management and related processes relative to the "pragmatic ideal" of the CISR-RMP to determine two things: (1) to see where, if anywhere, the extant risk management processes might be improved by evolution toward the CISR-RMP, and (2) whether the products of their existing or modified processes are consistent enough with other users of the CISR-RMP process to support interdependencies analyses, comparisons and aggregation. Where this review suggests changes to a user's existing processes, the user would be presented available options (pre-screened for effectiveness and consistency with the CISR-RMP) and the *user* would decide among them. The user would be responsible for acquiring, integrating and applying the chosen options, with continuing support from the CISR-RMP pilot team. If assistance is needed, the federal or state personnel responsible for training, technical assistance and quality assurance or other appropriate experts could provide the needed, very-specific assistance.

This "pragmatic-ideal" balancing approach of both the process framework and its implementation operationalizes the voluntary and collaborative nature of the plans of the DHS Office of Infrastructure Protection (DHS/IP) within its likely future budgets. It also allows collaboration with other federal programs designed to manage aspects of risk. Success in this approach could lead to the CISR-RMP's becoming a sustained, inherent part of routine management processes of CIs, local governments and regional coalitions, the place where it must be to be sustained and effective in truly increasing critical infrastructure security and resilience.

The description of the CISR-RMP in this report should be recognized as the "snapshot" frame from the moving picture of risk/resilience management advancement. The process is fully expected to continue to change and adapt to new methodological insights and deeper understanding of the challenges faced by diverse lifelines and other infrastructures, local and state governments, regional coalitions and the national government. This report is simply a point along that developmental continuum.

1. Introduction

A. The Challenge All too often, headlines draw attention to continuing terrorist challenges to United States interests, both at home and abroad. Yet, only a very small fraction of actual plots ever reach the news. At the same time, there seem to be almost daily broadcasts highlighting the frequency and severity of extreme weather and natural disasters. Such natural events have increased significantly, escalating the losses in human casualties and property damage. More than 1,100 fatalities and economic damages of more than $188 billion occurred in just the three years between 2011 and 2013, and that does not count lost productivity or economic activity or the federal government's $136 billion[1] in federal response and recovery grants – just to get back to "normal." Now, add one more issue to these major concerns: the long-term owner underinvestment in maintenance and rehabilitation of existing facilities and deferring construction of new facilities even as population and demand for CI services increase. This underinvestment has stretched existing infrastructures to meet higher demand by operating closer to their design maxima and kept aging facilities in service well beyond their design lives, making them more vulnerable to whatever hazards may occur. Climate change may render the design and construction standards of past times obsolete, as greater and more frequent loads and new operational demands are placed on existing structures and systems.

Significant portions of the human, material and economic losses from disasters occur because such events disrupt the delivery of vitally necessary services of interdependent lifeline critical infrastructures (CIs), including energy, water, transportation, communications and emergency services, without which communities can neither recover nor long survive. Any one infrastructure is interdependent with others, so the direct loss of one is exacerbated as an initial failure may cascade to other infrastructures in a "chain reaction" that can spread losses widely throughout a region and beyond.

B. The Federal Response The federal government's 2011 to 2013 outlays of more than $136 billion in response and recovery consisted of 96 programs in 19 federal agencies. In addition to these specifically post-event response and recovery programs, two recent Presidential Policy Directives identify a total of five mission areas of preparedness—prevention, protection, mitigation, response and recovery—each of which has significant pre-event decisions requiring risk/resilience analysis; action planning and resource allocation; program implementation; and performance evaluations. The purpose of these programs is to reduce the economic losses and human suffering, and, incidentally, federal post-disaster outlays, by making the nation more secure and resilient to hazard events before they strike.

Presidential Policy Directives 8 ("National Preparedness") and 21 ("Critical Infrastructure Security and Resilience"); along with Executive Orders 13636 (Improving Critical Infrastructure Cybersecurity), 13653 (Preparing the United States for the Impacts of Climate Change)[2]; and several recent advisory body reports explicitly establish disaster resilience as a national objective, along with security, and rely on risk analysis and management to advance them. Most of these documents recognize that the level of

[1] Weiss, D.J. and Weidman, J., "Disastrous Spending: Federal Disaster-Relief Expenditures Rise amid More Extreme Weather," Center for American Progress, accesses May 18, 2015 at https://www.americanprogress.org/issues/green/report/2013/04/29/61633/disastrous-spending-federal-disaster-relief-expenditures-rise-amid-more-extreme-weather/.

[2] "Presidential Policy Directive / PPD-8: National Preparedness" (PPD-8, 2011); "Presidential Policy Directive/ PPD-21 – Critical Infrastructure Security and Resilience" (PPD-21, 2013), and the associated "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience" (NIPP 2013), "Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach" (2013) and their respective predecessor documents, especially NIPP 2009 and "Risk Management Fundamentals: Homeland Security Risk Management Doctrine" (DHS/NPPD, 2011).

critical infrastructure security and resilience largely depends on decentralized decisions made by local CI owners and operators, local governments and regional partnerships. Indeed, the *Office of Infrastructure Protection Strategic Plan: 2012-2016*[3] (IP Strategy) is subtitled "Collaborate." All of these documents address a heavily overlapping set of specific hazards, all call for risk-based decision-making and all rely on "all-of-nation" and "all-of-community" efforts of CIs; state, local, tribal and territorial governments; private and civic entities; and public-private regional coalitions (RCs) to make the majority of these investments, some with state and/or federal assistance.

The National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013) mandated by PPD-21, advances "calls to action" that include, quoting directly:

- "Employ the THIRA [Threat and Hazard Identification and Risk Assessment] process as a method to integrate human, physical and cyber elements of critical infrastructure risk management. Using the existing process will facilitate better coordination of planning, resource allocation and evaluation of progress by State and local governments, as well as local infrastructure owners and operators…
- "Develop and advance a joint set of regional preparedness projects demonstrating the integrated application of critical infrastructure risk management and planning. This will involve Federal agencies responsible for implementing PPD-8 and PPD-21 working collaboratively with States, areas, rural communities, and regional coalitions."[4]

These bullets describe the functional and organizational scope for improved risk management: analysis of current and future risks; planning and resourcing of risk-reduction options; and evaluating the performance of programs by CIs, local governments and RCs. The report directs the Federal Emergency Management Agency (FEMA), which is responsible for PPD-8 and the design of the THIRA process; the DHS Office of Infrastructure Protection (IP); and the respective sector-specific agencies as defined in the NIPP, to collaborate to facilitate and support this fundamentally state/regional/local process. The present project is designed expressly to operationalize and advance these calls to action.

At present, the decision-makers in CIs and local governments are only beginning to recognize the magnitude of the challenge and their central role in meeting it. Only a few areas can boast effective RCs. Few of these decision-makers have experience or education in risk analysis and management. Although the respective policy documents set an expectation for these decision-makers to take on this role, there is a missing element: *there currently is no common, consistent, repeatable, defensible, transparent, integrated risk management process designed expressly for their use across the array of assets and hazards, including their interdependencies, that these users face today*.

C. Structure and Purpose of the Present Project PPD-21, NIPP 2013 and their predecessor documents all emphasize the central role of individual infrastructure systems and state and local governments in advancing the national goal of critical infrastructure security and resilience (CISR) at the regional scale. Regions are where dependencies and interdependencies are most immediate and complex, where the bulk of U.S. Gross Domestic Product is generated and where the majority of Americans live. NIPP 2013 and its *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*

[3] DHS National Protection and Programs Directorate, *Office of Infrastructure Protection Strategic Plan: 2012-2016: Collaborate*, DHS/NPPD/IP, Washington, August 2012.

[4] U.S. Department of Homeland Security, Office of Infrastructure Protection, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,* DHS/IP, Washington, DC, pp. 22-23.

describe a risk analysis framework as the key tool for identifying and understanding the most important risks to infrastructures and regional communities, for evaluating options for improving CISR and for assessing their performance in improving security and resilience over time.

The purpose of the present project is to determine the design specifications and develop an initial design for a CISR-RMP that will *operationalize the NIPP 2013 Framework* to *enable localities, lifelines, and other critical infrastructure and service providers to cooperatively assess all-hazards risk of loss and disruption to services, to rationally allocate available resources to initiatives that advance CISR as much as possible under constraints, and to evaluate the effectiveness of these initiatives*. Rationality is used here in the sense of actively seeking to maximize benefits under uncertainties and constraints.

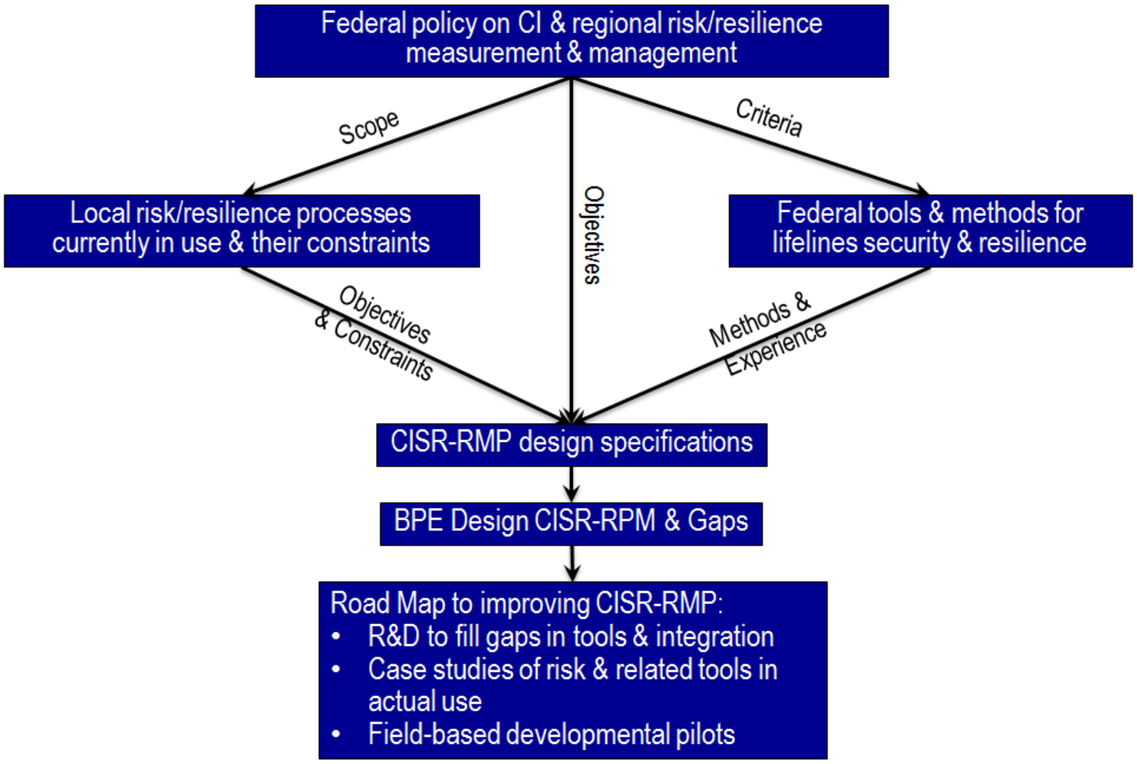

Federal policy on CI & regional risk/resilience measurement & management
Scope
Criteria
Objectives
Local risk/resilience processes currently in use & their constraints
Federal tools & methods for lifelines security & resilience
Objectives & Constraints
Methods & Experience
CISR-RMP design specifications
BPE Design CISR-RPM & Gaps
Road Map to improving CISR-RMP:
• R&D to fill gaps in tools & integration
• Case studies of risk & related tools in actual use
• Field-based developmental pilots

Figure 1. Structure of the CISR-RMP Project

The present project applies a business process engineering approach. It takes that framework and extends it into a workable, practical process that lifeline CIs, local governments and RCs can use to collaborate and rationalize the allocation of scarce resources for enhancing CISR. Rationality in this context means selecting and resourcing actions that yield the greatest benefit given constrained budgets, analytical and decision capabilities and political realities. This “bounded rationality” does not imply optimality, but rather seeks the most improvement within practical and intellectual constraints. The project team generically calls this process the CISR Risk Management Process (CISR-RMP) for this report.

The approach synthesizes CISR-RMP design specifications from three sources: (1) national policy and the NIPP risk management framework; (2) the risk management discipline used in economics, business, finance, operations research and engineering as applied to available federal lifeline CI risk tools; and (3) the on-the-ground realities facing local and regional decision-makers (Figure 1).

These design specifications guided the design of a CISR-RMP for lifeline CIs and emergency response entities individually, and link to a regional process that facilitates management of interdependencies and collaborative decision-making. CI and regional processes, in turn, interface with a state/national process for an overall national programmatic approach.

The project team compared the overall design with the characteristics of the federal tools to determine whether one or a combination of tools could be utilized, perhaps with modifications and integration, to complete the design. The team identified missing components as “gaps” to be filled by looking outside the federal lifeline programs to private and proprietary sources, or to be designed and developed through R&D.

In the final phase of the project, the team developed a summary “roadmap” for the steps that follow from the project’s findings, specifically:

- R&D to narrow the most important of the identified gaps in the available toolset, specifically a robust model information sharing protocol for exchanging highly sensitive dependencies data and methods for using that data for regional interdependencies and economic analysis;
- Case studies to better understand how actual lifelines and local agencies actually manage risk at present and how that might be improved from within; and
- “Proof-of-concept” developmental field tests to test and refine the process, gradually taking it to full regional scale.

Central to all of this is the need to accommodate the desires and constraints of the owners and operators of the lifeline CIs, local governments and regional coalitions. All parts of the CISR-RMP and all aspects of the development path forward are subject to change, within the bounds of the risk discipline, in response to the needs and requirements of the analysts and decision-makers.

2. Federal CISR Policy on CI Risk Management

The federal policy review defined the scope and purposes of the desired CISR-RMP process. The primary documents the team consulted were, first and foremost, PPD-21; IP Strategic Plan for 2012-2016; the NIPP 2013; its Supplemental Tool[5]; its immediate predecessor, NIPP 2009, for detailed specifications;[6] PPD-8; THIRA documentation;[7] and DHS doctrine on risk management.[8] Other documents were more summarily reviewed, including the National Preparedness

Table 1. Office of Infrastructure Protection Strategic Plan: 2012-2016: Selected Goals & Objectives

Goals	Objectives
1. Support and improve risk management activities across IP and the critical infrastructure community based on requirements and the best available information.	1.1: Conduct and guide national, regional, sector, cross-sector, and individual asset and system risk assessments.
	1.2: Focus resources and efforts on prioritized risk management activities that measurably help to achieve defined outcomes.
	1.3: Measure progress toward desired outcomes by demonstrating effectiveness of risk management activities.
	1.4: Improve the analysis and understanding of physical system impacts from cyber and control system exploits to better manage them.
2. Ensure effective coordination and information sharing with critical infrastructure partners to enhance protection and resilience activities during both normal operations and incidents.	2.1: Strengthen, grow, and sustain broad public-private partnerships to enhance understanding of regional and cross-sector interdependencies and to capitalize on risk reduction opportunities.
	2.2: Engage in multi-directional information sharing and provide stakeholders with timely and relevant information.
	2.3: Strengthen coordination and collaboration with various DHS operations centers to promote unity of effort for incident management.
3. Increase awareness of and participation in IP's voluntary programs; implement regulatory programs to enhance critical infrastructure protection and resilience.	3.1: Enhance the protection and resilience of Level 1/Level 2 and other sector, State, local, tribal, and territorial infrastructure through IP programs that are coordinated and have measurable impact.
	3.2: Share expertise and promote best practices in critical infrastructure protection and resilience.
	3.3: Integrate voluntary sector-specific, asset-level, and other tools into a single assessment methodology.

[5] "Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach," DHS/IP, 2013.

[6] *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, DHS/IP, 2009.

[7] *Threat and Hazard Identification and Risk Assessment Guide; Comprehensive Preparedness Guide (CPG) 201*, Second Edition, DHS/FEMA, August 2013.

[8] "Risk Management Fundamentals: Homeland Security Risk Management Doctrine," DHS/NPPD, 2011.

Goal[9] and National Preparedness System,[10] as well as the National Planning [Preparedness] Frameworks.[11]

The IP Strategic Plan for 2012-2016 contains a number of goals and objectives that pertain directly to the present project. These are displayed in Table 1. The underscored text in the objectives indicates specific areas in which an acceptable CISR-RMP should materially contribute to IP's strategic success.

Following on both the IP Strategic Plan and PPD-21, NIPP 2013 defines the national vision, mission and goals as follows (italics have been added to indicate phrases especially relevant to the current project):

- *Vision:* A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.
- *Mission:* Strengthen the security and resilience of the Nation's infrastructure, by managing physical and cyber risks through the *collaborative* and *integrated* efforts of the critical infrastructure community.
- Goals:
    - Assess and analyze *threats* to, *vulnerabilities* of, and *consequences* to critical infrastructure to inform risk management activities;
    - Secure critical infrastructure against human, physical, and cyber threats through *sustainable efforts to reduce risk*, while accounting for the *costs and benefits* of security investments;
    - Enhance critical infrastructure resilience by *minimizing service interruptions* and recovery time of incidents through *planning and mitigation* efforts;
    - *Share* actionable and relevant *information* across the critical infrastructure community to build awareness and *enable risk-informed decision making*; and
    - Promote *learning* and *adaptation* during and after exercises and incidents.

Clearly, risk management lies at the heart of NIPP 2013. Much more than its predecessors, the Plan calls for local/regional direction and decision-making based on sound, repeatable, transparent, and professionally defensible methods. This acknowledges that local CI owners and operators and local and state government agencies make the vast majority of the decisions and investments that largely determine the security and resilience of CIs.

In addition, NIPP 2013's Supplemental Tool and Risk Management Fundamentals provided that risk management would be documented, reproducible, defensible, unified in effort, transparent, adaptable, practical and customizable. Appendix 3A, NIPP Core Criteria for Risk Assessments in NIPP 09 (reproduced in Appendix B of this report) provides additional detailed specifications for how key terms are to be defined and measured.

The Plan and its Supplemental Tool also define basic terms, the core risk equation and the structural framework for the necessary risk management process. Figure 2 shows the NIPP 2013 framework, which consists of five phases or "chevrons" that will be used to structure the CISR-RMP.

[9] "National Preparedness Goal," First Edition, DHS/FEMA, September 2011.

[10] "National Preparedness System," DHS/FEMA, November 2011.

[11] "National Prevention Framework," May 2013; "National Protection Framework," July 2014; "National Mitigation Framework," May 2013; "National Response Framework," Second Edition, May 2013; and "National Disaster Recovery Framework," September 2011, all from DHS/FEMA.

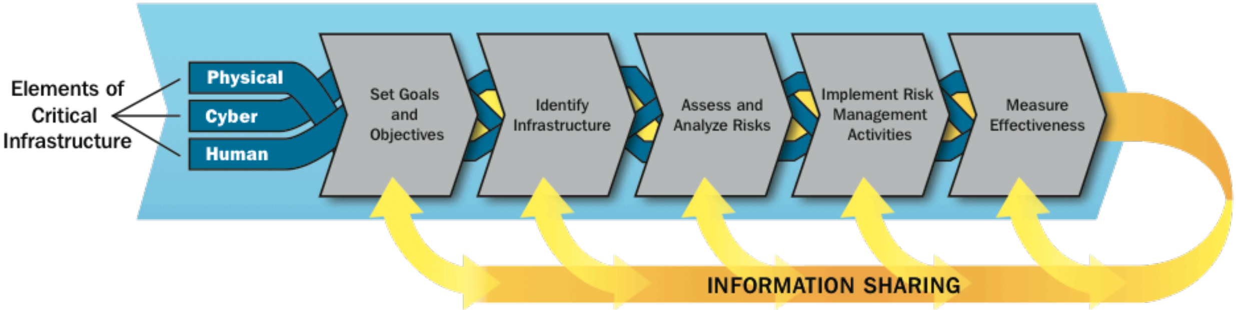


Figure 2. NIPP 2013 Critical Infrastructure Risk Management Framework

The five phases, as they apply to local lifeline CIs, local governments and regional coalitions, are listed below, with the key decisions to be made in each:

1. *Set Goals and Objectives* – devolve the national goals and priorities into local goals and objectives. For this project's purposes, this step also includes the specification of the threats and hazards of greatest concern to these decision-makers, i.e. what "keeps them up at night." *Issues*: What goals, objectives and threats are most important to the respective entities and to the region as a whole? What threats are of greatest concern?

2. *Identify Infrastructure* – define criticality for local analysts and decision-makers to use to focus on the most important systems, subsystems and assets relative to their respective organizational missions. The combinations of threats/hazards and critical assets, subsystems or systems (hereafter called threat-asset pairs) defines the set of scenarios for the analysis. *Issues:* Ranking assets by criticality and deciding which threats most affect them to define the threat-asset pairs.

3. *Assess and Analyze Risks* – estimate threat likelihood, vulnerability and consequences (including possible outages), both current and as anticipated in the future, and combining them into a "current conditions" baseline case for each threat-asset pair, often called the "cost of inaction." Consistent with long-standing DHS practice, risk is defined by the equation, Risk (R) = f(Threat Likelihood T), Vulnerability (V), Consequences (C). Because the CISR-RMP estimates these elements as point values, the product function is used: $R=T\times V\times C$. As discussed later, the risk may be to either the CI or to the regional public, by defining consequences as to the CI or public, respectively. *Issues:* Is the baseline level of risk acceptable to the decision-maker? Do dependencies and interdependencies pose unacceptable risks to the respective enterprises? Sort and rank unacceptable threat-asset pairs by risk and resilience to decide which should have options developed.

4. *Implement Risk Management Activities* – develop options to reduce unacceptable risk and enhance resilience by reducing threat likelihood, vulnerability or consequences (including outages); evaluate their life-cycle net benefits relative to their life-cycle costs; choosing the options with the greatest net benefits within budget and other constraints; and implementing and managing the selected options. *Issues:* For the selected threat-asset pairs, develop and cost-out options for improving risk and resilience; estimate the amount of risk/resilience improvement that will result; decide which options to resource to obtain greatest net benefits given budget and other constraints; and implement, monitor and manage the chosen options.

5. *Measure Effectiveness* – estimate the extent to which the selected options were implemented according to plan and, much more importantly, whether in fact, they have reduced risk and/or enhanced resilience. *Issues:* Were the options implemented as planned? Did they improve risk and resilience relative to the baseline? Was real progress made? Did they improve risk and resilience as much as estimated? Did they meet their risk/resilience-improvement objectives?

Improving the information used in the key decisions around these issues is essential to improving CISR. These decisions are the primary drivers in designing the CISR-RMP. To advance toward maximizing risk reduction and resilience, it is critical to avoid CISR-RMP design elements that could distort these decisions.

3. Design Logic, Defensibility Requirements and Federal Sponsored Lifeline Methods

A. Design Logic Business process engineering often contrasts existing processes in use in organizations with model processes that have been proven effective, then moving the former toward the latter. The current project seeks to define that model process, to use in assessing available tools and processes, and to guide improvements in actual organizations after the project is concluded.

Table 2 summarizes the logic for developing the major design requirements for the CISR-RMP: The issues of each phase of the NIPP 2013 Risk Framework are refined into a minimum set of key decisions (column A), the making of which requires a certain specific minimum set of process outputs (column B), the calculation of which in turn requires estimation, acquisition or assumption of a certain minimum set of specific terms (column C) and threat scenarios (column D). The ideal process is highlighted in red in the top row of the table. Design specifications for these elements follow from specific defensibility criteria. This section discusses these elements in light of their defensibility and then compares available federally sponsored risk tools for the lifelines and regional communities relative to the model process criteria. While Table 2 summarizes the most important of these design requirements, Attachment 1 displays the more detailed methodological specifications as row headings for the process, along with the comparison of several federally sponsored lifeline risk/resilience tools discussed later.

B. Defensibility Requirements The NIPP 2013 and its Supplemental Tool clearly indicate that risk analysis should be at the core of CISR management. Such a process should be simple, transparent, reproducible and defensible from the perspective of risk and decision science. A central criterion for risk analysis processes is defensibility: "[it] must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, as well as free from significant errors or omissions" (Supplemental Tool, p. 7). Defensibility is not simply a narrow, prudish academic consideration: the risk management disciplines have evolved to their current state by defining and demonstrating that certain practices contribute to maximizing benefits relative to costs and budget constraints better than their alternatives. They drive toward choosing more efficient options. This is how the project team defines rationality for this project: seeking to maximize net benefits subject to constraints, including limited analytical capability. Any method that could materially distort this decision-making is likely to result in sub-optimal, inefficient and irrational choices. Supporting precisely these decisions is the primary purpose of using risk analysis.

Table 2. Cursory Review of Federally Sponsored Risk Methods & Tools for Lifeline Infrastructures

Design Requirements Methods, Tools & Processes	A. Key Decisions								B.Process Outputs					C. Constituent Terms						D. Scenarios		E. Focus of Application	F. Apparent Maturity Level
Ratio Scale Methods	1. Rank Assets by Criticality	2. Rank by Risk	3. Decide to Design Options	4. Value Options	5. Rationalize Budget	6. Evaluate Performance	7. Regional Interdependencies Anal.	8. Aggregate to Reg., St., US	1. Conditional Risk | Threat = 1.0	2. Full Owners' Risk	3. Full Regional Public's Risk	4. Resilience Metric (Expected Outage)	5. Option Value (Net Benefit)	1. Event Threat Likelihood/Frequency	2. Vulnerability, Given Event	3. Consequences, to Owner & to Public	4. Outages of Service	5. Dependencies & Interdependencies	6. Option Life-Cycle & Budget Costs	1. Non-Standardized	2. Standardized		
CISR Risk Management Process Design Objectives	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥		🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥		🟥 A	Lifelines, Em. Mgt., Gov, All	5
Common Risk Model – Dams (USACE)	🟩	🟨	🟩	🟨	🟨				🟩	🟨 2			🟨	1	🟩	🟩			🟩		🟩 M	Dams	4
Component Level Risk Mgt for Bridges (FHWA)	🟩	🟨	🟩						🟩	🟨 2			🟨		🟩	🟩				🟩 M		Bridges	3
Component Level Risk Mgt for Tunnels (TSA)	🟩	🟨	🟩						🟩	🟨 2			🟨		🟩	🟩				🟩 M		Tunnels	3
Costing Asset Protections for Transportation Agencies (CAPTA, DoT, TRB)	🟩	🟨	🟩						🟩	🟨 2			🟨		🟩	🟩			🟩	🟩 N		Various Transportation	3
J100-10 (EPA, IP with AWWA); Nashville regional field test (S&T)	🟩	🟩	🟩	🟩	🟩		🟨	🟨		🟩	🟩	🟩	🟩	🟨 3	🟩	🟩	🟩	🟨 4	🟩		🟩 A	Water, Sewer, Elect.,etc.	4.5
J100-15 (AWWA), *in progress*	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩		🟩	🟩	🟩	🟩	🟨 3	🟩	🟩	🟩	🟨 4	🟩		🟩 A	Water, Sewer, Elect.,etc.	4.5
Threat & Hazard Identification & Risk Assessment (THIRA, FEMA)	🟩	🟩	🟩		🟨				🟩		🟩 2				🟨	🟩	🟨		🟩	🟩 A		Community, Core Capab.	3
Ordinal Scale Methods																							
Maritime Security Risk Analysis Method (USCG)	🟩	🟨	🟩		🟨					🟨				🟨	🟨	🟨					🟩	Ports	3
State Energy Assessments (DOE)	🟩	🟨	🟩							🟨				🟨	🟨	🟨	🟨			🟩	🟨	Electricity	3
Voluntary Chemical Assessment Tool (VCAT, IP)	🟩	🟨	🟩							🟨				🟨	🟨	🟨	🟨			🟩		Chemical	3
Vulnerability Assessment Framework (FHWA)	🟩	🟨	🟩								🟨			🟨	🟨	🟨				🟩		Highways	3
Vulnerability Assessment Scoring Tool (VAST, FHWA)	🟩	🟨	🟩								🟨			🟨	🟨	🟨				🟩		Highways	3

Notes: Scenarios: A = all; M = malevolent only; N = natural only

1. CRM uses T = 1.0 for single-dam assessments, but uses an "adversary value model" T = F(V,C|dam attack) to establish a relative risk for a set of dams.
2. Risk is conditional risk, assuming threat likelihood = 1.0.
3. Threat likelihood is calculated by a "proxy" method based on RAND/RMS and threat-asset V and C to model adversary selection of asset and attack mode.
4. Dependencies are modeled as loss of supply of critical resources, including utilities, personnel, supplies, and proximity, but are not analyzed across infrastructures.

Legend

Degree Satisfied	
🟥	Required
🟩	Fully
🟨	Partially
	Not

To assure defensibility, the project team rephrased the issues identified as arising from the NIPP 2013 Risk Framework into the minimum set of *key decisions* that must be explicitly addressed in a comprehensive CISR-RMP. They are as follows (see column A in Table 2):

1. Rank assets relative to their criticality to the enterprise's mission;
2. Rank threat-asset or threat-system scenarios by their risk and resilience;
3. Make a commitment to design specific action options that reduce risk and/or enhance resilience;
4. Establish the value and costs of such options from the perspective of the owners, as well as the public;[12]
5. Allocate budgets and other resources to achieve the greatest net benefit within budget and other constraints for both CI and regional decision-makers;
6. Evaluate performance of options that are selected and implemented in outcome terms – reduced risk and enhanced resilience;
7. Integrate individual CI risk analyses to support interdependencies analysis and management and to allocate resources of the region and higher levels of government; and
8. Aggregate risks and resilience levels to regional, state and national totals for overall management and accountability.

One of the most important requirements is the choice of key terms and the scale of measurement to estimate risk and resilience. While risk/resilience management should be flexible to the choice of options to improve security and resilience, CISR-RMP's specific purposes require that risk, fragility (expected outage),[13] benefits of options to reduce risk and/or expected outage, and costs of options be defined consistently and measured or estimated exclusively with ratio scales. *Ratio* scales of measurement exhibit equal intervals (e.g., the distance between 1 and 2 is the same as that between 75 and 76) and a true zero point, meaning the absence of the quantity, thus enabling all mathematical functions. Such scales are contrasted with *interval* scales (equal intervals with an arbitrary zero, e.g., Fahrenheit temperature), *ordinal* scales (directional magnitudes, but not necessarily equal intervals, e.g., rankings, preferences on a five-point scale), and *nominal* scales (differentiating, but not ordering). These latter scales have more limited application of mathematical functions (Stevens, 1944), so have limited utility in risk analysis and can contribute to distorting decisions. Ratio scales of measurement permit the full range of mathematical functions (e.g., can be added together or divided legitimately) and are clear in their meaning across users, systems and organizations, e.g., in information sharing for interdependency analysis. All terms important

[12] It is necessary to estimate risk and expected outage from the perspectives of both the lifeline CI owner and the regional public in order to identify and manage externalities (where actions by one actor impose benefits or costs on others without charge or compensation, e.g., toxic waste of a chemical plant) and public goods (once created, available to all without restriction, e.g., national defense). This is a key requirement to assure rationality at both CI and regional levels, with possible complementation by higher levels of government.

[13] "Risk" (the expected value of loss) is the negative quantity to be reduced to advance the positive goal of "security," and "expected outage," also called "fragility," is the negative quantity to be reduced to advance the positive goal of "resilience." Expected outage is defined as the probability-weighted likelihood of outage, while outage is the average daily unmet demand multiplied by the number of days of unmet demand. To make it an expected value similar to risk, it is weighted by the *same* likelihood of an event and the vulnerability of the asset to the associated risk. If a system is totally resilient, its expected outage is zero – the perfect case of resilience. The phrase, expected outage, was chosen because it is descriptive, the opposite of resilience in a physical sense (resilient objects return to their original shape after being stressed, while fragile ones break; resilience systems continue to function while stressed or restore function rapidly if interrupted, fragile ones fail). The term could readily be changed if another term is preferred.

to risk analysis can readily be expressed using ratio-scale metrics, such as threat likelihoods, vulnerabilities, most consequences (including outages), benefits and costs. All have true zero points and can be measured using equal intervals.

In an attempt to simplify, however, many risk methods use ordinal scales, such as low-medium-high-very high or green-yellow-red. Even when these are "quantified" by assigning numerical names to points on the ordinal scale, say a 1 to 4 or 1 to 10 scale, or still finer gradations, the nature of these scales do not change—they are fundamentally still ordinal scales, the *names* of which are numbers. There is no assurance that all the intervals are equal and necessarily contain open-ended categories, e.g., "greater than" or "less than." Only by *assuming* equal intervals, true zero and a value for open-ended categories can ordinal scales be used for addition, subtraction, multiplication or division, or used in benefit/cost or return on investment calculations. However, such assumptions cannot be justified or defended.

Yet, these are the mathematical functions needed to calculate the process outputs needed to support the key decisions. For example, valuing net benefits of an option requires that risk with the option be subtracted from the risk without it, then subtracted from the option's costs; benefit/cost ratios and return-on-investment calculations require division; and aggregation of risk or benefits requires that they be subject to addition; etc. All these calculations require ratio scales; they cannot be carried out legitimately using other scales without making assumptions that could distort decisions.

Ordinal-scale methods for CISR run significant risk of distorting decisions because they necessarily compress the scale of measurement, where both consequences and likelihoods can vary by *several orders of magnitude*. This is especially the case in the very largest consequences and the very smallest likelihoods – that is, where very unlikely events have disastrous consequences. In such cases, where the most discriminating risk analysis has the greatest value, ordinal scales collapse vastly different quantities into single categories, with consequences in the "greater than" top category and threat likelihood at the "less than" bottom category. Ordinal scales are often displayed as matrices of likelihood vs. consequences, usually with colors ("heat charts") indicating urgency for attention or action. They do not permit calculation of *value* of options for rational resource allocation beyond possible movement among categories. With ordinal risk, calculating benefits as the difference between the risk with and without an improvement option cannot meaningfully be done, nor can the difference be divided by costs, as in a benefit/cost ratio, nor can risks or benefits be added together (Hubbard, 2013).

The following are the minimum set of calculated output terms of the CISR-RMP needed to address the key decisions:

1 and 2. *Conditional and Full Owners' risk* is the expected value of the loss experienced by the critical infrastructure, weighted by both threat likelihood and vulnerability. *Note:* Conditional risk (i.e., setting threat likelihood to 1.0 for all scenarios) is shown in Table 2 because so many of the tools use it, *not* because it is conducive to answering the key decisions.

3. *Full Public's Regional Risk* is the sum of the expected direct and indirect losses to the regional community, including at least the sum of the owners' losses – after inclusion of interdependencies risks, lost gross regional product and a "statistical value of life and injuries."[14]

[14] The statistical value of life is an analytic construct based on future contributions to gross national product of a statistically typical person of average characteristics, e.g., age, gender, earning capacity, etc. Using it facilitates combining dollar losses and

4. *Resilience metric* measures the ability of an asset or system to continue functioning during a potentially disastrous event or, if it cannot continue, to restore function rapidly, within an acceptable amount of time. One such metric is expected outage (EO = f(T,V, O))—also called "fragility"—because it directly measures both the amount of daily service denied and the duration of that denial of service, (along with the same threat likelihood and vulnerability as in the risk estimate) with zero indicating perfect resilience, just as zero risk would indicate perfect security. Also like risk, this metric could be estimated for the CI, equivalent to expected lost gross revenue, and to the public, indicating the extent to which the region's public has experienced non-functioning CI, as lost economic performance (Rose, 2004 and 2006).
5. *Option*[15] *value* is the measure of merit in rational budget decision-making, so it is most useful to use net benefits (gross lifecycle benefits less lifecycle costs) when budget constraints prohibit funding all options with a benefit/cost greater than one. Using benefit/cost ratios when budgets are limited can result in selecting the most efficient options over options that produce the greatest total net benefits (Cox, 2008).

Calculating these outputs of the process requires that certain specific terms be estimated or collected (column C of Table 2). The requirement for ratio scales applies also to the following minimum terms:

1. Event Threat (or hazard) likelihood, T, the likelihood the event will occur;
2. Vulnerability, V, the likelihood the consequences will ensue after the event, given it occurs
3. Consequences – economic and financial losses, human casualties (with others qualitatively described), to the owner C_O and to the public, C_P, and outage (daily unmet demand times the number of days of denial);
4. Outage of service as a resilience metric defined as the daily unmet demand times the number of days of service denial;
5. Dependencies and interdependencies in the form of the likelihood of denial of necessary product or service to specific assets under specific threat scenarios; and
6. Costs – lifecycle and budgetary investments, respectively, where lifecycle cost is used in benefit cost analysis and budgetary cost is used in allocating a constrained budget.

Further, if the results of the tools are to be compared outside the immediate analysis, aggregated or used in interdependency analysis, they should all start from a common, standardized set of initial threats and hazards (that are mutually exclusive and collectively exhaustive, although some may be ignored as inapplicable or tolerable – see column D of Table 2) and proceed through the same estimation process logic. The results will be consistent and comparable across time and infrastructures, thus supporting progress reporting, interdependency analysis, higher-level trade-off decisions and outcomes-based performance assessment, and aggregated to higher levels of government and whole sectors for policy and program planning at those levels. Generally, if the requirement that risk be measured on ratio scales is not met, these uses cannot be supported.

The row headings in Attachment 1 show additional detailed specifications based on the risk disciplines. These were also used as criteria in the cursory tool review in the next section, with the results as shown there.

human casualties for considering overall risk and benefits of risk-reduction options. Generally, it is preferable to display to decision-makers the individual components of risk even if they are also combined for analysis.

[15] "Option" is used in its broader sense of alternatives available for choice, not in the financial derivatives sense.

C. A Summary Review of Federally Sponsored Tools To identify candidate tools for use or modification for a CISR-RMP, the project team conducted a series of meetings with federal agencies with responsibility for different aspects of CISR, especially the lifeline infrastructures. The inquiry was limited to federally sponsored tools because they can be acquired, modified and controlled by the federal government, whereas privately developed tools entail additional costs, proprietary rights and control issues. The federal respondents were asked to describe their tools, methods and processes for lifeline CI risk and vulnerability analysis and near term plans in some detail. Altogether, the team identified and reviewed twenty-one tools and processes through a series of screenings.

- Three of the tools were complementary tools that can be used to estimate important terms in the risk equation, e.g., economic consequences or future weather, but do not actually estimate risk or benefits. These were set aside. There are a significant number of such tools beyond those examined in this review.[16]
- Seven of the tools consisted of very detailed surveys that produce scores that benchmark the entity using the approach against others also using the survey. The Office of Infrastructure Protection (IP), the Transportation Security Agency (TSA) and the National Institute of Standards and Technology (NIST) make extensive use of this approach. For the purposes of CISR-RMP, these tools can identify areas of potential concern and suggest options for improving security and/or resilience. They operate through compliance with standards or best practices as defined by the experts who developed the tools. They do not measure risks, expected outage or benefits, so they cannot support rational decisions that maximize benefits within constraints. These were not further assessed for this project.[17]
- Five tools estimated elements of the risk equation, but relied on ordinal scales of measurement, so as previously discussed, they run a serious risk of distorting resource allocation decision-making away from the rational standard. They do provide evidence, however, that risk-oriented thinking is taking place among their users and might be able to be evolved into full ratio-scale risk methods by changing the scales used. These tools are shown on the lower portion of Table 2.
- Six tools (one in two versions, the first published in 2010 and the other in process of being updated) estimated the terms of the risk equation using ratio scales, as shown at the top of Table 2. Five of the six, however, use conditional risk, assuming that threat likelihood of at least one terrorist attack is 1.0, a certainty, for purposes of analysis. This approach is necessitated by the position of the Intelligence Community to decline to quantify these risks. Conditional risk unavoidably distorts the key decisions because the likelihood of terrorist attack on a specific asset or subsystem in a given location is several orders of magnitude smaller than the likelihood of other threats in an all-hazards analysis and may, itself, range over several orders of magnitude. Any of these could readily be converted to full ratio risk by providing the missing terrorism threat likelihood. Most of the agencies using these tools are aware of the issue and are generally ready for and favorable toward this change if (and in some cases only if) official threat likelihoods,

[16] The complementary tools were CMIP Climate Data Processing Tool (DOT/FHWA), Hydraulic Engineering Circular Vol. 25 (DOT/FHWA), and Water Health and Economic Analysis Tool (WHEAT, USEPA).

[17] The survey-based indicator tools were Baseline Assessment for Security Enhancement (BASE) for Mass Transit (DHS/TSA), BASE for Highway Vehicles (DHS/TSA), Infrastructure Survey Tool (IST, DHS/IP), Modified IST (DHS/FPS), NIST Cyber Security Framework (DOC/NIST), NIST Infrastructure Community Resilience Framework (DOC/NIST), and Pipeline Corporate Security Review (DHS/TSA).

approved by an authoritative source, are provided. Developed by the U.S. Army Corps of Engineers, the dams risk tool, Common Risk Method – Dams (CRM-D), uses conditional risk in two ways: for single facilities, threat likelihood is set to 1.0, but for multi-facility analysis, there is an adversary choice model to differentiate among the facilities, *given* that one of the facilities will be attacked.

- The one exception to using conditional risk is the standard, *ANSI/AWWA J100-10: Risk and Resilience Management of Water and Wastewater Systems*, which the American Water Works Association (AWWA) is currently in the process of updating to be released as ANSI/AWWA J100-15. J100-10 allowed conditional risk (though J100-15 will not), but also provided a “proxy” method for approximating terrorist threat based on the notion of the terrorist selecting a specific target and attack mode. It is referred to as the “proxy” method because it stands in lieu of a real estimate, a place-holder until an authoritative threat likelihood measure is available. The method uses the number of annual attacks, the region and target type choice of city, is based on an interpretation of global actual terrorist events by the RAND Corporation and Risk Management Solutions, Inc., (Willis, et al., 2007) and local conditions to estimate likelihood.[18] The proxy uses relative attractiveness to the terrorist, defined as the product of vulnerability (likelihood of success, given attack) and consequences measured earlier in the process divided by the sum of these products as one of the terms in the process. If the options reduced vulnerability or consequences, they reduced the attractiveness to the terrorist. Because vulnerability is measured from the point when the attack is initiated, additional assumptions were included to estimate the likelihood of pre-attack detection and interdiction based on the number of assailants and the difficulty in obtaining key items needed to mount the attack without calling attention. The resulting likelihoods ranged from 10^{-2} to 10^{-9}, which was judged as a reasonable range by the J100 Standard Committee. This approach uses some of the same ideas as CRM-D, but arrives at a complete threat likelihood proxy estimate, albeit by a number of heroic assumptions.

The last column of Table 2 shows the level of each tool on the capability maturity model used in U.S. Department of Defense (DOD) and several other agencies, including elements of DHS, ranging from (1) ad hoc, beginning, undocumented; through (2) repeatable; (3) defined enough to be a standard business process; (4) managed through quantitative metrics; to (5) optimizing choices and self-improvement. None of the tools relying on conditional risk can reach level 5 because conditional risk cannot be used to calculate benefits, lacking a terrorist threat likelihood. Tools using it in lieu of full risk cannot claim to make fully rational resource decisions, even within constraints, so the project team assigned them a level 3. CRM-D is higher because, on a portfolio level, the relative likelihood of an adversary’s choosing a specific dam is based on the dam’s relative attractiveness, so a very limited optimization is possible, although benefits calculations are limited to accepting the partial likelihood. J100-10, in defining and using crude, approximate terrorist threat likelihood, is able to support constrained optimization.

It is remarkable how the intelligence community’s declining to quantify terrorist or malevolent threat likelihood has impeded the application of risk management to CISR, considering that only one tool is actually able to support the all-important resource allocation decisions, and that is by using a very rough approximation.

[18] Willis personally provided a cursory review of the approach and concluded that it used the data in his report as intended (personal conversation with Brashear, 2010).

The project team found that the ratio scale tools all use roughly comparable concepts and definitions of conditional risk, vulnerability and consequences. All measure risk from the perspective of the owner of the CI as opposed to the public. Three of the tools apply only to terrorist or malevolent threats. The Transportation Research Board (TRB) *Costing Asset Protection: An All Hazards Guide for Transportation Agencies* (CAPTA) deals only with natural hazards associated with climate change and THIRA and J100 (both editions) use an all-hazards approach. The similarities are sufficient to conclude that, at this level of review, THIRA and J100 could either be converted to a common approach (perhaps with tailored versions to specifically apply to specific sectors) or a "Rosetta Stone" translator could be developed to make them comparable enough to analyze interdependencies, regional lifeline risk and resilience.

THIRA is the primary tool for the National Preparedness program under PPD-8. All states and the 28 highest risk regions currently participating in the Urban Areas Security Initiative (UASI) program use THIRA, as required to qualify for FEMA grants. THIRAs have been almost exclusively conducted by emergency managers. Although usually presented as comprehensive risk analysis for the "whole community," to date it has been limited to thirteen response and selected recovery core capabilities only. Most of the response options address capability sizing, location and operations during and immediately after an incident. Lifeline infrastructures have not been included in most THIRA assessments and virtually none has taken up THIRA as its risk tool. Some jurisdictions, e.g., San Francisco, have begun to educate potential users outside the emergency response community to the THIRA process, presumably to include them in future THIRA applications. Recall that NIPP 2013 calls for THIRA to be "employed" for critical infrastructure, but as this analysis suggests, using it could distort decisions relative to the rational standard because it uses conditional risk. While some infrastructure options may be operational or require a subtle adjustment in the physical design, many of the options will be very high-cost, very long-term, capital investments. For these, the use of conditional risk could lead to hugely wasteful allocations of significant quantities of resources.

THIRA is currently undergoing a "refresh" as part of the larger update of the Preparedness program, but it is not expected to incorporate likelihoods in any quantitative form, even for natural hazards.

J100-10, which is designed to comply with the details of NIPP 2009, Appendix 3 (see Appendix B) does support resource allocation. It has been applied to about 100 water and wastewater systems, including some of the nation's largest, such as Chicago, Illinois; the National Capital Region, among them the District of Columbia Water and Sewer Authority, Washington Suburban Sanitary Commission and Fairfax County (Virginia) Water Authority; Richmond, Virginia; Long Beach, California, and Minneapolis, Minnesota. It has also been used in electricity and highway systems, and was the primary tool in the regional resilience feasibility conducted in the Nashville-Davidson County (Tennessee) Area (Brashear, et al., 2011), where it was used successfully in electricity distribution, water/wastewater, highways, emergency communications and dispatch, fire suppression, emergency medical service and police emergency operations. Its core methodology, Risk Analysis and Management for Critical Asset Protection (RAMCAP) Plus, was adapted to eight diverse infrastructures and extensively field-tested in a program sponsored by DHS/IP.[19] J100 is the only tool that uses a ratio-scale measure of resilience (in this case, expected outage) at facility, system and regional levels.

It is important to note that federal agencies sponsored all of these tools, so they reflect federal concerns and focus on lifeline sectors predominantly operated by local public agencies, specifically water/ wastewater, dams and highways. In sectors that are predominantly operated in the private sector, such as energy and telecommunications, the project team found no comparable widely used tools. Based on confidential conversations with knowledgeable people in these industries, most companies are well aware of the threats and hazards they face, but use self-generated tools or proprietary tools applied by expert consultants. Exploring possible comparability or sharing of tools and/or data will likely require a location-specific approach.

D. CISR-RMP Design Lessons from the Review of Federally Sponsored Lifeline Risk/Resilience Tools Some of the reasons for these findings came from discussions with the federal personnel who presented these tools and made suggestions. They include:

- *Differing perceptions of risk* – Even among those tools that use risk concepts, there are at least three basic concepts: (1) Emergency responders tend to focus on vulnerabilities that could cause fatalities and serious injuries and, perhaps secondarily, major property losses as things to be addressed through robust preparation for the “worst-of-the-worst” operational eventualities. Because life is precious, conditional risk makes sense to them. (2) Those that take the conventional engineering/economics/business perspective focus on allocating resources to maximize net benefits of reduced casualties and financial losses, benefit/cost ratios or return on investment, so full risk from the *perspective of the CI owner* makes sense to them. (3) Those trained in public policy see the objective as constrained net benefit maximization (human and economic), but focus on the benefits and costs from the *perspective of the public*. Those holding any of these perspectives seldom agree, because they all believe they take the correct view. All three are legitimate in their respective domains: emergency response, enterprise management and public policy and programming, respectively, although any use of conditional risk can significantly distort decisions. A CISR-RMP should acknowledge this legitimacy and incorporate all three where appropriate. AWWA J100-10 recognizes the distinction between the owners’ and the public’s perspectives by estimating both.
- *Unclear roles and responsibilities* – While it is generally assumed that the CI owner has first responsibility for security and resilience investments, it is also clear that, in many cases, the CI owner must forego potential public benefits because the owner judges the level of benefits captured *directly* by the owner to be insufficient to justify the investment. Yet, neither the public nor local jurisdictions are aware of these decisions even though they may be profoundly impacted. Liability laws, corporate confidentiality and rate-justification requirements all act to limit the ability of CI owners to engage the public to collaborate financially in making these investments. Measuring risks and benefits to the public as well as the owner, and making adjustments in institutional and legal issues, could address this impediment.

[19] The methodology looked at nuclear power plants (and applied by all U.S. plants), nuclear waste management, chemical manufacturing, oil refining, LNG terminals, dams and locks, college campuses, and water/wastewater systems, and evolved into ANSI/AWWA J100-10.

- *Local expectations of federal bailouts* – Echoing state and local emergency managers, several federal employees candidly expressed the belief that if a major event should devastate a specific locality, the federal government will make it whole. Under this belief, local officials may regard risk/resilience management as optional or not important; tolerated if tied to grants; but not a significant decision-driver. In times of limited budgets and increasing numbers of increasingly serious events, the rapid and continuing escalation of federal outlays for disaster relief have caused numerous observers, including the Office of Management and Budget (OMB) and the U.S. Government Accountability Office (GAO), to note the need to reverse that trend for budgetary reasons. Risk/resilience analysis must be central to that effort, using a collaborative basis that allows both CIs and regional communities to make reasonable trade-offs and take responsibility for them.
- *Limited local expertise* – Few local CIs or jurisdictions employ risk experts. Most rely on outside consultants, who are often free to use processes and tools of their own design, for better or worse, thereby adding to the difficulty in comparing results. Hubbard (2009, pp. 68-77) attributes the popularity of ordinal risk and index tools over ratio-scale tools to the proselytizing of management consultants. When voluntary federal tools are supported by active user training, technical assistance and quality assurance (TTA&QA), they have been more widely accepted and used. This demonstrates that when such expertise is available at little or no cost, it contributes to the acceptance and proper use of the tools.
- *Local resistance to federal direction* – Early in the life of DHS, the agency's heavy handedness left the local level with a distaste for all federal direction. Many of the federal employees have since experienced "pushback" while trying to implement tools or requirements. The local CI and government employees, which see themselves as diverse and differentiated, fault federal programs for assuming uniformity across local settings. NIPP 2013 and related documents explicitly recognize this diversity through the voluntary nature of local participation, seeking federal-state-local collaboration in lieu of federal mandates. Such voluntary collaboration should be prominent in both the design of the CISR-RMP and the plan to implement it.
- *Organizational silos* – At the local and regional levels, the dependencies and interdependencies of CIs are among the most important threats to operational continuity and resilience. Risk tools advanced by federal agencies, each to its local counterpart, result in a variety of tools that cannot be used to compare risks or to support collaboration to manage interdependency risk. The development of common, consistent CISR processes (but not necessarily common tools) that all lifeline CIs (and other CIs and organizations in the community) and local jurisdictions can use, along with appropriate information-sharing protections, could allow reasonable collaboration and integration in both analysis and in equitably investing in solutions. Note: such a solution would also require agreement and collaboration among the federal agencies responsible for oversight of these CIs.
- *Lack of terrorism likelihood data* – Local jurisdictions and operating units of lifeline infrastructures do not have the ability to obtain information on the likelihood and nature of terrorist attacks. Several federal agencies also cited the lack of terrorism likelihood information as the principle driver of their use of conditional risk. Information sharing between the intelligence community and the CI community would address this. The U.S. Coast Guard is able to sustain its Maritime Security Risk Analysis Model (MSRAM) by securing the cooperation of the

intelligence community, of which it is part. AWWA J100-10 includes a "proxy" method for estimating terrorism threat likelihood based on RAND and Risk Management Solutions historical data and local conditions (Willis, *et al.*, 2007). An office of DHS could be assigned the responsibility of intermediating with intelligence agencies and translating their qualitative information to pragmatic direction for state and local agencies' use. Rough order-of-magnitude precision is all that is required, but it should be differentiated by location, target type and attack mode. Without this or some alternative, all-hazards risk analysis cannot be done without major risk of distorting users' and the public's decisions.

- *Lack of continuity and methodological maturation* – DHS and other federal agencies have begun several risk-management processes that existed for a relatively short time with limited testing and implementation, then were discontinued for reasons that are seldom explained. Examples include the RAMCAP series (which, in industry hands has become one of the most advanced of the originally federally sponsored tools, AWWA J100); Voluntary Chemical Assessment Tool (VCAT) (which was decommissioned in favor of a survey/index approach); the DHS Science & Technology (S&T) sponsored feasibility pilot test of Regional Resilience/Security Analysis Process (dropped due to S&T budget cuts); and others. The terminating events seem to be associated with changes in administrations, changes in senior personnel, frustration among users due to limited expertise, lack of organizational processes by the sponsors to support technical assistance or to facilitate local coordination and collaboration; etc. The result is that *few full risk analysis methods have matured to the point of effectiveness and self-perpetuation.* A process of iterative improvement, perhaps through an open-source process, would allow tools to accumulate experience and mature over time. The project team suggests shielding CISR-RMP development from these contingencies by organizing the federal effort for development and implementation in a non-federal center, along with long-term, multi-agency funding and governance that reflects the federal sponsors, end users from lifeline and other CIs and local governments, and recognized risk experts (both academic and practitioners).
- *Cybersecurity may always be standards-driven* – The "mere" facts of huge numbers of uncounted daily attacks (of all kinds and purposes) on CIs' cyber systems and the complexity of the CI systems involved makes full R=T×V×C risk management problematic for cybersecurity. This is especially true for "zero day" possibilities of vulnerabilities that have yet to be identified. Many such vulnerabilities can be attributed to errors in programming by third-party software developers. If one cannot define the specific nature of the threat or the system's vulnerability to it, it is difficult to see how conventional risk processes apply. The contemporary convention of best-practice standards-based guidance (e.g., the National Institute of Standards and Technology [NIST] Cybersecurity Framework, 2014) may be the best risk management process currently available for cybersecurity. Risk management processes can be fruitfully applied, however, to the threats of control-system failures of various durations and risk mitigation options, such as manual controls or back-up automation, and may be feasible and desirable.

Appendix D includes an expanded discussion of the technical criteria and the review of federally sponsored tools. Several of the lessons learned in this review and the associated discussions with federal employees were mirrored in the perceptions and frustrations of actual users of the tools, as summarized in the next section.

4. Local CI and Regional Decision Context and Constraints

To understand the decision context of risk management at the local lifeline, emergency response agency and region level, it is necessary to examine the current processes, decision environment and constraints in which these parties operate. The project team conducted a number of semi-structured interviews with a non-random selection of actual decision-makers, staffs and members in lifeline CIs, local agencies and regional public-private coalitions. These interviews provided a vivid understanding of on-the-ground conditions through the perceptions, aspirations and constraints of likely users: managers and analysts of local lifeline infrastructures and local government agencies. These interviews characterized the situations these individuals operate in and the pragmatic requirements of a CISR-RMP that they could and would use.

Overall, respondents from the predominantly public-sector lifelines (water/wastewater and roads, bridges and tunnels) and local governments were very forthcoming in sharing information about their use or non-use of risk analysis. This was much less true of lifelines typically owned and operated by private industry, particularly energy and telecommunications, perhaps based on their being highly regulated and keen to avoid additional regulation. The local emergency managers surveyed, however, generally found the private-sector providers in their service areas accessible and cooperative on substantive issues around emergency response and recovery.

The range of capabilities and expertise that directly focus on physical and cyber risks associated with interdependent lifelines and regions is wide. Some very large and forward-thinking jurisdictions and utilities have adopted risk management as standard operating procedures, but most have not, either neglecting to deal with CISR or simply complying with federal and state requirements. Many of the larger systems use risk methods that are unique, proprietary or narrowly threat-specific, and cannot readily be transferred or integrated. Outside of these, lifelines and local jurisdictions have actually performed very little risk analysis, and no resilience analysis beyond continuity of operations/continuity of government planning. They generally see resilience as synonymous with reliability or as an outcome of risk management rather than a goal in itself or something to be analyzed separately from risk. The availability of spare personnel and funds for hiring consultants to undertake substantive analysis is sharply limited. Requirements from an external authoritative source (e.g., higher government, industry standards, regulatory agency) can ease the allocation of the time and limited funds to risk analysis because it removes the need to justify the work.

In general, the respondents reported very little routine, systematic risk analysis outside the emergency response function and the water sector. The most frequently observed pattern: an event would happen, usually with an event-caused outage, to demonstrate a need for remedial investment. Many of the potential CISR-RMP users interviewed do not currently use formal risk analysis. Few of those who do were satisfied with their processes. In interviews for this project, a number of these potential users reported conducting a process simply to comply with requirements from higher authorities, rather than actually basing decisions on the results. All of them, however, have business processes that could readily use the results of risk analysis: strategic, capital and operational planning, operating and capital budgeting, performance appraisal, etc.

One reason for this limited use is the widely held belief among local agencies and many lifeline operators that if disaster strikes, the federal or state governments will step in to pay for recovery and restoration. This parallels the view of many of the federal employees interviewed in the tool review. Therefore, they doubt the value of investing in prevention, protection or pre-event mitigation. One respondent went so far as to say, “Investing 100-cent dollars of local taxpayer or ratepayer money before a highly uncertain future event seems irrational compared to paying 25-cent dollars of local taxes after the event has become a certainty, if and when it ever does.” Another risk-oriented respondent commented, “There is a huge need to educate and inform elected officials and professionals. They don’t see the payoff.” Several stressed the importance of continuity in risk analysis methods and results in educating elected and appointed budget- and rate-setting boards to the basic concepts of risk management. Clearly, the business case must be made for using risk analysis and investing in risk mitigation at all.

At the same time, state and local officials and infrastructure operators increasingly recognize the need to better understand all-hazards impacts on interdependent CIs. The interviewees expressed serious interest in using a simple, low-cost, transparent and manageable process to prioritize actions and investments in security and resilience. Ideally, such a process could be routinely carried out by their own staffs, perhaps with a minimal level of training and the availability of technical assistance. Increasingly, their focus is on pre-event prevention, protection and mitigation (including resilience), as well as post-disaster collaborative response, recovery, restoration of critical assets and systems. Those organizations that are interested appreciate expert advisors for both process and substantive suggestions on risk assessment options, but cost and time remain serious constraints.

A near universal issue, especially in the private sector, is fear of legal liability and negligence suits associated with conducting risk analyses and then experiencing casualties or damages due to a known risk that was determined to be too low priority to justify attention. Another issue is the costs associated with identifying risk that requires substantial investment to mitigate. Respondents believed that some corporate general counsels and city attorneys might resist risk analysis for these reasons. The respondents strongly recommended that the liability issues be resolved as soon as possible.

Virtually all the respondents were keen to better understand their risks and outage possibilities, especially as caused by dependencies on others and climate change, and to improve their ability to evaluate and justify security and resilience options. The project team did not encounter complacency, but the complacent might not have been amenable to being interviewed. All were acutely aware of their dependencies and interdependencies, especially to power outages, and some have taken steps to reduce this vulnerability with back-up power. Most infrastructure managers the project team spoke with were sensitive to the essential role played by their service in the well-being of their communities. Several public-sector owners spontaneously raised the issue of balancing risk reduction for their own systems with maintaining or restoring service rapidly to the customers, a concrete example of the dual NIPP objectives of security and resilience. Several indicated that it is crucial to address the economic impacts on the community as well as the utility as part of the risk analysis, “especially when there’s not enough return on investment to make the business case using impacts to the utility only,” as one local utility official said.

For the most part, resilience is equated to continuity of business, continuity of operations planning or continuity of government, and dealt with by continuity plans and exercises. In some major areas, however, public health officials and non-profits engaged in preparedness for community groups and at-risk individuals are focusing on community resilience with regional lifelines and other service providers. Across the nation, numerous utilities and service providers are incorporating resilience into their own continuity planning and are beginning to join with other organizations and associations focusing on community and regional resilience.

Several CI owners suggested linking any new methods directly with on-going local processes such as asset management and/or economic and community development, and integrating them to increase the likelihood that the methods would be sustained over time and potentially lead to savings in the costs of the analysis efforts. The water, electricity and highways subsectors have all taken up asset management mainly to address the risks of seriously aging assets, but extending to all hazards, including financial ones—in other words, full enterprise risk management. Many respondents mentioned the need to find a way to measure security (risk) and resilience (fragility, or expected outage) in ways that can be reported to and understood by rate-setting boards, local governments, customers, the general public and state and national agencies, especially those that provide grants.

Most CI operators had not thought about whether risk and resilience tools should be comparable across sectors, but those who had thought about it expressed the view that comparability would have many advantages, including in conducting interdependencies analyses and, especially, in better educating elected officials and their budget staffs, rate-setting bodies and the general public. Especially with larger investments in long-term security and resilience, selling risk reduction and resilience enhancements to these groups is necessary for the investments to be made.

Many respondents expressed significant concern about the locally pressing aspects of climate change. Along both coasts and the Gulf Coast, the concern is coastal storm surge and sea-level rise associated with increasingly intense storms. In the Midwest and South, the issues are severe ice storms and snow in winter, leading to major flooding with spring snow melt, and tornadoes and derechos in summer. Much of the West is experiencing extreme drought and rampant wildfires. Virtually all of them are seeking solutions, but the idea of formal risk analysis and option valuation is seldom seen as part of that search.

In most areas, the relevant agencies, e.g., emergency management, public health, public works and the respective utilities (whether publicly or privately owned), are stove-piped from one another, with little or no interaction, so interdependencies are virtually never analyzed (beyond the decision of whether to acquire back-up generators). CI managers are acutely aware of the issue, but lack the tools and data to address the issue. A major constraint on interdependency analysis is their reluctance to share highly sensitive information with anyone outside their own organizations. The former can be resolved by developing needed tools and models; the latter by developing a detailed protocol for defining the minimum effective set of data needed, listing necessary safeguards and establishing penalties for violations. The prospect of increasing their own ability to manage interdependencies may offset the concerns about exchanging the minimum data necessary, under well-understood and enforced safeguards. In both cases, field-testing at scale would be needed to establish the mutual value of interdependencies analysis and the credibility of the protections.

Beyond these generalizations, the respective lifelines exhibited subtle differences and distinctive features from one another:

Water/Wastewater. The water sector is a partial exception to the finding that little risk analysis is actually being performed by local CIs. The Bioterrorism Act of 2002 required all drinking water systems serving more than 3,300 people to conduct vulnerability or risk analyses and submit their results to the U.S. Environmental Protection Agency (EPA). In many utilities, this experience established an appreciation that risk analysis helped to make the case for needed investments in security and reliability. AWWA, the sole standards development organization for the water utility sector, adapted the water/wastewater method developed by the American Society of Mechanical Engineers (ASME) under DHS/IP sponsorship

(ASME, 2007b) into an American National Standard, ANSI/AWWA J100-10, the technical features of which were discussed previously. Released in 2010, J100-10 has sold several hundred copies, and DHS has designated the standard under the Safety Act, providing certain liability offsets to its users.

Many larger and mid-sized water and wastewater utilities have used J100-10 or are currently using it. One official of a large regional public water system pointed out that, "[They] use the EPA-recommended J-100 for Threat and Vulnerability Assessment for water and that it is quite sufficient." Another major private-sector water system representative stated that he has used RAMCAP (ASME, 2009, the immediate predecessor to J100-10) since the mid-2000s for vulnerability assessments and is exploring some new versions of software. (Most of the major water system engineering firms offer a service based on the standard.)

Transportation. In the lifelines other than water, respondents reported considerable interest in risk analysis and the beginnings of regular use by some of them. The transportation sector is also experiencing increased interest. *The Moving Ahead for Progress in the 21st Century Act* (MAP-21) (P.L. 112-141, signed July 6, 2012) set performance standards and requires a "risk-based asset management plan" that includes capital asset inventories with condition assessments, target improvements relative to performance measures, formal investment prioritization processes (based on risk-reduction and life cycle costs) and progress reporting for highways (including bridges and tunnels) and transit systems. States are encouraged to include all highway infrastructure assets within highway rights-of-way. Sharing rights-of-way with water and energy distribution systems is quite common, minimizing eminent domain issues, but augmenting interdependencies (proximity) risks. The rulemaking process to implement these requirements is currently on going. States will be required to conduct "risk management analysis" to assets relative to threats posed by "current and future environmental conditions, including extreme weather events, climate change, and seismic activity" in the words of the rulemaking summary; a ten-year financial plan; investment strategies to improve or preserve assets; and an on-going system for measuring and managing the condition of roads and bridges." At least one state department of transportation (Colorado) has initiated a project to adapt the J100-10 method to this task.

Energy. In electricity, the North American Electric Reliability Corporation (NERC) is focused on raising and maintaining bulk power reliability, i.e. continuity of service at defined quality levels by the major transmission grids. The overall method is to establish mandatory standards and monitor compliance. NERC has developed a Critical Infrastructure Protection method, NERC CIP, a conditional risk approach designed for compliance, now in its fifth edition. Nuclear power plants are subject to regular and continuing probabilistic risk analysis for a variety of hazards, but mostly for those that would cause a release of radioactive material or lead to major meltdown. As part of the earlier ASME RAMCAP development, all U.S. nuclear plants completed a RAMCAP analysis. Other power plants and distribution systems typically have robust physical security programs covering both physical and cyber security. Many routinely exercise the detailed models used to plan and/or control their systems' operations to identify ways of managing the loss of various assets. "N minus one" analyses, a simulation of how the systems would adapt to sustain service if major assets were out of service one at a time, are routine in many power distribution systems. While such exercises directly address routine resilience, the project team did not find standardized all-hazards risk analysis among these organizations. The IEEE Power and Energy Society very recently recommended integrating analysis for security and resilience with asset management for a holistic approach to all hazards, including wear and aging (Novosel *et al*., 2014).

Telecommunications. Telecommunications providers are less formal in their approach to risk. They rely on their design engineers and maintenance personnel to identify potentially vulnerable situations involving their primary assets and perform limited, informal benefit/cost analysis to justify investments in risk reduction and resilience enhancement. They rely on “industry best practice standards,” internal company standards and historical experience with equipment failures to identify areas of concern. Telecommunications depend heavily on electricity to operate, so they make extensive use of batteries and emergency generators at their sites to assure reliable function during power outages. One telecommunications executive predicted any federal initiative to implement risk analysis requirements would be strongly resisted as “sounding like regulation,” but expressed that a sound, *voluntary* framework advanced through a partnership with state and local government and other private entities would be more favorably received, especially if it provided extensive sharing of information useful to their decision-makers.

Emergency response. In emergency management of Urban Area Security Initiatives (UASI) regions, THIRAs are required for the grants, but are not used by FEMA in setting eligibility, grant amounts or specific allocations. THIRA is nominally comprehensive, covering all five preparedness mission areas for all hazards, but, so far, it is being used only in response, and executed largely by emergency managers at the local level, making it stove-piped as well. The FEMA guidance to date has only included 13 of 31 core capabilities that relate to response and early recovery. Those interviewed believed that THIRA is almost exclusively executed by emergency managers, with the funds very definitely expected to go to police, fire, rescue and emergency management, with only the smallest allocation, if any, directed toward infrastructures. THIRA has *not* been adapted for or adopted by lifeline infrastructures, despite the NIPP 2013 “call for action” to the contrary.

One typical respondent called THIRA a “good concept, but a pain… a necessary evil,” and suggested it be made “less bureaucratic,” yet provide more concrete definitional and procedural guidance for those using it, especially in selecting among competing options. The current, broadly defined directions were seen more as cause for anxiety about whether they were applying it correctly than as the flexibility envisioned by its authors. Other users made similar comments, seeing THIRA as “very basic,” and almost always used as a means to comply with requirements for grants than in broader risk management. In the few places where THIRA is used for decision support, interviewees said they use it to identify the most severe consequences and to rank response capability-building actions based on them. Vulnerabilities and, especially, threat likelihood play a much smaller role than consequences in resource allocation. The direct threat-capability linkage follows the traditional emergency management approach, so it feels natural to those using it. Emergency managers suggested a number of improvements to THIRA, including development of a simple, but explicit common methodology to help delineate and estimate vulnerabilities and consequences and sort out options to justify selections and flexibility in choices (as opposed to “mandates”), coupled with more information about what capabilities and best practices others are using successfully. Several users expressed concern that ignoring threat likelihood could encourage mis-allocations. In virtually all the jurisdictions, emergency managers and the uniformed first responders completed the THIRA assessment and received the majority of the FEMA funding. Infrastructures were consulted mostly in areas having to do with first-responders’ capabilities, e.g., water for fire suppression, electricity for shelters and mass care facilities.

In addition to THIRA, respondents noted other extensive, federally sponsored programs and tools that address vulnerability- and risk-related issues, including vulnerability analyses or surveys conducted by federal Protective Service Advisors (PSAs) and TSA field personnel. Several emergency managers reported that in the words of one, these “are a mixed bag.” Some offer substantial help and insight, but others less so, being intrusive, time consuming and overly prescriptive as to countermeasures that communities should implement. None had specifically received risk analysis assistance from PSAs, and several were skeptical that the surveys offered were effective in understanding risk or deciding what to do about it. Several respondents expressed the observation summarized by one, “DHS is about checking the boxes, not information sharing or problem-solving.”

In summary, lifeline CIs and emergency responders seldom conduct risk/resilience analysis to allocate resources to options to enhance CISR, but they are generally amenable to a competent process that provides substantial value to them in the near term (e.g., grant eligibility, aid in selecting and defending options, and concrete insight into their vulnerabilities to interdependencies), that is low-cost or no-cost, and simple enough for their staffs to perform and explain to management and oversight agencies.

Appendix C includes additional reporting of the results of the interviews and their interpretation.

5. CISR Risk Management Process Design

A. Detailed Design Specifications Table 3 summarizes the specifications drawn from (1) the policy review, (2) the technical defensibility assessment and (3) the review of the conditions of use for a CISR-RMP. It contains the most important design specifications, while more-detailed, technical ones are shown as the row titles in Attachment 1. The next section returns to this list of specifications to define the currently most pressing gaps in the available tool set.

Based on these specifications, the project team designed a CISR-RMP in enough detail to specify the necessary components, their characteristics and their logical sequence. The preliminary process integrates specific analysis-and-decision workflows divided into five phases that correspond to the five phases of NIPP 2013 and the Supplemental Tool. The phases are carried out through close interaction and information sharing among local lifeline enterprises (public and private); regional consortia or public-private partnerships; and state and federal CISR programs. Each phase is defined by the operational, analytic and decision tasks, and other information necessary to manage CISR rationally and effectively.

The design specifies the process at three levels:

1. The individual CI enterprise, where the focus is on rationalizing its own resources from its own perspective;
2. At the regional coalition or partnership level, where local collaborations can analyze interdependencies in confidence and rationalize resource allocation from the regional public’s perspective through negotiations with the CIs and the orderly search for new resources; and
3. At the state/national level, facilitating the CIs and regions through policy and programs; training, technical assistance, quality assurance (TTA&QA); the selective application of funds; and aggregates the results at each phase for reporting, policy-making and accountability.

Table 3. CISR-RMP Design Specifications by Source

Basis of Specification	CISR-RMP Design Specifications
Federal Policy	
NIPP 2013	1. CI risk estimated by identifying what assets are critical, taking interdependencies into account
	2. *Threat, vulnerability and consequences* to support rational choices among action options
	3. Selected options implemented & their performance evaluated
	4. Include physical, cyber and human assets
NIPP 2013 Supplemental	5. Documented – self-documenting, fully explicit; decision-oriented
	6. Reproducible – measurement reliability; comparable/consistent across time; minimum subjectivity
	7. Defensible – integrated & compliant with standards of risk & uncertainty management disciplines
Risk Mgmt Fundamentals	8. Unity of Effort – holistic integration & synchronization of entities w/ risk-mgmt responsibilities
	9. Transparency – clear, open and direct communications
	10 Adaptability – dynamic & responsive to changing conditions and improving methods
	11. Practicality – simple & useable, given analytic/data limitations, organizational & political realities
	12. Customization – common analysis but local choices, designs of improvement options
Implicit	13. Accountability – measurement & reporting of actual results in improved risks & resilience
	14. Advance PPDs 8 & 21, CISR R&D Plan, IP Strategic Plan for local/regional integrated programs
Technical Defensibility	15. Set goals, objectives & priorities (weights) systematically
	16. Standardized threat/hazard set that is mutually exclusive and collectively exhaustive
	17. Asset criticality based on mission
	18. Risk = Threat Likelihood × Vulnerability × Consequences, all in ratio scales, $, casualties, other
	19. Resilience measured in ratio scale (preferably based on expected outage, fragility) in units & $
	20. Common definitions, process & threats for consistent, comparable metrics across sectors
	21. Meet all conditions for meaningful aggregation within/across sectors and to higher levels
	22. Uncertainty explicitly treated using at least sensitivity analysis
	23. Dependencies & interdependencies modeled explicitly
	24. Options based on site/design/construct, prevent, protect, mitigate, respond & recovery
	25. Explicit valuation of risk/fragility reduction benefits & life-cycle costs
	26. Rational resource allocation to options
	27. Managed, monitored & documented implementation and operations of selected options
	28. Resources allocated so incremental benefits are paid by CI, local govt, regional P3, state, federal
	29. Explicit performance evaluation of amount of risk- & fragility-reduction achieved
	30. Full uncertainty with Monte Carlo simulation or risk & expected outage, with interdependencies
User Design Specs	31. Model protocol for information sharing
	32. External initiation by recognized authority, e.g., industry standard, state or federal standard
	33. Easy to use, free or low-cost system, with improvements through open process
	34. Enable analysis to address internal business case and regional community case simultaneously
	35. Provide immediate and obvious value to CI & local government decision-makers
	36. Analysis conducted by employees of CIs & local agencies, with training and technical assistance
	37. Standard threat/hazard set including, especially, weather hazards due to climate change
	38. Common analytical process for dependencies, but *not* mandated solutions
	39. Low or no-cost technical assistance from local, state or federal employees trained in depth
	40. Liability resolution for untreated risks accepted in a rational, analytically based trade-off process
	41. Address major dependencies & interdependencies in fully protected information sharing process
	42. Integrate with extant asset mgmt, planning, budgeting, development systems of CIs, local govt

* Certain desirable specifications, such as full capture of uncertainty and correlations in estimates, Monte Carlo combination of results, output as distributions and portfolio optimization, are deferred for the near term as requiring too much user education to be included at present. These should be developed for the future and introduced as user sophistication grows.

This section summarizes a business process design for a CISR-RMP that meets these specifications. This section then reviews this design relative to design specifications in Table 3 to identify the availability and apparent effectiveness of available components. Where components are missing or inadequate, “gaps” are defined for additional R&D, developmental field pilot testing and, when all components meet minimum acceptability, field demonstration pilots.

B. Design Summary of CISR-RMP for the Single Enterprise Based on the design objectives and the tool that best meets the technical criteria, the project team developed an initial enterprise-level CISR-RMP, as summarized in Figure 3. (Note: For this report an “enterprise” is an individual CI, government agency, or other organized entity, public or private, that voluntarily chooses to use the CISR-RPM.) The process parallels the five phases of the NIPP 2013 Risk Management Framework through which the enterprise fulfills the objectives of the NIPP Framework while managing its own security and resilience in its unique situation. The work performed in each of its five phases includes:

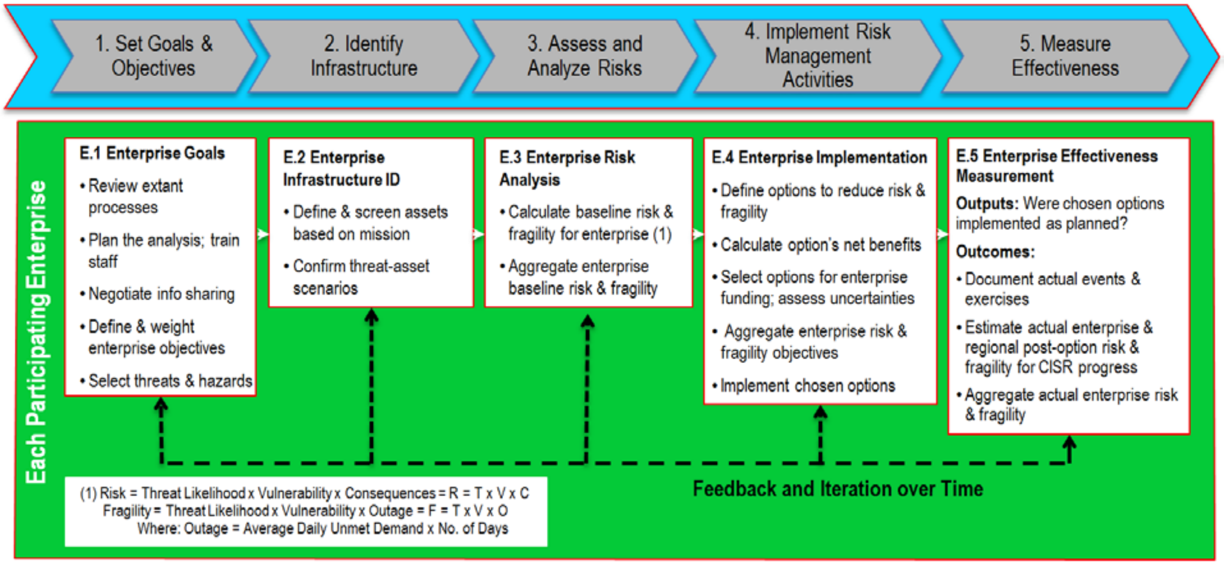

1. Set Goals & Objectives
2. Identify Infrastructure
3. Assess and Analyze Risks
4. Implement Risk Management Activities
5. Measure Effectiveness
Each Participating Enterprise
E.1 Enterprise Goals
• Review extant processes
• Plan the analysis; train staff
• Negotiate info sharing
• Define & weight enterprise objectives
• Select threats & hazards
E.2 Enterprise Infrastructure ID
• Define & screen assets based on mission
• Confirm threat-asset scenarios
E.3 Enterprise Risk Analysis
• Calculate baseline risk & fragility for enterprise (1)
• Aggregate enterprise baseline risk & fragility
E.4 Enterprise Implementation
• Define options to reduce risk & fragility
• Calculate option's net benefits
• Select options for enterprise funding; assess uncertainties
• Aggregate enterprise risk & fragility objectives
• Implement chosen options
E.5 Enterprise Effectiveness Measurement
Outputs: Were chosen options implemented as planned?
Outcomes:
• Document actual events & exercises
• Estimate actual enterprise & regional post-option risk & fragility for CISR progress
• Aggregate actual enterprise risk & fragility
Feedback and Iteration over Time
(1) Risk = Threat Likelihood x Vulnerability x Consequences = R = T x V x C
Fragility = Threat Likelihood x Vulnerability x Outage = F = T x V x O
Where: Outage = Average Daily Unmet Demand x No. of Days

Figure 3. NIPP 2013 CI Risk Management Framework & Summary of Single Enterprise CISR Risk Management Process

E.1 Define the enterprise’s goals and objectives based on its mission and functions; prioritize them by systematically assigning relative importance weights; review the existing business processes to see which could contribute the risk management process as defined by this model CISR-RMP; plan the analysis, train the analysts and select the threats and hazards of greatest concern from a standard threat/hazard set.

E.2 Identify and screen the systems, subsystems and assets that are crucial to the mission and functions, and compose threat-asset pair scenarios.

E.3 Calculate current and projected ***enterprise baseline*** risk and fragility (i.e., no new risk mitigation) for each threat-asset pair and aggregate them in a form useful for decision-making in the next phase.

E.4 Sort the threat-asset pairs into those the enterprise will accept without treatment, those it will transfer through insurance and those it will act upon. Develop mitigation/resilience options to address this last group, and estimate the amount the options will reduce one or more of the elements in the risk and fragility equations, re-estimating risk and fragility, then *valuing the options from the enterprise* *perspective* based on their net benefits[20] and life-cycle costs. Select and implement those options that best meet the CISR goal (i.e., greatest net benefits) and other enterprise goals up to the budget constraint. Their gross benefits are their ***enterprise outcome objectives***, and, in aggregate, the enterprise CISR objectives.

E.5 Evaluate the performance of the options relative to their implementation and operations plans and the progress they have made by re-estimating current ***actual enterprise outcomes*** of reduced risk and fragility based on the results of any real events (local or remote but similar) and local exercises; compare the actual performance to the enterprise's baseline and objectives; and make mid-course corrections.

When it is possible to make use of the enterprise's existing business processes, models and tools in planning and conducting CISR risk management, it eases the integration of the CISR-RMP into the on-going, routine business processes of the enterprise. Risk management ceases to be a special event and becomes normal.

The process then repeats and improves based on feedback, changing conditions and consideration of additional assets and hazards. The results of the process may be aggregated for local and higher-level decision-making in Phase 3 – baseline risk and fragility; Phase 4 – option valuation and risk and fragility reduction objectives of options; and Phase 5 – actual, overall CISR progress from the original baseline and the degree actual outcomes met mitigation objectives.

Processes much like this are essential to success in industries where risk is a central part of their business models, e.g., pharmaceuticals; natural resource exploration and development; nuclear power generation; and, of course, insurance and reinsurance; among others. All of them use probabilistic risk analysis conducted using ratio-scale metrics and standard threat events. Many quantify not only the point estimates, but also the uncertainty in these estimates, a future step for the CISR-RMP. Even without this improvement, use of this general approach with these measurement scales is essential to meeting the diverse requirements of a CISR-RMP for interdependent enterprises and regional collaboration.

C. Design Summary of CISR-RMP Process for the Regional Coalition This enterprise-level process is linked to a regional process, as shown in Figure 4. The regional process iterates between each of the enterprises and a voluntary regional coalition or public-private partnership through information sharing and collaboration. A formal, legally binding information-sharing and protection agreement governs communications that flow between the two levels. Such an agreement and the interactive process are necessary to allow: (1) CI interdependencies analyses, (2) funding or cost sharing of options with exceptional benefits that the enterprises individually cannot justify, (3) the evaluation of actual outcomes of reduced risk and fragility, including interdependencies, and (4) aggregation of results at phases 3, 4 and 5 for reporting and accountability.

The work flow of the regional coalition ("the region") parallels that of the enterprises and interacts with them as follows:

R.1 Form or adapt a voluntary regional coalition through a series of meetings, workshops and tabletop exercises for CI and local government managers to increase understanding that failures of lifeline

[20] Net benefits are the difference in risk between the threat-asset pair's risk with the option and without it (the gross benefit) less the life-cycle costs of the option. Where benefits and/or costs extend beyond the present year, both are estimated over time and discounted to present value.

infrastructures are major threats to everyone that cannot be addressed by enterprises working alone; negotiate and adopt the information sharing and protection agreement; define and weight regional goals and objectives; and select the threats and hazards from the standard set and reconcile them with those of the participating enterprises.

R.2 Identify regionally critical infrastructure systems and define threat-system scenarios as the basis for working with the enterprises to assure all regionally important threat-sysem scenarios are reflected in the enterprises' threat-asset pairs.

R.3 Analyze dependencies, interdependencies and regional ecomomic impacts using the results of the enterprise baseline risk and fragility analyses, then estimate an overall ***regional baseline*** risk and fragility from the perspective of the regional public; and aggregate it for use by regional decision-makers and, in a summarized form, the general public.

R.4 Re-analyze the dependencies, interdependecies and economic impacts, assuming both enterprise-funded and unfunded options, by ***valuing all options from the public perspective***. Some options with very large public benefits may be unfunded by enterprises because of insufficient *enterprise* benefits or falling below the budget constraint.[21] These represent foregone public benefits that could be obtained by inducing the enterprises to accept top-ranked unfunded options. Inducements could be financial incentives, funded locally or from outside the community; regulations, building codes and land use zoning; privatizing parts of CIs, federal and state grants-in-aid; etc. In aggregate, the reductions in risk and fragility associated with the full set of funded options are the ***regional CISR objectives.***

R.5 Evaluate the ***actual regional outcomes*** performance of all the implemented options, based on enterprise information and indepenent validation of the amount that aggregate risk and fragility have been reduced, to gauge the extent to which the region has made progress from the regional baseline and met its regional objectives. Aggregate regional performance for use at higher levels of government and with the general public.

The participating enterprises use risk management process that are logically and methodologically equivalent—i.e., all are versions of the model CISR-RMP, so their results are consistent and comparable—as customized for their existing internal processes, technologies and settings. By doing so, they voluntarily participate in the regional process because each stands to gain, potentially significantly, from the collective analysis of interdependencies; the possibility of external, incremental funding or cost-sharing; and the positive image of contributing to regional public well-being. Importantly, each enterprise benefits from the resilience of the region in which they operate. The regional coalition facilitates both integration of the enterprise analyses and collective decision-making to capture otherwise foregone public benefits. As experience accumulates, the regional coalition also becomes a shared trusted source of new ideas for cost-effective options and local information sources.

Attachment 2 and Appendix E describe the CISR-RMP for enterprises and regional coalitions in greater detail.

[21] This step addresses the classic problems of the "tragedy of the commons," "co-benefits" and other externalities, public goods and other underinvestment in options with public benefits. Note that the enterprises are expected to make the investments that they can justify, which the regional coalition may confirm in shared analyses under the information sharing agreement. The sequence of decisions results in a form of "optimizing at the margin" across the enterprises and the region as a whole.

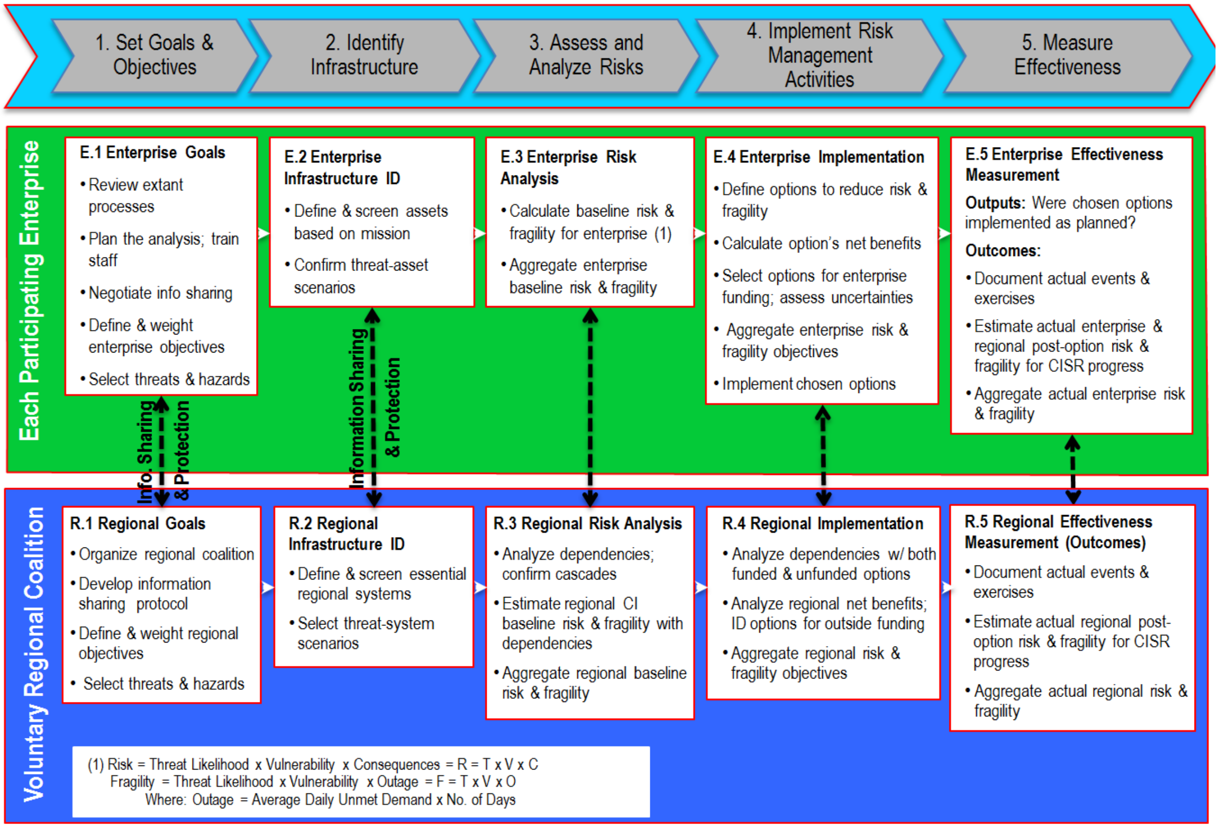
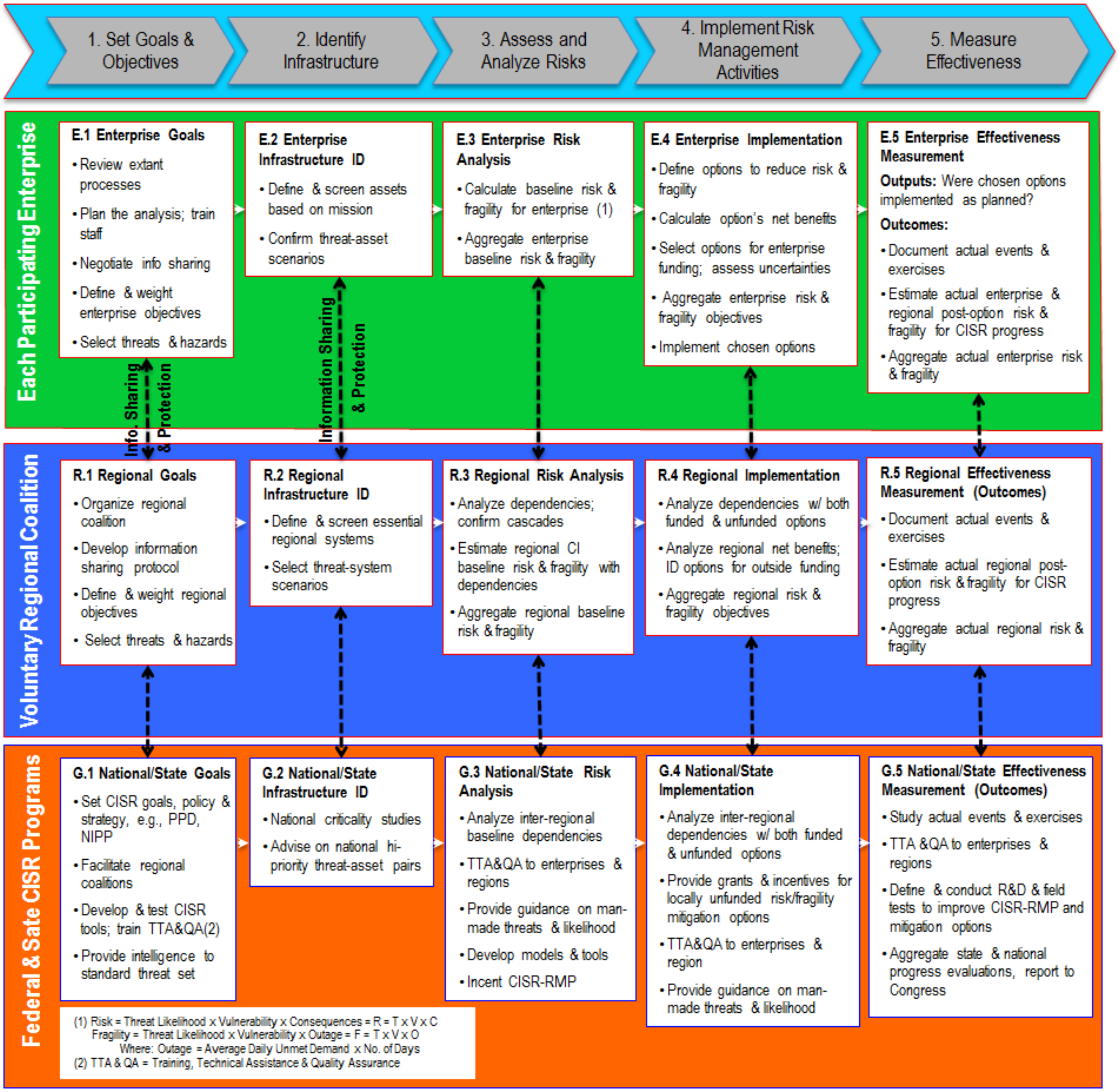

1. Set Goals & Objectives
2. Identify Infrastructure
3. Assess and Analyze Risks
4. Implement Risk Management Activities
5. Measure Effectiveness
Each Participating Enterprise
E.1 Enterprise Goals
• Review extant processes
• Plan the analysis; train staff
• Negotiate info sharing
• Define & weight enterprise objectives
• Select threats & hazards
E.2 Enterprise Infrastructure ID
• Define & screen assets based on mission
• Confirm threat-asset scenarios
E.3 Enterprise Risk Analysis
• Calculate baseline risk & fragility for enterprise (1)
• Aggregate enterprise baseline risk & fragility
E.4 Enterprise Implementation
• Define options to reduce risk & fragility
• Calculate option's net benefits
• Select options for enterprise funding; assess uncertainties
• Aggregate enterprise risk & fragility objectives
• Implement chosen options
E.5 Enterprise Effectiveness Measurement
Outputs: Were chosen options implemented as planned?
Outcomes:
• Document actual events & exercises
• Estimate actual enterprise & regional post-option risk & fragility for CISR progress
• Aggregate actual enterprise risk & fragility
Info. Sharing & Protection
Information Sharing & Protection
Voluntary Regional Coalition
R.1 Regional Goals
• Organize regional coalition
• Develop information sharing protocol
• Define & weight regional objectives
• Select threats & hazards
R.2 Regional Infrastructure ID
• Define & screen essential regional systems
• Select threat-system scenarios
R.3 Regional Risk Analysis
• Analyze dependencies; confirm cascades
• Estimate regional CI baseline risk & fragility with dependencies
• Aggregate regional baseline risk & fragility
R.4 Regional Implementation
• Analyze dependencies w/ both funded & unfunded options
• Analyze regional net benefits; ID options for outside funding
• Aggregate regional risk & fragility objectives
R.5 Regional Effectiveness Measurement (Outcomes)
• Document actual events & exercises
• Estimate actual regional post-option risk & fragility for CISR progress
• Aggregate actual regional risk & fragility
(1) Risk = Threat Likelihood x Vulnerability x Consequences = R = T x V x C
Fragility = Threat Likelihood x Vulnerability x Outage = F = T x V x O
Where: Outage = Average Daily Unmet Demand x No. of Days

Figure 4. NIPP 2013 CI Risk Framework & Summary of Enterprise and Regional CISR Risk Management Process

D. Design Summary of CISR-RMP for the Federal/State Governments Satisfying a long-standing Congresssional requirement, the regional and enterprise aggregations can help state and federal agencies assess the effectiveness of their CISR programs that operate through the local and regional enterprises and coalitions. Conversely, state and federal CISR programs can contribute to the effectiveness of the enterprise and regional programs by performing a number of necessary functions in each phase of the process (Figure 5). State and/or national CISR programs:

G.1 Begin each cycle by setting goals, policies and strategies; facilitate regional coalitions; develop and test methods and tools for use at all three levels; and train federal and state personnel who will provide ***training, technical assistance and quality assurance*** (TTA&QA), including validation of methods, data, assumptions and results, to regions and enterprises; and integrate timely, qualitiative and quantitative intelligence into the specifications of the standard threat and hazard set.



	1. Set Goals & Objectives	2. Identify Infrastructure	3. Assess and Analyze Risks	4. Implement Risk Management Activities	5. Measure Effectiveness
Each Participating Enterprise	**E.1 Enterprise Goals** • Review extant processes • Plan the analysis; train staff • Negotiate info sharing • Define & weight enterprise objectives • Select threats & hazards	**E.2 Enterprise Infrastructure ID** • Define & screen assets based on mission • Confirm threat-asset scenarios	**E.3 Enterprise Risk Analysis** • Calculate baseline risk & fragility for enterprise (1) • Aggregate enterprise baseline risk & fragility	**E.4 Enterprise Implementation** • Define options to reduce risk & fragility • Calculate option's net benefits • Select options for enterprise funding; assess uncertainties • Aggregate enterprise risk & fragility objectives • Implement chosen options	**E.5 Enterprise Effectiveness Measurement** **Outputs:** Were chosen options implemented as planned? **Outcomes:** • Document actual events & exercises • Estimate actual enterprise & regional post-option risk & fragility for CISR progress • Aggregate actual enterprise risk & fragility
Voluntary Regional Coalition	**R.1 Regional Goals** • Organize regional coalition • Develop information sharing protocol • Define & weight regional objectives • Select threats & hazards	**R.2 Regional Infrastructure ID** • Define & screen essential regional systems • Select threat-system scenarios	**R.3 Regional Risk Analysis** • Analyze dependencies; confirm cascades • Estimate regional CI baseline risk & fragility with dependencies • Aggregate regional baseline risk & fragility	**R.4 Regional Implementation** • Analyze dependencies w/ both funded & unfunded options • Analyze regional net benefits; ID options for outside funding • Aggregate regional risk & fragility objectives	**R.5 Regional Effectiveness Measurement (Outcomes)** • Document actual events & exercises • Estimate actual regional post-option risk & fragility for CISR progress • Aggregate actual regional risk & fragility
Federal & Sate CISR Programs	**G.1 National/State Goals** • Set CISR goals, policy & strategy, e.g., PPD, NIPP • Facilitate regional coalitions • Develop & test CISR tools; train TTA&QA(2) • Provide intelligence to standard threat set	**G.2 National/State Infrastructure ID** • National criticality studies • Advise on national hi-priority threat-asset pairs	**G.3 National/State Risk Analysis** • Analyze inter-regional baseline dependencies • TTA&QA to enterprises & regions • Provide guidance on man-made threats & likelihood • Develop models & tools • Incent CISR-RMP	**G.4 National/State Implementation** • Analyze inter-regional dependencies w/ both funded & unfunded options • Provide grants & incentives for locally unfunded risk/fragility mitigation options • TTA&QA to enterprises & region • Provide guidance on man-made threats & likelihood	**G.5 National/State Effectiveness Measurement (Outcomes)** • Study actual events & exercises • TTA &QA to enterprises & regions • Define & conduct R&D & field tests to improve CISR-RMP and mitigation options • Aggregate state & national progress evaluations, report to Congress

(1) Risk = Threat Likelihood x Vulnerability x Consequences = R = T x V x C
Fragility = Threat Likelihood x Vulnerability x Outage = F = T x V x O
Where: Outage = Average Daily Unmet Demand x No. of Days
(2) TTA & QA = Training, Technical Assistance & Quality Assurance

Figure 5. NIPP 2013 Framework & Summary of Enterprise, Regional, State and/or Federal CISR Risk Management Process

G.2 Conduct studies to identify infrastructures and systems with national or international criticality (e.g., the North American power transmission grid) and the threats or hazards with the greatest consequences to them, then advise the responsible enterprises and regions so they are certain to be addressed in their respective CISR analyses.

G.3 Analyze ***baseline*** dependencies and interdependencies of systems that are larger than regions and provide the results to regional and enterprise interdependencies analysis; provide direct TTA&QA to enterprises and regions, including quantitative intelligence guidance to enterprises and regions on man-made threat likelihoods; develop new and improved tools and models; and provide incentives for enterprises and regions to adopt CISR-RMP into their standard business processes.

G.4 Analyze dependencies and interdependencies of the larger systems, assuming implementation of *all* options, both funded by enterprises and/or regions and unfunded, ***valuing the unfunded options from the national perspective*** to determine if significant national benefits would be foregone if they remain unfunded; provide grants, cost-sharing or other incentives to fund those with greatest national public net benefits; and provide quantitative intelligence support and direct TTA&QA to enterprises and regions analyzing their own sets of options.

G.5 Study actual events around the world for insight into vulnerabilities, consequences of various types and levels of attacks and natural events, as input to modeling and estimation; provide TTA&QA to enterprises and regions in evaluating program outcomes (validation is most important here); conduct R&D and field tests to improve the CISR-RMP (methods, models and data) and risk/fragility mitigation options; aggregate regional and state performance assessments to a national assessment that compares actual performance of the participating enterprises and regions against the national baseline for ***measuring progress against the baseline and performance against objectives*** for evaluating national CISR programs; and submit periodic reports of all phases to the Administration and Congress.

The importance of state and/or federal personnel providing TTA&QA is that it enhances the quality and consistency of the analyses; provides local, no-cost advice and coaching; accelerates learning by enterprise and regional personnel; offsets some of the local costs; and integrates the analytical efforts of diverse enterprises and regions into coherent state and national programs. A centrally directed TTA&QA capability is virtually universal among industries where risk management is essential to their success.

Evidence with related tools indicates that when federal tools are accompanied by federal TTA&QA, significant numbers of enterprises and local governments provide access, information and their expertise in their own systems. According to GAO (2015), in Fiscal Years 2011 through 2013, PSAs performed 3,255 assessments, the Federal Protective Service performed 1,458 and TSA performed 545. During the same period, the Coast Guard directly performed 93 risk analyses and oversaw up to 3,500 assisted self-analyses using the ordinal risk tool, MSRAM. THIRA, the partial risk tool by FEMA with essentially complete market penetration for its target audience, is supported by annual training programs and is required of all states and UASI regions that desire to participate in certain FEMA grant programs, although the amount and purposes of the grants are not tied to THIRA results. This suggests that though active, supported federal involvement is necessary to move technical CISR risk assessment tools of any type into widespread use by targeted users, it clearly can be done.

This overall CISR-RMP design presents an additional opportunity. If the national program is built around the concepts of open-source software, it may be able to very rapidly iterate to incorporate improvements based on the experience and creativity of an active community of users; adapt to unforeseen circumstances and additional sectors; and enhance analysts’ and decision-makers’ abilities to tailor the process to their own needs, while maintaining the consistency of the process and comparability or results.

6. A Roadmap to Implementation

As summarized in the last section and described in more detail in Attachment 2 and Appendix E, the CISR-RMP is a business process, *not* a tool. Its functional logic and principles may be implemented through a variety of tool configurations and still serve the purposes of interdependencies analysis and an integrated regional public-private approach. This notion is central to the implementation approach outlined in this section.

The project team concluded the project with a "roadmap" to operationalize the risk management process by simultaneously closing the most critical component gaps and a novel way of initiating CISR-RMP implementation in the field. As with the process design itself, the implementation approach is a balancing of the "ideal"—all users apply the same CISR-RMP in the same way—and the "pragmatic"—users design and incorporate their own CISR-RMP functionality as they see fit. The former would imply a degree of coercion incompatible with the collaborative approach described in the policy documents and NIPP 2013. The latter risks the rise of indefensible methods and non-comparability of results, foregoing the ability to conduct interdependencies analysis, regional analysis, cross-sector comparisons and aggregation—all key design objectives.

As noted in Section 4, a great deal of the use of federally sponsored risk analysis tools has been limited to compliance, sometimes begrudging, with requirements rather than as core drivers of risk-based decision-making. Substantial frustration was expressed about federal personnel and contractors trying to impose new approaches without appreciation for the local situation or the existing tools and processes already in use. The CISR-RMP described in this report represents a model approach, but it could be implemented in a wide variety of specific forms while still enabling users and regional coalitions to meet the objectives requiring direct comparability. A promising, but untried approach would be to find ways to start with and adapt the *existing* business processes to incorporate the essential elements of the CISR-RMP into the users' routine management processes so completely that it is sustained and used routinely as part of planning and resource allocation. In other words, truly enable the lifelines, local jurisdictions and regional coalitions to make the decisions that determine security and resilience in ways that raise the rationality of the overall regional effort.

Unlike the usual "top down, outside-in" federally sponsored, local/regional risk management programs, the CISR-RMP team would approach prospective users with a more organic, "bottom-up, inside out" business process engineering solution. The team recognizes that these organizations are "going concerns," in the parlance of accounting, with data, models (digital and mental), processes and the relationships currently in place, and builds upon them, evolving the existing processes to meet the most important specifications of the CISR-RMP, but not necessarily in the same way or with the same tools. The approach developed in this project suggests an innovative, business process engineering approach to implementation: build directly on the tools and data already being used by the lifeline CIs, with *them* choosing the particular versions of optional CISR-RMP tools to use, as integrated into their on-going processes.

Operationalizing a lifelines and regional risk/resilience management process means working out the implementation details. This will entail three related efforts:

a. Gap-narrowing – closing the most important gaps in the CISR-RMP design with at least one acceptable tool (acceptable alternatives would be preferred) so that the design will be complete;

b. Case studies – a series of detailed case histories of how actual infrastructure and local government users of some of the more advanced tools (e.g., AWWA J100, CRM-Dams, THIRA and/or others) have implemented and used them in decision-making, to increase the in-depth understanding of how these tools have been implemented and used and the relationships of these tools with other business processes, e.g., continuity planning, asset management, capital planning and budgeting, operations planning and budgeting; and

c. Developmental field pilot projects (first one, followed by an additional two or three, as experience with the first and resources permit) in diverse regions, with diverse lifeline infrastructures to develop and test the organic, bottom-up approach in actual field settings.

The first two efforts should proceed simultaneously because they both are needed as preparation for planning the developmental field pilots. The second and third will provide user validation of the CISR-RMP and the organic implementation process.

A. Design vs. Specifications: Narrowing Primary Gaps in Available Methods Before actually field testing the complete process, some methodological gaps must be closed, all of which will require integration to move data among the components, to culminate in the desired calculations and decision-oriented displays. Table 4 summarizes the design specifications, notes the primary CISR-RMP features that address them; and rates their readiness for use. The majority of the specifications are fulfilled with the synthesis of extant tools and methods currently available and ready for use, most having been widely used already. The remaining gaps are indicated by a readiness score of 7 out of 10 or less, with the text shown in red.

How these gaps might be closed is discussed below, where the numbers in the headings refer to the respective lines on Table 4:

1. Dependencies modeled explicitly; 23. Dependencies/interdependencies & regional economics; 38. Common analytical process for dependencies; and ***42. Integrates with extant asset management/ planning/budgeting systems –*** Interdependencies have long been recognized as one of the larger threats to continued operations of infrastructures, and literally thousands of academic studies have been published. (A Google search on the subject returned 8.5 million items.) Yet, to date, none of these approaches have become seen as the "standard approach." Some require significantly more data and computing capability than most of the intended users are likely to find acceptable or feasible. Many exist only at the conceptual or academic "breadbox" level. While they show promise, it is beyond the scope of the present project to sort them all out. ANSI/AWWA J100-10 and J100-15 treat dependencies as threats and instruct users to analyze them as such, but typically, users are unable to estimate the likelihood or duration of an outage by CIs they depend on because they are caused by events in other systems, about which they know very little. The few interdependencies modeling efforts that have been successfully applied on the scale of a region were seen as one-off demonstrations. Moving the respective infrastructures toward using comparable methods and threat sets makes interdependency analysis feasible, but alone, this comparability simply sets the conditions for the analysis. Moreover, interdependencies are constantly changing as equipment configurations are changed in the course of normal operations.

Most interdependencies analyses are so data intensive that it is unlikely that they will be routinely justified on the basis of occasional interdependencies studies alone. However, virtually all lifeline CIs, especially the larger ones, maintain models of their operations, digital or mental, for planning and management. These contain important data for risk/resilience analyses. It would be more likely that the CIs would collect and maintain necessary data if the same data also support one or more routine, necessary core business process, such as operations, asset management, situational awareness and/or capital planning. The recommendation would be to work with the operators of the field projects to identify relevant data and analytic tools they already use for related purposes and assess the feasibility of using them for interdependencies analysis, perhaps with some adjustment or augmentations, such as geospatial display capability, asset descriptors (including throughput) and the major links connecting dispersed assets.

If such a "merger" of CISR-RMP and other, necessary business processes were to take place, it would also increase the likelihood, frequency, quality and visibility to executives of the risk/resilience analysis. If this approach were demonstrated feasible and valuable, it is also likely that the developers of these systems would add risk/resilience analysis as a standard feature in their offerings, significantly accelerating the application of the CISR-RMP.

16. Standardized threat/hazard set; likelihood of man-made threats – Defensibility requires that the event set be mutually exclusive and collectively exhaustive (when "no event" is included). Comparability requires that it start with a common standardized threat that users may add to or delete from as they believe local conditions justify. The most important new element is that a federal agency must provide a quantified estimate of at least the order of magnitude of malevolent threat likelihood that the users can apply. As noted, while law enforcement routinely provides crime statistics, the intelligence community has declined to do so. One direct consequence of the absence of terrorism threat likelihood information is that all but one of the tools examined are unable to support the core decisions leading to rational resource allocation and effective risk/resilience management. The one exception is able to do so because it "stuck its neck out" to propose an interim "proxy" solution until more authoritative estimates become available. Only the federal government can provide the common threat set with all the needed likelihoods. Ideally, the CISR and Preparedness agencies would provide a consensus set, based on classified and non-classified information, but "massaged" to protect sources and methods. In the interim, an updated version of the J100 proxy method could be used.

22*. *Uncertainty explicitly treated and ***30. Full uncertainty & Monte Carlo simulation of risk/fragility –*** In the long term, estimating the key components of risk as probability distributions (technically, "probability density functions") and combining them by Monte Carlo simulation (maintaining correlations) would both capture and communicate the inherent uncertainty in each scenario and allow decision-makers to consider these uncertainties in making choices. It would also permit use of portfolio optimization techniques to more nearly optimize the collection of choices. This level of sophistication, however, is very seldom present in even the largest lifeline infrastructures. For the present, uncertainty should be addressed using sensitivity analysis of the components of risk and expected outage. The approach would be to see how far off each estimate would need to be to cause a change in the choices indicated, then asking whether that level of the variable is plausible. This method highlights where additional research or discussion with experts would be useful to confirm or refine the estimates. With experience using simplified risk methods, users often request sophistication. For example, novices prefer single-point estimates for the elements of risk, but with experience, they feel increasingly frustrated making point estimates of variables they know to be highly uncertain, and the exact point when they are ready to begin using ranges, then weighted ranges, i.e., probability distributions. When the users realize they cannot directly perform the calculations with distributions, they are ready for Monte Carlo

Table 4. CISR-RMP Design Specifications Fulfilled by CISR Risk Management Process
[Entries in Red Indicate That the Specification Warrants Additional Development]

Basis of Specification	#	CISR-RMP Design Specifications (Abbreviated from Table 3)	Features of CISR-RMP to Meet Deign Specifications	Read-iness
Federal Policy Design Specs *NIPP 2013 (from PPD-21)*	1	CI risk for critical assets & interdependencies	Criticality based on role in carrying out core mission; interdependencies modeled explicitly	10, 7
	2	*R = T × V × C; rational resource allocation*	R=T × V × C for each, CI & region; rational resource allocation based on net benefits to CI &region	10,10
	3	Selected options implemented & performance evaluated	Implementation monitored & actual reduction in risk & fragility measured	10,10
	4	Include physical, cyber & human assets	Physical & human explicitly treated; cyber treated as loss of automated control & according to Cyber Frwk	9
NIPP 2013 Supplemental	5	Documented –fully explicit; decision-oriented	Self-documenting in use; whole analysis oriented to 3 core decisions: TA pairs to analyze, options, eval.	10
	6	Reproducible –reliability; comparable/consistent data	Consistency/comparability rigorously controlled	10
	7	Defensible – integrated & compliant with risk disciplines	Meets basic tenets, with purposeful (temporary) simplification to aid introduction & initial use	10
Risk Mgmt Fundamentals	8	Unity of Effort – holistic integration & synchronization	Common process for all ICs & local agencies with explicit regional depend./interdepend. & all 3 decisions	8
	9	Transparency – clear, open and direct communications	Clear process & measurements, protected direct communications on regional scale	10
	10	Adaptability – dynamic & responsive	Process explicitly open for expected improvements & adaptations to emerging threats & hazards	10
	11	Practicality – simple & useable, given realities	Readily useable by local staff (when trained & assisted), practical level of initial modeling	8
	12	Customization – common analysis but local choices	Common, consistent process but complete openness to locally designed risk- & fragility-reduction options	10
Implicit	13	Accountability – measure actual improved risks/resilience	Same methods from baseline & investment decisions evaluate actual risk/fragility reduction; true outcomes	8
	14	Advances PPDs 8 and 21, CISR R&D Plan & IP Strat. Plan	Practical yet rigorous risk basis for all pieces – includes both CIs and community emergency resp./recov.	9
Technical Defensibility Specs	15	Goals, objectives & systematic weights	Goals, objectives & priority weightings using AHP	10
	16	Standardized threat/hazard set; likelihood of man-made	Standardized mutually exclusive, collectively exhaustive threat/hazard set; locally adaptable	10, 2
	17	Asset criticality based on mission	Explicit asset identification & criticality assignment based mission and gross consequences of loss	10
	18	*R = T×V×C*, all on ratio scales, in $, casualties, other	*R = T×V×C*, all in ratio scales, all in point estimates (with sensitivity analysis); later probability distributions.	10
	19	Resilience measured on ratio scale, in units & $	Resilience measured by Fragility = Outage ×*V×C, Outage = Duration* × *Severity; all ratio point estimates*	10
	20	Consistent, comparable metrics across sectors	Common process has been used in water, roads/bridges, electricity distribution, emergency ops & comm.	9
	21	Meaningful aggregation within/across sectors & levels	Expected values on ratio scales may be added because the necessary conditions all met	10
	22	Uncertainty explicitly treated	Uncertainty analyzed by sensitivity analysis for decision-change	6
	23	Dependencies/interdependencies & regional economics	All consistency requirements met; actual modeling in progress	3, 7
	24	Options from design/construct/prevent/protect/mitigate/R/R	Full spectrum of potential options explicitly considered	10
	25	Explicit option valuation in $ of benefits & life-cycle costs	Options valued by consistent life-cycle net benefits & costs from both CI and regional public's perspective	10
	26	Rational resource allocation to options, $ to $	Joint-benefit options explicitly analyzed; rational trade-off analysis at both CI & regional levels	9
	27	Managed, implementation and operations of options	CI's routine accounting & project management techniques for implementation	10
	28	Incremental $ to incremental benefits by level, CI to Federal	Mobilizes private, utility, local public, state & Federal $ in sequence to apply incremental $ to incr. benefits	9
	29	Explicit performance evaluation risk/fragility reduction, in $	Actual experience (local & other) plus exercises & red-teams support full actual risk/fragility measurement	7
	30	Full uncertainty & Monte Carlo simulation of risk/fragility	Minimal acceptable by risk discipline, but deferred in favor of user acceptance based on point estimates	3
User Design Specifications	31	Model protocol for information sharing	Several regions have developed such, but have not been synthesized or legally vetted	7
	32	External initiation by recognized authority	THIRA, J100, and several Federal indicator or ordinal tools have been accepted and are in use	10
	33	Easy to use, free or low-cost open system,	THIRA, J100 are being used without complaint about cost or effort, but could be circumstantial	9
	34	Internal business case & regional community case, both in $	Provides both based on analysis of same threats, vulnerabilities, different perspectives on consequences	9
	35	Immediate and obvious value to decision-makers	Being used by decision-makers in several CIs	9
	36	Conducted by employees of CIs & local agencies	Being done by local employees with and without outside consulting experts	10
	37	Standard threat/hazard set including climate change	Standard threat/hazard set, with local modifications, well accepted; climate-related threats major concern	10
	38	Common analytical process for dependencies	CISR-RMP has set the conditions, esp. common, consistent estimates, but tool must be developed/tested	5
	39	Low or no-cost Federal/state technical assistance	Positive examples from PSAs, FPS, FEMA, TSA; existing Federal/state personnel could be trained (?)	8
	40	Liability resolution for untreated, analyzed risks accepted	Major challenge beyond scope of present project; needs major effort	2
	41	Major interdependencies information sharing	Solid examples in several regions, but their analyses are rudimentary; adequate tool development key	5
	42	Integrates with extant asset mgt./planning/budgeting systems	Uses same metrics as these systems and complements asset management by quantifying risk & fragility	6

simulation. And so forth. For the near term, using point estimates, which all the federally sponsored tools call for, is sufficient. Concurrent with introduction of the simplified methods, training materials and software should be developed to move to the next level of uncertainty management.

29. Explicit performance evaluation risk/fragility reduction – This is a new idea for the application of risk analysis. The rationale is that if one trusts risk analysis enough to assess the risks and to allocate resources to risk-reduction options using these methods, the same methods can be used to measure the outcomes of those options—*provided* that safeguards are in place to control natural human instincts to favorably shade the results of their own work. Federal or state employees supplying TTA&QA would review both pre-investment risk/resilience analysis and post-investment performance evaluation, providing the necessary discipline to the process and coordinating the aggregation of results of analysis for reporting to higher levels of government.

31. Model protocol for information sharing and ***41. Major interdependencies information sharing –*** Interdependencies analysis will necessarily entail sharing a certain amount of very sensitive information among Cis; in particular, whether they will be able to supply their service under specific threat conditions and, if not, the likelihood and duration of service interruption. Comparability and a common threat set enable the respective CIs to answer these questions, but they still may be reluctant to share this information with others. The need is a legally vetted, detailed model protocol that spells out the conditions for information sharing, the confidentiality responsibilities of all relevant parties and serious penalties for breaches. The recommendation is for the federal government to prepare a model protocol based on best practices for information sharing in government and industry and to offer it to anyone undertaking interdependencies analyses, for adaptation to local concerns and conditions.

40. Liability resolution for untreated, analyzed risks – The CISR-RMP seeks to upgrade the rationality of decisions made in allocating resources for CISR for the greatest benefits, given constraints. This implies that choices must be made, with some risk-reduction options being funded and some not. Currently, many corporate and municipal general counsels fear that if an event were to happen, evidence that the CI or city was aware of the risk and declined an option to mitigate it could increase the CI’s liability, including punitive damages. Such counsels often oppose risk analysis for this reason, which is highly counterproductive to the objectives of CISR. The recommendation is that the federal government issue a clarification that if demonstrably competent risk analysis and management have been performed and a mitigation option declined in favor of other options with higher net benefits, punitive damages would not be appropriate. Of course, DHS and U.S. Department of Justice (DOJ) legal staffs must vet this recommendation.

Stage One pre-field, gap-closing research would address all of these to the extent possible from the field. Where on-going, specific federal roles are called for in the CISR-RMP design (e.g., developing the standard threat set with likelihoods and TTA&QA), the pilot project team would work closely with the sponsoring agency to develop the detailed requirements and test them in the pilot.

B. Case Studies: Learning How Risk Tools are Implemented and Used in Organizational Context

To better understand the context and process of risk analysis by lifelines, local agencies and, if possible, regional coalitions, a series of case studies should be conducted. These should consist of case histories of the process from tool selection through full application to the making of consequential decisions. The cases should be selected to capture actual use of the leading risk tools (e.g., AWWA J100, CRM-Dams, and THIRA). Locations would be sought opportunistically to result in a set of diverse settings and contexts. Developers or sponsors of the respective tools would be asked to nominate sites and organizations that are early adopters and/or effective users. Where possible, and depending on the tool under study, site selection would favor regions where more than one lifeline have recently undertaken risk analysis and where regional resilience coalitions already are active.

Once nominated, relevant managers in these organizations would be asked to permit researchers to interview their staff and document their experience with the chosen tool on an unattributed basis. The case studies would not specify the organization or its location unless acceptable to the organization.

The specific areas of inquiry should include:

- What was done about risk before the selection and use of the subject tool?
- What circumstances caused there to be a tool selection event? What motivated the organization to seek a new approach?
- Who selected the subject tool, how and why?
- What orientation, training or technical assistance was provided before and during application of the tool? By whom?
- Who led and who participated in the application of the tool to analyze baseline risk? How much time did each participant invest? What outside costs (e.g., consultants, data services, etc.,) were incurred?
- What information sources were used in making the necessary estimates of consequences, vulnerabilities, threat likelihood and outages? What information did the participants want that was not available at the time of the analysis?
- Were dependencies on other lifelines, suppliers, employees, etc., included in the analysis? How? What information was used and what was its source?
- How was the baseline risk summarized and by whom?
- Who decided whether risk-reduction or resilience enhancement options should be developed?
- Were options developed for specific threat-asset pairs or more broadly?
- If options were developed, were they subjected to some form of return-on-investment, benefit-cost or cost-effectiveness analysis?
- How were the options submitted to decision-makers for their consideration?
- What criteria did the decision-makers use in selecting which options to fund? Were these decisions a special event or part of routine planning and budgeting?
- Were the selected options implemented?
- Was the performance of the implemented options evaluated in some way? If so, how?
- Is there a plan to conduct an update or re-analysis of risks in the future? What commitments have been made to do so?

In addition to documenting the actual risk management process, additional, relevant processes would also be described, but in less detail. The purpose of describing these is to determine whether the risk analysis/management process might be integrated with these more routine processes to become a routine part of overall management, an organic part of good stewardship. These results could be seen as some compensation to the organization for cooperating in the project.

Ideally, several such case studies should be conducted in diverse lifelines and regions to suggest what aspects are general and which are adaptations to unique local conditions. Some sites could be selected at a very early stage of implementation and followed in real time, while others might be settings where a recent risk analysis using one of the leading tools has been recently completed. In addition to the documentation case histories themselves, they would be synthesized for lessons learned about actual application of the leading tools as parts of business processes. This synthesis would be interpreted for new insights in two areas: (1) greater substantive understanding and possible initial user validation of the analytical aspects of the model CISR-RMP because the leading tools in the cases are those that have been characterized in the model process; and (2) deeper understanding of the typical and the range of variation in organizational settings in which implementation and use take place—insights that will be needed to describe the collaborative, organic implementation and integration of the model into on-going business processes.

C. Field-Based Developmental Demonstration Pilots The design of the field-based pilots will draw heavily from the lessons learned in the case studies and gap-narrowing efforts, and would be substantially conditioned by the choices of regions and lifeline infrastructures to be included. Candidate regions would be those with lifeline CIs and local governments expressing interest in upgrading risk management explicitly, including interdependencies analysis, planning/resource allocation and implementation management across their risk mitigation and resilience decision-making. Sites would be chosen from regions that have at least expressed interest in a regional security and a resilience coalition, and at least one lifeline infrastructure already using or beginning to use one of the leading tools. Ideally, the regional coalition would already be operational and two or more lifelines would be using leading tools. The number of regions where the water and/or wastewater utilities use J100 and the local governments use THIRA is large enough that this desirable situation is rather likely. Beyond that, it would be desirable to select regions that are diverse in parts of the country and size to enable generalizations from the pilots' results.

In each region, the general approach would follow the organic, bottom-up approach as refined from the case studies and would proceed according to the first four phases of the NIPP 2013 Framework, as detailed in the CISR-RMP in Figure 5 and Attachment 2. The project planning steps in E1 and R1 would be especially important in these early efforts, as user personnel or contractors would document the existing risk, planning and budgeting processes at both enterprise and regional coalition levels and obtain examples of their inputs and outputs to determine options for evolving them to incorporate the core processes of the CISR-RMP, with the user organizations choosing which to employ. Based on these decisions, detailed implementation plans would be developed with the user staffs.

A small pilot project team would work with willing users to review their existing risk management processes (e.g., asset management, contingency and continuity planning, and budgeting) relative to the "pragmatic ideal" of the CISR-RMP to determine two things: (1) to see where, if anywhere, the extant processes might be improved by an evolution toward the CISR-RMP, and (2) whether their existing output is sufficiently consistent with other users of the CISR-RMP process to support interdependencies analyses and aggregation. Where this review suggests changes to the users' existing processes, the user would be presented available options (pre-screened for effectiveness and consistency with the CISR-

RMP) and the *user* would decide among them. The user's personnel or their contractors would be responsible for acquiring, integrating and applying the chosen options. If assistance is needed, the federal or state personnel or private-sector experts could provide training, technical assistance and quality assurance.

CISR-RMP Phases 2, 3, 4 and possibly 5 (optional because of the necessary time lag), would follow at both enterprise and regional levels, respectively, under closely monitored, facilitated and documented conditions, to glean all information that would be useful in enhancing the process for broader application in the initial regions and stepping out to additional regions. For the pilot tests, an additional documentation task would produce integrated summary documentation of each test and an update to the CISR-RMP process description and implementation approach, incorporating the results of the tests.

This organic, "pragmatic-ideal" CISR-RMP approach operationalizes and implements the voluntary and collaborative nature of DHS/IP's policy and plans without many of the major issues identified in the interviews with federal personnel and, especially, users in CIs and local governments. Judged from the perspective of the typical analysts and decision-makers interviewed, most federal risk and security programs for local application approach potential users by supplying a complete, fully refined and operational software tool with contractors to drive the work and conduct the analysis, while asking the user organization to supply the necessary data—the time-consuming part. Some approaches have gone so far as suggesting that the contractors build detailed models of the users' systems. This approach has met with resistance from the supposed beneficiaries and few such attempts have resulted in positive and sustained use of the approach after the federal experiment is completed. Even in the best cases, risk analysis and management has been seen as an episodic special event, often in response to federal or state requirements or tied to grant eligibility, rather than a routine and continuing part of management.

This common, top-down approach ignores the fact that virtually all staff and managers of CIs and local governments have models (formal, digital and/or mental) of their systems that they use regularly in design, planning, operations and management. Offering to model anew operational systems that are well understood and often modeled by their operators and managers can be off-putting, even insulting to these individuals who are the most expert in the systems they operate. Most have thought deeply about their operations and risks, even if they have not formally analyzed them. Many have experienced frustration from being on the receiving end of previous federal experiments. Many have engaged risk or security consultants for one-off studies and may be following their advice, or even using the tools left in place.

Consistent with the business process engineering approach, the roadmap suggests approaching prospective user organizations with the CISR-RMP described at no more detailed level than in this report (probably less) and offering that, after a review of their existing processes, *they* will make the decisions that will make the process operational in their organizations, while enabling them to better manage dependencies and interdependencies and contribute to regional resilience. The project team assisting the users would work closely with lifeline CIs, local governments and regional coalitions to *evolve* their *current* processes and preferences to meet the standard of defensibility and comparability essential to the CISR-RMP, making as few changes to the existing processes as possible and integrating the revised processes with the extant ones.

The CISR-RMP team would document the relevant current processes of risk management, asset management, operations and capital planning and budgeting, and contrast them *functionally* with the CISR-RMP to see where the existing processes could be used as-is or evolved to meet the standards of effectiveness and defensibility in ways that integrate readily with current, on-going processes in place. In some areas, new elements will be necessary and would be defined for acquisition or development in a subsequent implementation phase. The users would take ownership of “their” defensible process, so they would use it as an integral part of the organization’s standard process and continue its use.

The results of analyses using these adapted processes from each lifeline would be comparable enough to support interdependencies analysis and regional resource allocation for public benefit, as well as aggregation with state and local levels for policy and program decision-making. Being able to obtain precise information about specific dependencies relative to specific hazard events would motivate participation in the larger program because this information is seldom available by other means.

The labor and data would be provided primarily by user organizations, in accordance with agreed information sharing procedures developed in the first phase of the RMP, with guidance and assistance by the pilot project team. The experience of the team would provide the prototype for later direct technical assistance by federal or state employees (or equivalent in each region) who would perform the TTA&QA as part of program support and integration. The program could expand nationally as CIs and governments choose to undertake the CISR-RMP approach. A variety of incentives could accelerate these choices at manageable federal costs. Because the program would integrate “horizontal” solutions across several otherwise siloed, “vertical” functions in a region, the process could provide the underpinnings for a number of government agencies, private-sector organizations and foundations to target their programs on the most pressing local needs, while encouraging the local CIs and agencies to develop integrated CI/regional CISR programs of their own invention.

The initial pilot should be sited in a major region so it will face the full range of complex challenges of such regions, but should be bounded to a small, geographically bounded area where co-located interdependent lifelines are of particular concern. The regions selected should be diverse geographically and culturally to test the generality of the CISR-RMP, e.g., one on each coast and the third or fourth in the South or Midwest. Potential candidate regions where there are established public private collaborations and prior interdependencies work include such examples as the San Francisco Bay Area, the Hampton Roads (Virginia) area, New Orleans and the National Capitol Region. Preferably, a meaningful sub-region should be defined where at least some of the lifelines are willing to participate in the project. It should be large enough to be a thorough test, and include critical interdependencies where interdependent and especially co-located infrastructure assets pose risk of prolonged disruptions, but small enough to complete the pilot in a relatively short amount of time. Such a geographic scope may encompass a portion of a single large locality or a few smaller cities with shared lifeline providers, businesses and community services. As the project demonstrates effectiveness, it can be expanded to the full region, as well as to other regions. Other lifelines, as well as local governments or other entities may join at any time if they agree to the rules governing the coalition and are acceptable to the existing members.

7. Benefits of Developing and Demonstrating the CISR Risk Management Process

Successful completion of this roadmap will result in a number of direct and indirect potential benefits to the nation and its regions. The CISR-RMP as described:

- Supports the *whole decision cycle:* (1) *sets* security and resilience *priorities*, (2) *evaluates and selects* improvement *options* and (3) *manages* implemented options by actual, measured *performance.*

- Encourages *full integration* of the CISR-RMP functionality into the on-going routine business process of its users, so it can be sustained and routinely applied.
- Supports these decisions over the long term (capital plans and budgets), near term (operating plans and budgets) and real-time (situational awareness and incident and restoration management).
- Quantifies true *outcomes* terms: *resilience (expected outage), security (risk), benefits and progress*, rather than intermediate "output" or vague indices.
- Facilitates efficient, rational decisions because benefits are clearly defined and expressed in dollar terms, both prospective and actual, so results can be compared in conventional net-benefit, return-on-investment and benefit/cost analyses to support budget allocation decisions.
- Performs technically correct analyses but uses transparent and simple enough techniques that engineering, operations and/or management personnel of CIs and local governments can conduct the analyses and interpret the results themselves in making sound decisions, without the need for outside experts, making the results credible to decision-makers.
- Mobilizes and coordinates *private, utility, state and local funds* and generates information necessary for federal assistance and innovative finance.
- Models and manages *interdependencies* among infrastructures explicitly that can potentially cause cascading impacts on other infrastructures, their customers and the region.
- Analyzes the consequences of impairment of *cyber and manual process control systems.*
- Synthesizes descriptions of evolving crises for situational awareness and models alternative response plans before and during a crisis.
- Sequences facility *restarts* and service *restoration* after disasters.
- Incorporates man-made, technological and accidental, natural, proximity, dependency, aging infrastructure and cyber threats.
- Supports analysis and options for adaptations to climate changes in terms of sea level rise and increased severity and frequency of major storms, droughts, etc.
- Establishes an open and competitive environment for development of alternative tools that assist in carrying out the functionally and results-consistent process, which could stimulate significant new offerings by software developers and consulting firms.
- Provides common, natural metrics necessary to *measure progress* for infrastructure and regional managers, federal and state grant programs, insurers, credit-rating agencies, etc.
- Supplies an *integrating analytical structure* for holistic solutions to local challenges and for these "bottom-up" solutions to be aggregated and integrated for state and truly national programs.
- Motivates *public-private* and *private-private partnerships* around common, measured resilience, security and value objectives and action programs.
- Complements the "vertical" sector structure of the NIPP by providing "horizontal" integration of CIs, state and local governments and their stakeholders in *every* participating metro area and community.

- Educates public, private and non-profit stakeholders to the nature of the systems that support functioning communities and the requirements for their continuity of operations.
- Provides a platform for local implementation of climate change mitigation programs.
- Complements implementation of PPD-8 – Preparedness; the National Preparedness Goal; and the National Preparedness System, especially in the Protection, Mitigation and Recovery mission areas.
- Operationalizes the risk management approach defined in NIPP 2013 (and NIPP 2009).
- Implements key elements of the DHS/IP Strategic Plan: 2012 – 2016.
- Fulfills the recommendations of the State, Local, Tribal and Territorial Government Coordinating Council, the Regional Coalition Coordinating Council, and several DHS and Presidential advisory groups.
- Meets recommendations of the Homeland Security Advisory Committee for an American Resilience Assessment methodology and toolkit.
- Accords with recommendations of the National Research Council and several other expert groups' recommendations and with most of the relevant DHS plans, frameworks and policy.

This "pragmatic-ideal" approach operationalizes and implements the voluntary and collaborative nature of DHS/IP's plans within its likely future budgets. If successful, it could lead to the CISR-RMP's becoming a sustained, inherent part of routine management processes of critical infrastructures, local governments, and regional partnerships—the place where it must be to be sustained and effective in truly increasing critical infrastructure security and resilience.

Attachment 1. Detailed Technical Criteria vs. Federally Sponsored Lifeline Risk/Resilience Manangement Methods

NIPP 2013 Phase		CISR-RMP Design Objectives	Full Ratio Risk & Resilience						Conditional Ratio Risk					Ordinal Risk				
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
		Sponsor	OR/Econ/ Engg	DHS/IP/S&P CISR-RMP		DHS/S&T	AWWA	EPA/IP/ AWWA	USACE	FEMA	DoT/FHWA		DHS/TSA	USCG	DHS/IP	DoE	DOT/FHWA	
		Method/Tool	Discipline Ideal	Minimum Require-ment	Currently Available	Nashville Feasibility Pilot (1)	J100-15 In Progress	J100-10	Dam Security Tool/CRM(2)	THIRA	CAPTA	Component-Level: Bridges	Component-Level: Tunnels	MSRAM	VCAT (withdrawn)	State Energy Assess. (3)	VAST (4)	Vulner. Assessm't Framework
1. Set Goals and Objectives	1.	1. Goals & Objectives -- means for users to define and weight																
	2.	Convene & organize regional coalition or public-private partnership		🟦	🟦													
	3.	Adapt Common Information Sharing & Protection Protocol		🟦	Current Need													
	4.	Goal Setting & weighting																
	5.	a. Formal goal weighting (Multi-Attribute Utility Theory or Analytical Hierarchy Process)		🟦	🟦	🟦												
	6.	b. Informal but explicit goal statement required	🟦	🟦	🟦		🟦	🟦	🟨	🟦	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
	7.	c. Assumed to be risk and/or fragility reduction							🟨	🟦	🟦	🟦	🟦	🟦	▨	▨	▨	▨
	8.	2. Threats -- explicitly included																
	9.	a. Standard, including																
	10.	i. Terrorism	🟦	🟦	Current Need	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		
	11.	ii. Crime & Vandalism	🟦	🟦	🟦	🟦	🟦	🟦	🟨		🟨			🟨				
	12.	iii. Episodic natural hazards, e.g., storms	🟦	🟦	🟦	🟦	🟦	🟦		🟦	🟦			🟨			🟦	🟦
	13.	iv. Slowly evolving climate change, e.g., sea level rise, drought	🟦	🟦	🟦	🟦	▨			🟦	🟦			🟨			🟦	🟦
	14.	v. Cyber attack	🟦	🟦	🟦	🟦	▨	▨	🟨	▨	▨			🟨				
	15.	vi. Dependency	🟦	🟦	🟦	🟦	🟦	🟦		▨				🟨				
	16.	vii. Proximity	🟦	🟦	🟦	🟦	🟦	🟦						🟨				
	17.	viii. Age/wear/accidents	🟦	🟦	Current Need		🟦		🟨		▨			🟨				
	18.	ix. Product/service contaminated	🟦	🟦	🟦	🟦	🟦	🟦						🟨				
	19.	b. Local additions acceptable	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟦				🟨				
	20.	c. Required but no standards set								🟦						🟦		
2. ID Infra-structure	21.	3. Asset Identification																
	22.	a. Devolved from mission, function	🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟦				🟦	🟦	🟦	
	23.	b. Screened for criticality		🟦	🟦	🟦	🟦	🟦	🟦		▨				🟦	🟦	🟦	🟦
	24.	c. Required, but no standard ID process								🟦		🟦	🟦	🟨				
3. Assess and Analyze Risk (Partial)	25.	4. Risk/Resilience Analysis																
	26.	a. Risk = f(T, V, C), & fragility metrics each *estimated as distributions*, combined thru Monte Carlo simulation	🟦	Future Strategic Enhance-ments														
	27.	b. Dependencies modeled as system-of-systems, with uncertainties	🟦															
	28.	c. Portfolio modeling to find efficient combinations from correlations	🟦															
	29.	d. Post-event analysis-based real-time resource allocation	🟦	Future														

LEGEND

	Suspected	Not Suspected		
Unknown	🟨			
	Fully Present	Partially Present	Missing	
Ratio Scale	🟦	▨	Current Need	Future Need
Ordinal Scale	🟩	▧		

Attachment 1 is continued on the next page.

Notes: (1) AWWA J100-10 was the risk tool used in the Nashville Feasibility Pilot.

(2) Common Risk Model for Dams addresses human malevolent threats only. It is a conditional risk method applied in two different ways. For a single dam, threat likelihood is set to 1.0 for all scenarios, but if the analysis is for a set of dams, the likelihood of thre adversary selecting any particular dam is is estimated based on its asumed relative attractiveness based on Likelihood of Success (Vulnerabiity) and Consequences. The assumptioon is also that at least one dam will; be attacked, so the calculated risk is still conditional, but incorporating adversary choice moves it one step closer to full risk.

(3) DOE's State Energy Assessment Initiative is more a meta-analysis of needs & requirements.

(4) VAST is designed to be used with Vulnerability Assessment Framework.

Attachment 1 (Continued). Detailed Technical Criteria vs. Federally Sponsored Lifeline Risk/Resilience Manangement Methods

NIPP 2013 Phase		CISR-RMP Design Objectives	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
			Full Ratio Risk & Resilience						Conditional Ratio Risk					Ordinal Risk				
		Sponsor	OR/Econ/ Engg	DHS/IP/S&P CISR-RMP		DHS/S&T	AWWA	EPA/IP/ AWWA	USACE	FEMA	DoT/FHWA		DHS/TSA	USCG	DHS/IP	DoE	DOT/FHWA	
		Method/Tool	Discipline Ideal	Minimum Require-ment	Currently Available	Nashville Feasibility Pilot (1)	J100-15	J100-10	Dam Security Tool/CRM(2)	THIRA	CAPTA	Component-Level: Bridges	Component-Level: Tunnels	MSRAM	VCAT (withdrawn)	State Energy Assess. (2)	VAST (3)	Vulner. Assessm't Framework
3. Assess and Analyze Risk (Continued)	30.	e. Risk = f(T, V, C), each *estimated as points*		🟦	🟦	🟦	🟦	🟦	▨	▨	▨	▨	▨					
	31.	i. T = Threat Likelihood as absolute probability		🟦	🟦	🟦	🟦	🟦	▨					🟨				
	32.	ii. V = Vulnerability as conditional probability		🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	▧	▧	▧	▧	▧	▧	▧
	33.	iii. Co = Consequences to owner	🟦	🟦	🟦	🟦	🟦	🟦	🟦									
	34.	-- Liabilities: Human casualty & other	🟦	🟦	🟦	🟦	🟦	🟦	🟦			🟨	🟨	🟨	🟨	🟨	🟨	🟨
	35.	-- Direct dollar losses to owner	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	36.	iv. Cr = Consequences to the region & nation	🟦	🟦	🟦	🟦												
	37.	-- Human casualties (incl. VSL)	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	38.	-- Loss of Gross Regional Product	🟦	🟦	Current Need	▨	▨	▨		🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	39.	-- Environmental impacts	🟦	🟦	🟦	🟦				🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	40.	-- Symbolic/psychological/confidence	🟦	🟦	🟦	🟦				🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	41.	-- National security	🟦	🟦	🟦	🟦				🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	42.	f. Fragility or other outage or continuity metric	🟦	🟦	🟦	🟦	🟦	🟦		▨								
	43.	g. Dependencies modeled as system-of-systems, deterministic	🟦	🟦	Current Need	▨	🟨			▨								
	44.	h. Calculate risk & fragility to both enterpirise and regional public	🟦	🟦	🟦	🟦	🟦	🟦										
4. Implement Risk Management Activities	45.	5. Risk-Based Decision-Making																
	46.	a. Sorts risks to accept, transfer, manage	🟦	🟦	🟦	🟦	🟦	🟦										
	47.	b. Requires definition of options for managing	🟦	🟦	🟦	🟦	🟦	🟦	▨	🟦				🟨				
	48.	c.Estimates benefits based on risk analysis	🟦	🟦	🟦	🟦	🟦	🟦	▨			▧	▧	▧	▧	▧	▧	▧
	49.	d.Requires estimation of costs	🟦	🟦	🟦	🟦	🟦	🟦	▨	🟦				🟨				
	50.	i. Life-cycle costs	🟦	🟦	🟦	🟦	🟦	🟦	🟨					🟨				
	51.	ii. Budget requirements	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟨	🟨	▧	🟨	🟨	🟨	🟨
	52.	e.Joint benefits analysis	🟦	🟦	🟦	🟦	🟦											
	53.	f. Specific decision-rules for selecting options	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟨	🟨	🟨	🟨	🟨	🟨	🟨
	54.	g Sensitivity analysis of major uncertainties	🟦	🟦	Current Need		🟦	▨		🟦								
	55.	h. Routine management control systems to monitor costs and implementation milestone	🟦	🟦	🟦					🟦								
	56.	i. Post-event analysis-based real-time resource allocation	🟦	Future														
5. Measure Effectiveness	57.	6. Performance Evaluation																
	58.	a. Inputs & process assessment	🟦	🟦	🟦													
	59.	b. Outputs assessment	🟦	🟦	🟦													
	60.	c. Risk analysis based outcomes assessment, with exercises & actual events	🟦	🟦	Current Need													

LEGEND	Suspected	Not Suspected		
Unknown	🟨			
	Fully Present	Partially Present	Missing	
Ratio Scale	🟦	▨	Current Need	Future Need
Ordinal Scale	🟩	▧		

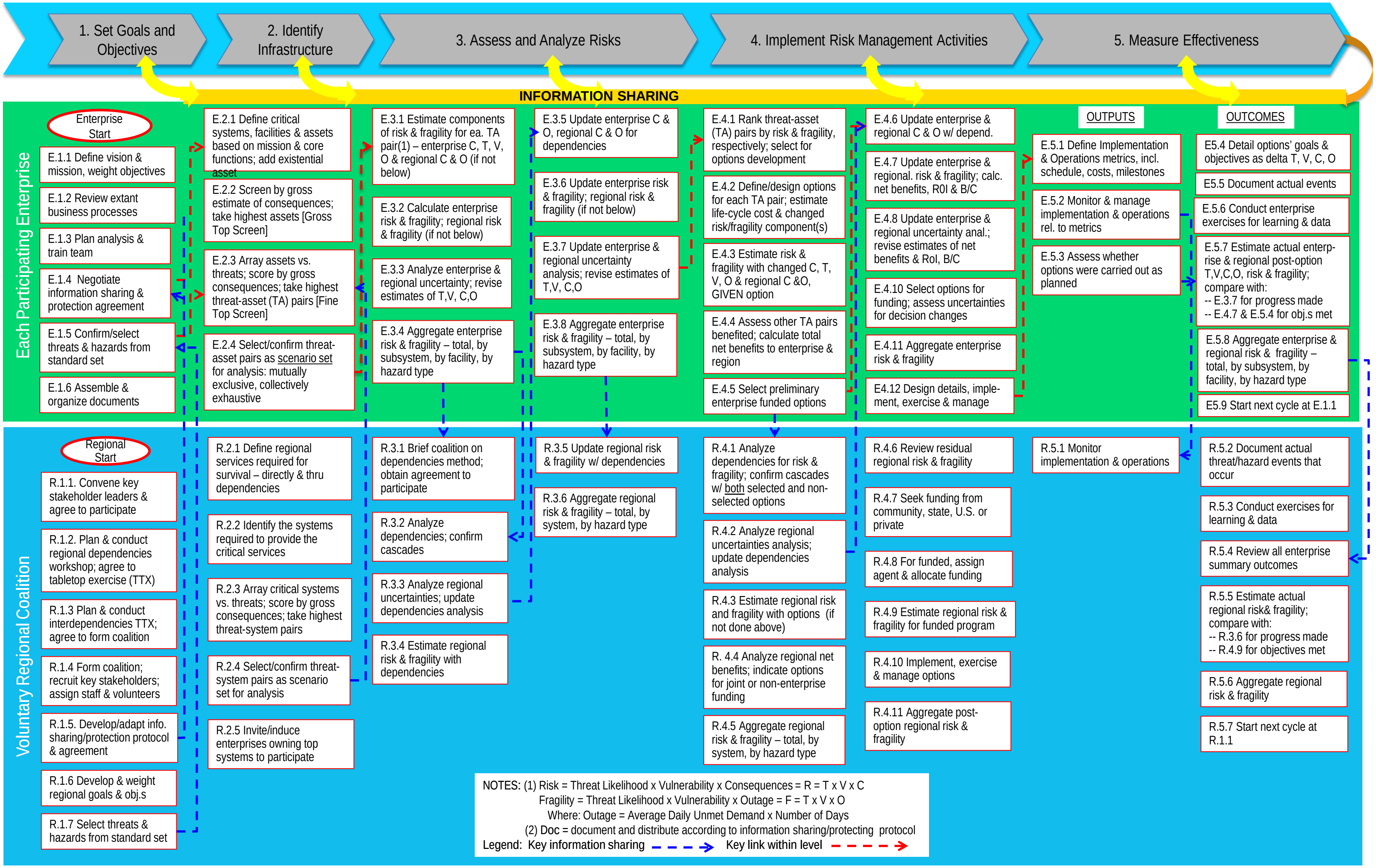
Notes: (1) AWWA J100-10 was the risk tool used in the Nashville Feasibility Pilot.

(2) Common Risk Model for Dams addresses human malevolent threats only. It is a conditional risk method applied in two different ways. For a single dam, threat likelihood is set to 1.0 for all scenarios, but if the analysis is for a set of dams, the likelihood of thre advesary selecting any particular dam is is estimated based on its asumed relative attractiveness based on Likelihood of Success (Vulnerabiity) and Consequences. The assumptioon is also that at least one dam will; be attacked, so the calculated risk is still conditional, but incorporating adversary choice moves it one step closer to full risk.

(3) DOE's State Energy Assessment Initiative is more a meta-analysis of needs & requirements.

(4) VAST is designed to be used with Vulnerability Assessment Framework.

Attachment 2. NIPP 2013 Critical Infrastructure Risk Management Framework and the CISR Risk Management Process



1. Set Goals and Objectives

2. Identify Infrastructure

3. Assess and Analyze Risks

4. Implement Risk Management Activities

5. Measure Effectiveness

INFORMATION SHARING

Each Participating Enterprise

Enterprise Start

E.1.1 Define vision & mission, weight objectives

E.1.2 Review extant business processes

E.1.3 Plan analysis & train team

E.1.4 Negotiate information sharing & protection agreement

E.1.5 Confirm/select threats & hazards from standard set

E.1.6 Assemble & organize documents

E.2.1 Define critical systems, facilities & assets based on mission & core functions; add existential asset

E.2.2 Screen by gross estimate of consequences; take highest assets [Gross Top Screen]

E.2.3 Array assets vs. threats; score by gross consequences; take highest threat-asset (TA) pairs [Fine Top Screen]

E.2.4 Select/confirm threat-asset pairs as scenario set for analysis: mutually exclusive, collectively exhaustive

E.3.1 Estimate components of risk & fragility for ea. TA pair(1) – enterprise C, T, V, O & regional C & O (if not below)

E.3.2 Calculate enterprise risk & fragility; regional risk & fragility (if not below)

E.3.3 Analyze enterprise & regional uncertainty; revise estimates of T,V, C,O

E.3.4 Aggregate enterprise risk & fragility – total, by subsystem, by facility, by hazard type

E.3.5 Update enterprise C & O, regional C & O for dependencies

E.3.6 Update enterprise risk & fragility; regional risk & fragility (if not below)

E.3.7 Update enterprise & regional uncertainty analysis; revise estimates of T,V, C,O

E.3.8 Aggregate enterprise risk & fragility – total, by subsystem, by facility, by hazard type

E.4.1 Rank threat-asset (TA) pairs by risk & fragility, respectively; select for options development

E.4.2 Define/design options for each TA pair; estimate life-cycle cost & changed risk/fragility component(s)

E.4.3 Estimate risk & fragility with changed C, T, V, O & regional C &O, GIVEN option

E.4.4 Assess other TA pairs benefited; calculate total net benefits to enterprise & region

E.4.5 Select preliminary enterprise funded options

E.4.6 Update enterprise & regional C & O w/ depend.

E.4.7 Update enterprise & regional. risk & fragility; calc. net benefits, R0I & B/C

E.4.8 Update enterprise & regional uncertainty anal.; revise estimates of net benefits & RoI, B/C

E.4.10 Select options for funding; assess uncertainties for decision changes

E.4.11 Aggregate enterprise risk & fragility

E4.12 Design details, implement, exercise & manage

OUTPUTS

E.5.1 Define Implementation & Operations metrics, incl. schedule, costs, milestones

E.5.2 Monitor & manage implementation & operations rel. to metrics

E.5.3 Assess whether options were carried out as planned

OUTCOMES

E5.4 Detail options' goals & objectives as delta T, V, C, O

E5.5 Document actual events

E.5.6 Conduct enterprise exercises for learning & data

E.5.7 Estimate actual enterprise & regional post-option T,V,C,O, risk & fragility; compare with:
-- E.3.7 for progress made
-- E.4.7 & E.5.4 for obj.s met

E.5.8 Aggregate enterprise & regional risk & fragility – total, by subsystem, by facility, by hazard type

E5.9 Start next cycle at E.1.1

Voluntary Regional Coalition

Regional Start

R.1.1. Convene key stakeholder leaders & agree to participate

R.1.2. Plan & conduct regional dependencies workshop; agree to tabletop exercise (TTX)

R.1.3 Plan & conduct interdependencies TTX; agree to form coalition

R.1.4 Form coalition; recruit key stakeholders; assign staff & volunteers

R.1.5. Develop/adapt info. sharing/protection protocol & agreement

R.1.6 Develop & weight regional goals & obj.s

R.1.7 Select threats & hazards from standard set

R.2.1 Define regional services required for survival – directly & thru dependencies

R.2.2 Identify the systems required to provide the critical services

R.2.3 Array critical systems vs. threats; score by gross consequences; take highest threat-system pairs

R.2.4 Select/confirm threat-system pairs as scenario set for analysis

R.2.5 Invite/induce enterprises owning top systems to participate

R.3.1 Brief coalition on dependencies method; obtain agreement to participate

R.3.2 Analyze dependencies; confirm cascades

R.3.3 Analyze regional uncertainties; update dependencies analysis

R.3.4 Estimate regional risk & fragility with dependencies

R.3.5 Update regional risk & fragility w/ dependencies

R.3.6 Aggregate regional risk & fragility – total, by system, by hazard type

R.4.1 Analyze dependencies for risk & fragility; confirm cascades w/ both selected and non-selected options

R.4.2 Analyze regional uncertainties analysis; update dependencies analysis

R.4.3 Estimate regional risk and fragility with options (if not done above)

R. 4.4 Analyze regional net benefits; indicate options for joint or non-enterprise funding

R.4.5 Aggregate regional risk & fragility – total, by system, by hazard type

R.4.6 Review residual regional risk & fragility

R.4.7 Seek funding from community, state, U.S. or private

R.4.8 For funded, assign agent & allocate funding

R.4.9 Estimate regional risk & fragility for funded program

R.4.10 Implement, exercise & manage options

R.4.11 Aggregate post-option regional risk & fragility

R.5.1 Monitor implementation & operations

R.5.2 Document actual threat/hazard events that occur

R.5.3 Conduct exercises for learning & data

R.5.4 Review all enterprise summary outcomes

R.5.5 Estimate actual regional risk& fragility; compare with:
-- R.3.6 for progress made
-- R.4.9 for objectives met

R.5.6 Aggregate regional risk & fragility

R.5.7 Start next cycle at R.1.1

NOTES: (1) Risk = Threat Likelihood x Vulnerability x Consequences = R = T x V x C
Fragility = Threat Likelihood x Vulnerability x Outage = F = T x V x O
Where: Outage = Average Daily Unmet Demand x Number of Days
(2) Doc = document and distribute according to information sharing/protecting protocol
Legend: Key information sharing - - - → Key link within level - - - →

Bibliography

Amram, M. and Kulatilaka, 1999. *Real Options: Managing Strategic Investment in an Uncertain World*, Harvard Business School Press, Boston, MA.

Anderson, C.W., J.R. Santos, and Y.Y. Haimes. 2007. “A risk-based input-output methodology for measuring the effects of the August 2003 Northeast Blackout.” *Economic Systems Research*, 19(2): 183-204.

ANSI/ASME-ITI/AWWA. 2010. J100-10 Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems, an American National Standard, AWWA, Denver, CO.

Approach, Springfield, IL: Charles C. Thomas, 2006, pp. 226-48.

ASME-ITI. 2004. *Risk Analysis and Management for Critical Asset Protection: General Guidance*, ASME, New York, NY.

ASME-ITI. 2005a. *Introduction to Risk Analysis and Management for Critical Asset Protection*, ASME, New York, NY.

ASME-ITI. 2005b. *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Applied to Terrorism and Homeland Security*, ASME, New York, NY.

ASME-ITI. 2005c. *Sector-Specific Guidance: Nuclear Power Plants*, ASME, New York, NY.

ASME-ITI. 2005d. *Sector-Specific Guidance: Nuclear Spent Fuel Transportation and Storage*, ASME, New York, NY.

ASME-ITI. 2005e. *Sector-Specific Guidance: Petroleum Refinin*g, ASME, New York, NY.

ASME-ITI. 2005f. *Sector-Specific Guidance: Chemical Manufacturing*, ASME, New York, NY.

ASME-ITI. 2005g. *Sector-Specific Guidance: Liquefied Natural Gas Off-Loading Ports*, ASME, New York, NY.

ASME-ITI. 2006. *The RAMCAP Framework©, Version 2.0*, ASME, New York, NY.

ASME-ITI. 2007a. *Sector-Specific Guidance: Dams and Navigational Locks*, ASME, New York, NY.

ASME-ITI. 2007b. *Sector-Specific Guidance: Water and Wastewater Systems*, ASME, New York, NY.

ASME-ITI. 2009. *All-Hazards Risk and Resilience: Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach*, ASME, New York, NY.

ASME-ITI/ANSI. 2010. *Higher Education Risk to Natural and Manmade Hazards. An American National Standard*, ASME, New York, NY.

Ayyub, B.M., 2003. *Risk Analysis in Engineering and Economics*, Chapman& Hall/CR, Boca Raton, FL.

Barker, K.A., Santos, J.R. 2010. “Measuring the efficacy of inventory with a dynamic input–output model.” *International Journal of Production Economics*, 126(1): 130-143

Bell, D.E., Keeney, R.L., and Raiffa, H. 1977 (eds.), *Conflicting Objectives in Decisions*, Wiley, New York, NY.

Bernstein, P. L. 1998. *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons, New York.

BICE. 2009. *Sustainable Critical Infrastructure Systems – a Framework for Meeting 21st Century Imperatives. Board on Infrastructure and the Constructed Environment*, Division on Engineering and Physical Sciences, U.S. National Academy of Sciences, National Academies Press, Washington, DC.

Bier, V.M., 2005. "Game-Theoretic and Reliability Methods in Counter-Terrorism and Security," *Modern Statistical and Mathematical Methods in Reliability, Series on Quality, Reliability and Engineering Statistics*, World Scientific Publishing Co.

Bier, V.M., and Azaiez, M.N., 2009 (editors). *Game Theoretic Risk Analysis of Security Threats, International Series in Operations Research and Management Science*, Springer, New York, 2009.

Brashear, J.P., 2009. *Optimizing Infrastructure Investments for the 21st Century*, ASME Innovative Technologies Institute, LLC, Washington, DC.

Brashear, J.P., 2010. “The Risk Analysis and Management for Critical Asset Protection,” a chapter in John G. Voeller (ed.), *Wiley Handbook of Science and Technology for Homeland Security*, Wiley, Hoboken, NJ.

Brashear, J.P., *et al*., 2011. *Regional Resilience/Security Analysis Process for the Nation's Critical Infrastructure Systems*, ASME, New York, NY.

Brealey, R. and Myers, S. 2000. *Principles of Corporate Finance. Sixth Edition*, Boston, MA, Irwin McGraw-Hill.

Brigham, E., L. Gapenski and M. Ehrhardt. 1999. *Financial Management: Theory and Practice. Ninth Edition*, The Dryden Press, Fort Worth, TX.

Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, http://create.usc.edu/ (contains terrorism risk analysis papers from various CREATE symposia).

Corbett, John. Ian McHarg. 2001. Overlay Maps and the Evaluation of Social and Environmental Costs of Land Use Change. http://www.csiss.org/classics/content/23.

Cox, L.A., 2008a.”What's Wrong with Risk Matrices?” *Risk Analysis*, 28(2).

Cox, L.A., 2008b. “Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks,” *Risk Analysis*, 28 (6).

Crowther, K.G., Y.Y. Haimes, G. Taub. 2007. “Systemic Valuation of Strategic Preparedness with Illustrations from Hurricane Katrina.” *Risk Analysis*, 27(5): 1345–1364.

CSIS. 2006. *Guiding Principles for Strengthening America’s Infrastructure.* Center for Strategic and International Studies, Commission on Public Infrastructure.

De la Barra T. 1995. *Integrated Land Use and Transport Modeling: Decision Chains and Hierarchies*. Cambridge University Press, New York, NY.

Decision Lens 2009. *Analytic Hierarchy Process*. http://www.decisionlens.com/products/process/.

Dietzenbacher E. and M.L. Lahr. *Wassily Leontief and Input-Output Economics*, Cambridge University Press, Cambridge, UK, 2004.

Dyer, J. S. 1990. “Remarks on the analytic hierarchy process.” *Management Science*, 36(3) 249-258.

Forman, E.H. and S.I. Gass. “The analytical hierarchy process – an exposition.” *Operations Research* 49.4 (July-August 2001): 469(18)

Forman, E.H. and Selly, M.A., 2001. *Decision by Objectives: How to Convince Others That You Are Right*, World Scientific, River Edge, NJ.

Forrester, Jay W. 1961. *Industrial Dynamics*. Pegasus Communications. ISBN 1883823366.

Forrester, Jay W. 1969. *Urban Dynamics*. Pegasus Communications. ISBN 1883823390.

Gass, S.I. 2005. “Model World: The Great Debate – MAUT Versus AHP.” *Interfaces*, Vol. 35, No. 4, July-August, pp. 308-312.

Gheorghe, A.V. and Mock, R., *Risk Engineering: Bridging Risk Analysis with Stakeholders Values*, Kluwer Academic Publishers, Dordrecht, Switzerland.

Gheorghe, A.V. and Nicolet-Monnier, M., 1995. *Integrated Regional Assessment of Accidental Releases*, Kluwer Academic Publishers, Dordrecht, Switzerland.

Haggerty, M., J.R. Santos, and Y.Y. Haimes. 2008. “A Transportation-Based Framework for Deriving Perturbations to the Inoperability Input-Output Model,” *Journal of Infrastructure Systems*, 14(4): 293-304.

Haimes, Y.Y. and P. Jiang. 2001. “Leontief-Based Model of Risk in Complex Interconnected Infrastructures.” *Journal of Infrastructure Systems*, 7(1): 1-12.

Haimes, Y.Y., B.M. Horowitz, J.H. Lambert, J.R. Santos, K. Crowther, and C. Lian. 2005. “Inoperability Input-Output Model for Interdependent Infrastructure Sectors,” *Journal of Infrastructure Systems*, 11(2): 67-79.

Hubbard, D.W., 2009. *The Failure of Risk Management: Why It's Broken and How to Fix I*t, Wiley:

Hoboken, N.J.

Hunt, J.D. and D.C. Simmonds. 1993. “Theory and application of an integrated land-use and transport modeling framework.” *Environment and Planning B*, 20: 221–244.

Hutchinson, Harry. 2005. “Calculating Risks: Can the Science that Judges the Safety of Nuclear Plants Secure the Infrastructure of a Nation.” *Mechanical Engineering*.

IEEE Joint Task Force on Quadrennial Energy Review, 2014. *IEEE Report to DOE QER on Priority Issues*, Chapter 4. Asset Management Challenges and Options, Including the Implications and Importance of Aging Infrastructure, pp. 50-66, IEEE: Washington, DC, on June 20, 2015, found at http://smartgrid.ieee.org/images/pdf/ieee_report_to_doe_qer_on_priority_issues.pdf.

Isard, W. 1960. *Methods of Regional Analysis: An Introduction to Regional Science*. MIT Press, Cambridge, MA.

Jordan, M. 2003. “Punctuations and agendas: A new look at local government budget expenditures.” *Journal of Policy Analysis and Management* 22 (3) (June 1): 345-360. doi:10.1002/pam.10136.

Keeney, R.L. and Raiffa, H., 1976. *Decisions with Multiple Objectives: Preferences and Trade-Offs*, Wiley, New York, NY.

Kendrick J. and D. Saaty. 2007. *Use Analytic Hierarchy Process for Project Selection*. Decision Lens Inc., 2007.

Kirkwood, Craig W. 1997. *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets,* Wadsworth Publishing Co., New York.

Kohler, G., 1999. *Risk Assessment and Decision Making in Business and Industry: A Practical Guide*, CRC, Boca Raton, FL.

Kohler, G., 2000. *Risk Modeling for Determining Value and Decision Making*, Chapman & Hall/CRC, Boca Raton, FL.

Kunruether, H. and Rose, A (eds.) 2004. *The Economics of Natural Hazards, Volume I and II,* Edward Elgar Publishing, Northampton, MA.

Leontief, W.W. 1951. “Input-Output Economics.” *Scientific American*, pp. 15-21, October.

Leontief, W.W. 1951. *The Structure of the American Economy, 1919-1939*, Second Edition. Oxford University Press, New York.

Lewis, Ted, 2015. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley: Hoboken, NJ.

Lian C., Santos, J.R., Y. Y. Haimes. 2007. “Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors.” *Risk Analysis* 27(4): 1053-1064.

Lian, C. and Y.Y. Haimes. 2006. “Managing the Risk of Terrorism to Interdependent Infrastructure Systems Through the Dynamic Inoperability Input-Output Model.” *Systems Engineering*, 9(3): 241-258.

LMSRA. 2009. Building America’s Future National Survey of Registered Voters. Luntz Maslansky Strategic Research Analysis.

Luce, R.D., H. Raiffa. 1957. *Games and Decisions*, John Wiley and Sons, New York.

Markowitz, H. M. 1952. “Portfolio Selection.” *J. Finance* 7 (1): pp. 77-91.

Markowitz, H.M., 1959. *Portfolio Selection: Efficient Diversification of Investments.* Wiley: New York, NY, reprinted by Yale University Press, 1970, New Haven, CT.

McCarthy, J. A., and Brashear, J.P., 2005. *Critical Infrastructure Protection in the National Capital Region: Risk-Based Foundations for Resilience and Sustainability,* University Consortium for Infrastructure Protection, Critical Infrastructure Program, George Mason University School of Law, Arlington, VA.

Miller R.E. and P.D. Blair, 2009. *Input-output Analysis: Foundations and Extensions*, 2nd ed. University Press, Cambridge, UK.

Morgenstern, O. and Von-Neumann, J. 1944. *Theory of Games and Economic Behavior*. Princeton University Press.

Moteff, John. September 2, 2004. “Risk Management and Critical Infrastructure Protection: Assessing, Integrating and Managing Threats, Vulnerabilities, and Consequences,” Congressional Research Service, Library of Congress (order code RL32561).

Multihazard Mitigation Council. December 2005. *Natural Hazard Mitigation Saves: Independent Study to Assess the Future Benefits of Hazard Mitigation Activities, Volume 2 - Study Documentation.* Prepared for the Federal Emergency Management Agency of the U.S. Department of Homeland Security by the Applied Technology Council under contract to the Multihazard Mitigation Council of the National Institute of Building Sciences, Washington, D.C.

NASBO. 1999. *Capital Budgeting in the States*. National Association of State Budget Officers.

National Cooperative Highway Research Program (NCHRP), 2001. *Report 456: Guidebook for Assessing the Social and Economic Effects of Transportation Projects*. National Academies Press, Washington, DC.

National Institute of Standards and Technology, in preparation. *Community Resilience Planning Guide,* U.S. Department of Commerce, Washington, DC.

National Research Council. 2002. “Making the Nation Safer: The Role of Science and Technology in Countering Terrorism,” The National Academic Press, Washington, D.C.

National Research Council. 2010. *Review of the Department of Homeland Security’s Approach to Risk Analysis*, John F. Ahearne, Chair, National Academies Press, Washington, DC.

Newendorp, P.D., 1996. D*ecision Analysis for Petroleum Exploration*, Planning Press, Aurora, CO.

Novosel, D., et al., *IEEE Report to DOE QER on Priority Issues*, IEEE Joint Task Force on Quadrennial Energy Review, Washington, September 5, 2014.

Okuyama, Y. and Chang, S.E. (eds.), 2004. *Modeling Spatial and Economic Impacts of Disasters.* Springer, Berlin, Germany.

Perrings, C. 2001. “Resilience and Sustainability.” In H. Folmer, H. L. Gabel, S. Gerking, A. Rose (Eds.), *Frontiers of Environmental Economics*. Cheltenham, pp. 319–41. U.K.: Edward Elgar.

Raiffa, H., 1970. *Decision Analysis: Introductory Lectures on Choices under Uncertainty*, Addison-Wesley, Reading, MA.

Resurreccion, J.Z. and Santos, J.R., 2011. “Developing an Inventory-Based Prioritization Methodology for Assessing Inoperability and Economic Loss in Interdependent Sectors,” *IEEE Proceedings of Systems and Information Engineering Design Symposium*, pp. 176-181.

Rose, A. 2004. “Economic Principles, Issues, and Research Priorities in Natural Hazard Loss Estimation” in Okuyama Y. and Chang S. (eds.), *Modeling the Spatial Economic Impacts of Natural Hazards*, Heidelberg: Springer, 2004, pp.13-36.

Rose, A. 2006. “Economic Resilience to Disasters: Toward a Consistent and Comprehensive Formulation,” in Paton D. and Johnston D. (eds.), *Disaster Resilience: An Integrated Approach*, Springfield, IL: Charles C. Thomas, 2006, pp. 226-48.

Rose, A. and Liao, S., 2005. “Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions,” *Journal of Regional Science,* Vol. 45, No. 1, 2005, pp. 75-112

Saaty, T. L. 1980. *The Analytic Hierarchy Process,* McGraw-Hill Book Co., New York.

Saaty, T.L. and Alexander J. 1989. *Conflict Resolution: The Analytic Hierarchy Approach*, Praeger, New York.

Saaty, T.L. and Vargas, L. 1982. *The Logic of Priorities: Applications in Business, Energy, Health and Transportation*, Kluwer-Nijhoff Publishing, Boston.

Saaty, T.L., 1988. *Decision Making for Leaders: An Analytical Hierarchy Process for Decisions in a Complex World*, RWS Publications, Pittsburgh, PA.

Santos, J. R., 2008. “Inoperability Input-Output Model (IIM) with Multiple Probabilistic Sector Inputs,” *Journal of Industrial Management and Optimization*, 4(3): 489-510.

Santos, J.R. and Haimes, Y.Y., 2004. “Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures,” *Risk Analysis* 24(6): 1437-1451.

Santos, J.R., 2006. “Inoperability Input-Output Modeling of Disruptions to Interdependent Economic Systems.” *Systems Engineering*, 9(1): 20-34.

Santos, J.R., K. Barker, and P. Zelinke, 2008. “Sequential Decision-making in Interdependent Sectors with Multiobjective Inoperability Decision Trees,” *Economic Systems Research*, 20(1): 29-56.

Santos, J.R., Y. Y. Haimes, and C. Lian, 2007. “A Framework for Linking Cyber Security Metrics to the Modeling of Macroeconomic Interdependencies,” *Risk Analysis*, 27(4): 1283-1297.

Savage, L.J. 1954. *The Foundations of Statistics*, Wiley: New York.

Savage, S.L. 2003. *Decision Making with Insight*, Brooks/Cole-Thomson Learning, Belmont, CA.

Savage, S.L., 2009. *The Flaw of Averages*, Wiley: Hoboken, NJ.

Simon, Herbert, 1957. "A Behavioral Model of Rational Choice", in *Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting*. New York: Wiley.

Snowden, D. 2002. “Complex acts of knowing: paradox and descriptive self-awareness.” *Journal of Knowledge Managemen*t 6 (2): 100–111.

Springer, D., and G. Dierkers. 2009. *An Infrastructure Vision for the 21st Century: Strengthening our Infrastructure for a Sustainable Future*. National Governors Association.

Stevens, S. S., 1946. “On the Theory of Scales of Measurement,” *Science*, June 7, Vol.103, No. 2684: 677–680.

Steyaert, Patrick, and Janice Jiggins. 2007. “Governance of complex environmental situations through social learning: a synthesis of SLIM’s lessons for research, policy and practice.” *Environmental Science & Policy* 10 (6) (October): 575-586. doi:10.1016/j.envsci.2007.01.011.

The Infrastructure Security Partnership (TISP), 2006 and 2011. *Regional Disaster Resilience: A guide for developing an action plan.* American Society of Civil Engineers, Reston, VA; updated and expanded in 2011, available from TISP, Society of American Military Engineers, Alexandria, VA.

Tyler, C., and J. Willand. 1997. “Public budgeting in America: A twentieth century retrospective.” *Public Budgeting and Financial Management*, 9: 31.

U.S. Department of Commerce, 1997. *Regional Multipliers: A User Handbook for the Regional Input-Output Modeling System*, Washington, DC: U.S. Government Printing Office.

U.S. Department of Commerce, 2006. National Institute of Standards and Technology. *Ninth Annual Report on Federal Agency Use of Voluntary Consensus Standards and Conformity Assessment*. Washington, D.C.: Government Printing Office.

U.S. Department of Homeland Security, 2003a. *Homeland Security Presidential Directive-5: Management of Domestic Incidents*. Available online: <http://www.fas.org/irp/offdocs/nspd/hspd-5.html>

U.S. Department of Homeland Security, 2003b. *Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection*. Available online: <http://www.fas.org/irp/offdocs/nspd/hspd-7.html>

U. S. Department of Homeland Security, 2004. “DHS Interim Rule on Procedures Associated with Sharing and Handling of Information Designated as Critical Infrastructure Information.” *Federal Register*, Vol. 69, No. 34, pp. 8074-8089.

U.S. Department of Homeland Security, 2006. *National Infrastructure Protection Plan*, Washington, DC.

U.S. Department of Homeland Security, 2008. *National Response Framework (NRF)*. Available online: <http://www.fema.gov/NRF>

U.S. Department of Homeland Security, 2009. *National Infrastructure Protection Plan (NIPP)*, Washington, DC. Available online: <http://www.dhs.gov/files/programs/editorial_0827.shtm>

U.S. Department of Homeland Security, 2010. *DHS Risk Lexicon*, 2010 Edition.

U.S. Department of Homeland Security, 2011. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, Washington, DC.

U.S. Department of Homeland Security, 2013a. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,* Washington, DC.

U.S. Department of Homeland Security, 2013b. *NIPP Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*, Washington, DC.

U.S. Department of Transportation, 2003. U.S. Department of Transportation, "Revised Departmental Guidance Valuation of Travel Time in Economic Analysis," signed 2-11-03.

U.S. Department of Transportation, 2011. Trottenberg and Rivkin, *Economic Value of a Statistical Life*, Washington, DC.

U.S. Environmental Protection Agency, 2000. *Guidelines for Preparing Economic Analyses*. EPA 240-R-00-003.

U.S. Environmental Protection Agency, 2004. *Risk Management Plan (RMP) COMPTM*. www.epa.gov/emergencies/rmp.

U.S. Environmental Protection Agency, 2010. *Valuing Mortality Risk Reductions for Environmental Policy: A White Paper (Draft)*. National Center for Environmental Economics.

U.S. Government Accountability Office, 2001. *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T.Washington, DC, October 12.

U.S. General Accountability Office, 2015. *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, GAO-14-507, Washington, DC, September 17.

U.S. Office of Management and Budget (OMB), 2003. *OMB Circular No. A-4*, "Regulatory Analysis."

U.S. Presidential Executive Order (EO) 13010: *Establishing the President's Commission on Critical Infrastructure Protection (PCCIP)*, July 15, 1996. Available online: <http://www.fas.org/irp/offdocs eo13010.htm>

U.S. Presidential Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity*, February 12, 2013. Available online: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

U.S. Presidential Policy Directive/PPD-8: *National Preparedness*, March 30, 2011.Washington, DC.

U.S. Presidential Policy Directive/PPD-21: *Critical Infrastructure Security and Resilience*, February 12, 2013.Washington, DC.

ULI. 2009. *Infrastructure 2009: Pivot Point*. The Urban Land Institute and Ernst & Young, Washington, DC.

US Census Bureau, 2007. *Journey to Work and Place of Work*. Available Online: <http://www.census.gov/population/www/socdemo/journey.html>

Wallenius et al., 2008. "Multiple Criteria Decision Making and Multi-attribute Utility Theory," *Management Science* 54(7), pp. 1336–1349.

Willis, H.H., LaTourette, T., Kelly, T.R., Hickey, S. and Neill, S. (2007). *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, RAND Corporation, Santa Monica, CA 2007.

Appendix A.
Acronyms

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers (ASME)
AWWA J100	American Water Works Association Standard J100
B/C	Benefit/cost
BASE	Baseline Assessment for Security Enhancement for mass transit
CAPTA	Costing Asset Protections for Transportation Agencies (CAPTA, DoT)
CI	Critical Infrastructure
CISR	Critical Infrastructure Security and Resilience
CISR-RMP	Critical Infrastructure Security and Resilience-Risk Management Process
CRM-D	Common Risk Model – Dams
DHS	Department of Homeland Security
DSAT	Dams Sector Analysis Tool
EPA	Environmental Protection Agency
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
GAO	Government Accountability Office
IP	Office of Infrastructure Protection
IST	Infrastructure Survey Tool (IP)
MAP-21	*The Moving Ahead for Progress in the 21st Century Act*
MIST	Modified IST (FPS)
MSRAM	Maritime Security Risk Analysis Method (USCG)
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OMB	Office of Management and Budget
PPD-21	Presidential Policy Directive/ PPD-21: Critical Infrastructure Security and Resilience
PPD-8	Presidential Policy Directive/ PPD-8: National Preparedness
PSA	Protective Security Advisor
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RC	Regional Coalition
ROI	Return on investment
S&T	Science and Technology Directorate
THIRA	Threat and Hazard Identification and Risk Assessment
TRB	Transportation Research Board
TSA	Transportation Security Administration
TTA&QA	Training, technical assistance and quality assurance
VAST	Vulnerability Assessment Scoring Tool
VCAT	Voluntary Chemical Assessment Tool
WHEAT	Water Health and Economic Analysis Tool

Appendix B.
NIPP 2009 Core Criteria for Risk Assessments
(NIPP 2009, Appendix 3A, pp. 147-8, verbatim)

The NIPP core criteria for risk assessments identify the characteristics and information needed to produce results that can contribute to cross-sector risk comparisons. This appendix provides information for developing new and modifying existing methodologies so they can be used to support national-level comparative risk assessment, incident response planning, resource prioritization, and protective measures development and implementation. This appendix summarizes the information providedin section 3.3, which can be referenced for additional details on these topics.

Many stakeholders conduct risk assessments to meet their own decisionmaking [sic] needs, using a broad range of methodologies. Whenever possible, DHS seeks to use information from stakeholders' assessments to contribute to an understanding of risks across sectors and regions throughout the Nation. To do this consistently, the challenge of minimizing the disparity in the approaches must be addressed through the core criteria identified below. These criteria include both the analytic principles that are broadly applicable to all parts of a risk methodology and specific guidance regarding the information needed to understand and address each of the three components of the risk equation: consequence, vulnerability, and threat.

The basic analytic principles ensure that risk assessments are:

- **Documented**: The methodology and the assessment must clearly document which information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
- **Reproducible**: The methodology must produce comparable, repeatable results, even though assessments of different CIKR will be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decisionmakers [sic].
- **Defensible**: The risk methodology must be technically sound, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. The uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates must be communicated.
- **Complete**: The methodology must assess consequence, vulnerability, and threat for every defined risk scenario and follow the more specific guidance for each of these as given below.

CORE CRITERIA GUIDANCE FOR CONSEQUENCE ASSESSMENTS

- Document the scenarios assessed, tools used, and any key assumptions made.
- Estimate the number of fatalities, injuries, and illnesses, where applicable and feasible, keeping each separate estimate visible to the user.
- Estimate the economic loss in dollars, stating which costs are included (e.g., property damage losses, lost revenue, loss to the economy) and what duration was considered.

- If monetizing the human health consequences, document the value(s) used and the assumptions made.
- Consider and document any protective or consequence mitigation measures that have their effect after the incident has occurred, such as the rerouting of systems or HAZMAT or fire and rescue response.
- Describe the psychological impacts and mission disruption, where feasible.[22]

CORE CRITERIA GUIDANCE FOR VULNERABILITY ASSESSMENTS

- Identify the vulnerabilities associated with: physical, cyber, or human factors (openness to both insider and outsider threats); critical dependencies; and physical proximity to hazards.
- Describe all protective measures in place and how they reduce the vulnerability for each scenario.
- In evaluating security vulnerabilities, develop estimates of the likelihood of an adversary's success for each attack scenario.
- For natural hazards, estimate the likelihood that an incident would cause harm to the asset, system, or network, given that the natural hazard event occurs at the location of interest for the risk scenario.

CORE CRITERIA GUIDANCE FOR THREAT ASSESSMENTS

- For adversary-specific threat assessments:[23]
  - Account for the adversary's ability to recognize the target and the deterrence value of existing security measures.
  - Identify attack methods that may be employed.
  - Consider the level of capability that an adversary demonstrates with regard to a particular attack method.
  - Consider the degree of the adversary's intent to attack the target.
  - Estimate threat as the likelihood that the adversary would attempt a given attack method against the target.
  - If threat likelihoods cannot be estimated, use conditional risk values (consequence times vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision.
- For natural disasters and accidental hazards:
  - Use best-available analytic tools and historical data to estimate the likelihood that these events would affect CIKR.

In addition to the guidance available in the NIPP, and as resources allow, DHS provides direct assistance to partners who are developing and modifying risk methodologies. To discuss the possibility of such assistance, contact DHS at NIPP@dhs.gov.

[22] The assessment of the psychological impacts and mission disruption are currently maturing capabilities. Mission disruption is an area of strong NIPP partner interestfor collaborative development of the appropriate metrics to help quantify and compare different types of losses. While development is ongoing, qualitative descriptionsof the consequences are a sufficient goal.

[23] Threat information can be received through HSIN.

Appendix C.
User and Stakeholder Considerations, Conditions and Constraints Relevant to CISR-RMP Design

A series of structured interviews with a non-random sample of typical stakeholders from lifeline CIs, local governments and regional P3s was conducted to define the level of use of risk analysis in lifeline infrastructures and local governments and the conditions and constraints under which they operate. The results of these discussions are reported below in three sections. The first addresses individual organizations, the second addresses the constraints on organizing and managing CISR on a regional, collective basis, and the third examines constraints on using risk analysis among interdependent CIs.

C.1. Individual CISR Organizations

The range of capabilities and expertise that directly focus on physical and cyber risks associated with interdependent lifelines and regions is wide. While some very large jurisdictions and utilities have adopted risk management as standard operating procedures, many of these capabilities are unique, proprietary or narrowly threat specific, and cannot be readily integrated. The exception has been water and wastewater utilities, where significant and growing numbers of even mid-sized utilities have begun to conduct risk analysis. (The water sector experience is discussed later.) Outside of these, lifelines and local jurisdictions have actually performed very little risk analysis (and no resilience analysis beyond continuity of operations/continuity of government planning). Interest in and willingness to entertain using such approaches, however, is growing. Many local jurisdictions are largely unaware of what risk analysis is and what it requires. Spare personnel capacity and funds for hiring consultants to undertake substantive analysis are sharply limited. For those organizations that are interested, expert advisors are appreciated in both process and substantive suggestions on risk assessment options, but cost and time remain serious constraints.

The belief is widespread among local agencies and many lifelines operators that if disaster strikes, the federal or state governments will step in to pay for recovery and restoration. Therefore, they doubt the value of investing in prevention, protection or pre-event mitigation. One went so far as to say investing 100% of local taxpayer money before a disaster where the federal government would pay 75% after one would be “irrational.” “There is a huge need to educate and inform elected officials and professionals—they don’t see the payoff,” commented one risk-oriented respondent.

The few assessments or analyses that are being done are essentially sector-specific, with the exception of FEMA’s Threat and Hazard Identification and Risk Analysis (THIRA), which has not been adopted by lifeline infrastructures. In most metropolitan areas, the relevant agencies, e.g., emergency management, public health, public works and the utilities (whether publicly or privately owned), are siloed from one another, with little or no interaction. THIRA is nominally comprehensive, covering all five preparedness mission areas for all hazards, but, so far, is being used only in response and executed largely by emergency managers at the local level—making it stove-piped as well. The FEMA guidance to date has only included 13 of 31 core capabilities that relate to response and early recovery. Those surveyed believed that THIRA is almost exclusively executed by emergency managers. One called it a “good concept” but a “pain… a necessary evil” and suggested it be made “less bureaucratic” and provide more concrete guidance for those using it; others made similar comments, seeing is it as “very basic,” and that

THIRA is almost always used more as compliance with requirements for grants than in broader risk management.

In the few places where THIRA is used for decision support, it is to identify the most severe consequences—and to rank response capability-building actions based on them. The direct threat-capability linkage seems to follow the traditional emergency management approach, so it feels natural to those using it.

Respondents commented:

- "Emergency management training leads to 'belt-and-suspenders' preparedness. Preparing for worst-case event-driven reaction response is substantially easier than analysis-driven proactive action."
- "In addition to acting on the threats with the 'greatest consequence,' some attention is paid to those with "most frequent, repetitive failures, and situations not handled well in the past."
- "Emergency managers focus almost exclusively on contingency planning and preparation for contingencies – virtually all on preparing for post-event actions – and see little or no value in prevention, protection or pre-event mitigation."

Improvements to THIRA suggested by emergency managers included development of a simple, but explicit common methodology to help sort out options and justify selections and flexibility in choices (as opposed to "mandates"), coupled with more information about what capabilities and best practices others are using successfully. Several respondents expressed frustration with the relatively small amount of concrete direction in the THIRA guidelines.

In addition to THIRA, there are extensive, federally sponsored programs and tools that address vulnerability- and risk-related issues. Examples are vulnerability analyses or surveys conducted by Protective Service Advisors and Transportation Security Administration field personnel. Several emergency managers reported that in the words of one, these "are a mixed bag." Some offer a degree of help or insight, but are time consuming and overly prescriptive as to countermeasures that communities should implement. Several respondents expressed the observation summarized by one: "DHS is about checking the boxes, not information sharing or problem-solving."

Certain perceptions that constrain use of risk analysis are widespread. Several CI and local government respondents said that "we have what we need" regarding current risk assessment capabilities. With the exception of a few proactive and enlightened CI operators, lifelines and other CI emergency management and security directors see the risk assessment capabilities used by their organizations as adequate. The emergency management director for a large metropolitan county observed that he is happy with just the FEMA THIRA process.

Currently available lifelines risk analysis methods pose additional constraints. Private sector risk assessment tools may be proprietary and/or difficult to integrate with other systems. Importantly, lifelines and other CI risk assessment approaches focus on damage and disruption of internal assets and seldom take external dependencies and interdependencies into account. CI operators may be unaware of, or, if concerned, lack expertise to address infrastructure dependencies and interdependencies below superficial levels. Cyber and IT systems pose risks that few regard themselves as equipped to handle and some lack appreciation of the impacts of IT and electronic control systems disruptions. This can include disruption of CI operations and damage to physical CI elements after a regional cyber attack. Recent, well-documented hacking of commercial systems has begun to increase awareness of the threat to local government and CIs and to the lack of capabilities to deal with it.

A near universal issue, especially in the private sector, is fear of legal liability and negligence suits associated with conducting risk analyses and then experiencing casualties or damages due to a known risk that was determined to be too low priority to justify attention. Another issue is the costs associated with identifying risk that require substantial investment to mitigate. Respondents believed that some corporate general counsels and city attorneys might resist risk analysis for these reasons.

C.2 CISR Risk Analysis by Lifeline Infrastructures

Overall, respondents from public-sector lifelines—water/wastewater and roads, bridges and tunnels—were very forthcoming in sharing information about their use or non-use of risk analysis. This was much less true of those typically performed by private industry—particularly energy and telecommunications—perhaps based on their being highly regulated and keen to avoid additional regulation. Local emergency managers surveyed, however, generally find them accessible and cooperative on substantive issues around emergency response and recovery in their service areas.

The water sector is a partial exception to the finding that little risk analysis is actually being performed by local CIs help. The Bioterrorism Act of 2002 caused all drinking water systems serving more than 3300 people to conduct vulnerability or risk analyses and submit their results to the U.S. Environmental Protection Agency. This experience established in many utilities an appreciation that risk analysis helped to make the case for needed investments in security and reliability. The American Water Works Association (AWWA), the sole standards development organization for the water utility sector, adapted the water/wastewater method developed by ASME under DHS OIP sponsorship into an American National Standard, ANSI/AWWA J100. Released in 2010, it has sold several hundred copies, and has been designated by DHS under the Safety Act.

Many of the larger and mid-sized water and wastewater utilities have used it or are currently using it. One official of a large regional public water system pointed out that they use the EPA-recommended J-100 for Threat and Vulnerability Assessment for water and that it is quite sufficient. Another major private sector water system stated that he has used RAMCAP (the immediate predecessor to J100[24]) since the mid-2000s for vulnerability assessments and is exploring some new systems. Consistent with ANSI rules, the standard is being updated, with a new version to be released in late 2015. EPA and DHS each automated versions of the standard, as did several engineering companies for their own use and sale. One of these is being offered as open-source software to elicit rapid iteration toward improvements and new features.

Many potential users were aware that different software packages to implement the standard were developed by both DHS and EPA and that there was contention between the agencies and the industry about whether either was fully compliant with the standard and which would be deemed “official.” Some utilities reported that they are waiting for the perceived DHS-EPA disagreement to be resolved and/or the updated version to be released before conducting their own analyses. There has been no announcement by either agency clarifying the issue, but DHS is no longer developing its version while EPA is. In the

[24] Disclosure: One of the authors of this report, Brashear, led the ASME team that developed RAMCAP for water/wastewater systems, the precursor of ANSI/AWWA J100-10. He has been a member of the AWWA J100 Standards Committee since its inception and is currently engaged in updating it as J100-15. Brashear updated the basic RAMCAP methodology, specified it as an element in regional portfolio planning, and used J100-10 in the Nashville Regional Feasibility Pilot, discussed later in this report.

meantime, engineering firms built software to support their consulting practices and/or to offer for sale. One of these is offered as open source, so users are provided source code that they may modify.

In the other lifelines, considerable interest in risk analysis and the beginnings of regular use by some of them were reported. The transportation sector may also be experiencing increased interest. The Moving Ahead for Progress in the 21st Century Act (MAP-21) (P.L. 112-141, signed July 6, 2012) sets performance standards and requires a “risk-based asset management plan” that includes capital asset inventories with condition assessments, target improvements relative to performance measures, formal investment prioritization processes (based on risk-reduction and life cycle costs) and progress reporting for highways (including bridges and tunnels) and transit systems. States are encouraged to include all highway infrastructure assets within highway rights-of-way. The rule-making process to implement these requirements is currently on going. States will be required to apply “risk management analysis” to assets relative to threats posed by “current and future environmental conditions, including extreme weather events, climate change, and seismic activity” in the words of the rule-making summary; a ten-year financial plan; investment strategies to improve or preserve assets and an on-going system for measuring and managing the condition of roads and bridges.” At least one state department of transportation has initiated a project to J100 method used in the water sector to this task. A later section of this report describes another method being developed by the National Highway Administration to manage risks associated with climate change.

In electricity, the National American Electric Reliability Corporation is focused on raising and maintaining bulk power reliability – continuity of service at defined quality levels by the major transmission grids. The overall mode is to establish mandatory standards and monitor compliance. Nuclear power plants are subject to regular and continuing probabilistic risk analysis for a variety of hazards, but mostly those that would cause a release of radioactive material or lead to major meltdown. Other power plants and distribution systems typically have robust physical security programs covering both physical and cyber security. Many routinely exercise the detailed models used to plan and/or control their systems’ operations to plan ways of managing the loss of various assets. “N minus one” analyses—simulation of how the systems would adapt to sustain service if major assets were out of service—are routine in many power distribution systems. While such exercises directly address routine resilience, we did not find standardized all-hazards risk analysis among these organizations.

Telecommunications providers are less formal in their approach to risk. They rely on their design engineers and maintenance personnel to identify potentially vulnerable situations involving their primary assets and perform limited, informal benefit/cost analysis to justify investments in risk reduction and resilience enhancement. They rely on “industry best practice standards,” internal company standards and historical experience with equipment failures to identify areas of concern. Telecommunications depends heavily on electricity to operate, so they make extensive use of batteries and emergency generators at their sites to assure reliable function during power outages.

One telecommunications executive predicted any federal initiative to implement risk analysis requirements would be strongly resisted as “sounding like regulation,” but expressed that a sound, voluntary framework advanced through a partnership with state and local government and other private entities would be more favorably received, especially if it provided extensive information sharing.

Additional relevant findings from several individual organizations across the sectors included:

- Virtually all the respondents were keen to better understand their risks and fragilities and to improve their ability to evaluate and justify security and resilience options. We did not encounter complacency, but the complacent might not have been amenable to being interviewed.
- All were acutely aware of their dependencies and interdependencies, especially to power outages, and some have taken steps to reduce this vulnerability with back-up power.
- Urban Area Security Initiative (UASI) grants go through the states to local emergency mangers, and most respondents see them as designated for police and fire departments, virtually without discussion. The Bay Area UASI does provide a few hundred thousand dollars out of a $25+ million dollar annual grant budget to a small number of regional resilience projects focusing on lifelines interdependencies and logistic and regional catastrophic disaster planning.
- Most infrastructure managers we spoke with were sensitive to the essential role played by their service in the community. Several indicated that it is crucial to address the economic impacts on the community as part of the risk analysis, "especially when there's not enough return on investment to make the business case using impacts to the utility only," as one local utility official said.
- Several public sector owners spontaneously raised the issue of balancing risk reduction –usually seen as mitigating consequences and reducing the costs of recovery—and maintaining or restoring service rapidly to the customers, a concrete version of the dual NIPP objectives of security and resilience.
- Resilience is for the most part equated to continuity of business, continuity of operations planning or continuity of government and dealt with by continuity plans and exercises. In some major metropolitan areas, however, public health officials and non-profits engaged in preparedness for community groups and at-risk individuals are focusing on community resilience with regional lifelines and other service providers. Across the nation, numerous utilities and service providers are incorporating resilience into their own continuity planning and are beginning to join with other organizations and associations focusing on community and regional resilience.
- Although local emergency managers often involve infrastructure operators in their exercises and in disaster planning, local government exercises seldom include private businesses or industry.
- Councils of Governments are universally seen as useful conveners of local elected officials or city managers, but typically lack authorities and are generally kept relatively weak by their local government members.
- Local government emergency responders seem generally pleased with the help provided by DHS/IP Protective Security Advisors (PSAs), but say that the quality varies considerably. None said he or she received specifically risk analysis assistance from PSAs, and several were skeptical that the surveys offered were effective in dealing with risk or deciding what to do about it.
- Several owners suggested linking the new method directly with on-going local processes such as asset management and/or economic and community development, and later integrating them to increase the likelihood that the methods would be sustained over time and potentially lead to savings in the costs of the analysis efforts.

- Many respondents mentioned the need to find a way to measure security (risk) and resilience (fragility) in ways that can be reported to price-setting boards, local governments, customers, the general public and state and national agencies, especially those that provide grants.
- Most CI owners had not thought about whether risk and resilience tools should be comparable across sectors, but those who had thought about it expressed the view that comparability would have many advantages, including better educating elected officials and their budget staffs, rate-setting bodies and the general public. Especially with larger investments in long-term security and resilience, selling risk reduction and resilience enhancements to these groups is necessary for the investments to be made.
- Respondents expressed significant concern about the locally pressing aspects of climate change. Along both coasts and the Gulf Coast, the concern is coastal storm surge and sea-level rise associated with increasingly intense storms; in the mid-west and south the issues are severe ice storms and snow in winter, leading to major flooding with spring snow melt, and tornadoes and derechos in summer; much of the west is experiencing extreme drought. Virtually of them are seeking solutions, but the idea of risk analysis and option valuation is seldom seen as part of that search.

In brief, interest is serious and widespread in adopting effective, comprehensive CISR risk management processes if they are simple enough for user organizations to conduct, understand and use, especially information that investment-proposal level executives can use to justify CISR improvement recommendations, with some conditions. These conditions include that the process should be:

- Be proposed and provided by an external authority such as a recognized industry standard; a local standard adopted by CIs and governments, collectively; or a federally encouraged voluntary program, especially one associated with grant-making;
- Be easy-to-use, low-cost or free, readily available open system that can be iteratively improved over time based on user suggestions based on experience with it;
- Provide immediate and obvious value to the CI owner and local governments to gain access, personnel time and, ultimately effective investments in improving CISR;
- Be conducted by employees of the organization, perhaps with outside training, technical assistance or advisory services; local managers should be able to obtain answers from their own trusted people for the results to be used;
- Maintain a favorable balance between the time and resources invested by the user organizations and the value produced in the eyes of its decision-makers;
- Emphasize that a common process is an alternative to regulation or mandated “one-size-fits-all” solutions—and would result in better, tailored and more locally effective programs that advance users’ own and national goals;
- Include no-cost technical assistance from locally based federal employees (possibly those with extant local relationships) trained in depth in the CISR risk management methodology to make it easier to sell and easier to carry out;
- Resolve issues of legal liability in advance for risks analyzed, then accepted in an orderly, rational analysis-based trade-off process; and

- Critically, address dependencies and interdependencies with adequate but fully protected information sharing.

C.3 Constraints on Interdependencies Analysis and Integrated Regional CISR Solutions

Infrastructure dependencies and interdependencies require that most, if not all, security and resilience challenges address dependencies and interdependencies among CIs and local governments in a regional analytic approach. This, in turn, requires cross-sector, multi-jurisdiction, and multi-discipline information sharing and protection.

Challenges remain in projecting damage to interdependent lifelines and consequent impacts to all assets, the economy, and environment. For example, in the Bay Area, many of the region's utilities and transportation assets cross or are located near earthquake fault lines and subject to potential flooding from storm surge, sea-level rise, and winter storms. In the recent South Napa 6.0 magnitude earthquake, there were widespread water pipeline breaks with unexpected additional new breaks occurring as the system was re-pressurized and service restored. Water and fuel distribution pipelines, electric power, communications lines and roads are often co-located, so several can be damaged in the same event. Water and wastewater systems depend on electricity to operate, but power distribution requires water for cooling of control system computers and control centers. All infrastructures depend on transportation to allow employees to report to work and for repair crews to access damage sites. Very few vehicles move unless debris is cleared, broken culvers are bridged and fuel is available. Communications companies increasingly rely on battery backup for cell towers and mobile units to deliver emergency generators to where they are needed, requiring fuel and cleared roads. And so forth, and so on.

Local jurisdictions have begun to take steps to coordinate more closely with one another and to engage with state, federal and private sector partners. At the same time, local government agencies remain largely isolated from lifelines and other CIs. In most major metropolitan regions, jurisdictions and agencies (e.g., public health and emergency management) remain largely siloed, exercise within these silos, and do not include CIs in their risk and resilience assessment activities. For example, the August 2014 South Napa Earthquake revealed that City of Napa officials lacked contact information to connect with regional utilities other than PG&E. While preparedness gaps have been or are being addressed across the country, many of the more crucial shortfalls identified recently in exercises and incidents remain. It is not uncommon to have CI and local government representatives complain that the exercises and workshops they attend identify the same lessons learned over and over again.

After the San Bruno gas explosion in September 2010, PG&E began a concerted effort in the San Francisco Bay Area to meet with the region's several counties and solicit information on county-owned critical assets for early restoration in a power disruption event. Two-way sharing of information on key assets, however, is extremely rare. Some larger cities and counties have developed GIS-based mapping of public critical assets, but commonly do not share information on key assets with local offices—or each other.

During and immediately after a major disaster, scarce resources (e.g., mutual aid personnel, fuel, equipment, materials, supplies, etc.) needed for response, recovery and restoration must be prioritized, allocated and distributed, requiring near real-time, regional scale modeling, decision-making and coordination. While acknowledged, these needs remain largely unaddressed.

Inconsistent modeling and analysis techniques across CIs and local agencies pose another constraint on exchanging information, producing validated results, and agreeing on joint actions or coordinating joint programs. Harmonization of state, local, and lifelines risk assessment capabilities is necessary, especially in threat, impact and interdependencies modeling. An example is federal flood inundation models currently being used in different climate change adaptation studies across the country. FEMA and the U.S. Corps of Engineers are addressing the issue with federal partners and other stakeholders.

Currently available models are unable to project cascading consequences**.** While the National Laboratories have spent more than a decade and hundreds of millions of dollars on modeling these, they have taken their mission to be support for national policy making and emergency decision-making at the national level. Their approach relies on significant amounts of sensitive data, some of it very difficult to obtain, and sophisticated models designed solely for federal use and run only on supercomputers. No one has yet devolved these into user-friendly "reduced form" models that would be appropriate for use by local governments, lifeline CIs or metropolitan P3s.

Information sharing constraints pose issues for all substantive regional collaboration, as reported by respondents from all the lifelines, especially those that are privately owned. Procedures are lacking for sharing and protecting specifically needed but sensitive information needed for interdependencies analysis. Procedures for multi-stakeholder information sharing exist. For example, the Puget Sound Region of Washington State has a set of procedures developed by the Pacific Northwest Region and the Washington State Fusion Center. Future information sharing will require clear protocols defining what may be shared, what information security will be applied by all recipients, penalties for disclosure, and treatment of legal liability for information breaches leading to damages or losses, both in a major event and during routine times.

Financial and investment considerations also impede open and full regional collaboration. Regional risk assessments require the participation and commitment of multiple service providers and jurisdictions – which is challenging to motivate and secure. Utilities must in certain cases request and justify funds or rate increases to support upgrades through Public Utilities Commissions, which may be reluctant to provide support. Local governments may lack staff and resources—or interest. It may be challenging to find ways and mechanisms to integrate public and private funds for such assessments or identified mitigation measures. Particularly local government agencies may not wish to participate in a risk assessment that would "commit" them to expend resources they lack.

This review of the situation and constraints suggests that it would be beneficial for federal sponsorship and collaborative activities with CI and state and local organizations to develop risk and resilience analysis capabilities and pilot projects to evaluate, refine and validate these capabilities. THIRAs are being prepared by every state and major urban area with guidance, training and technical assistance by FEMA. The Protective Service Advisors (PSAs) and TSA inspectors have collaborated with local governments and CIs to perform thousands of assessments using the standardized approaches. These examples demonstrate that local officials and CI managers are responsive to federal offers to collaborate to advance CISR goals.

Appendix D.
A Limited Survey of Federal Processes, Methods and Tools for Risk/Resilience Management at Regional and Local Levels

An essential criterion for risk analysis processes is defensibility—"[it] must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, as well as free from significant errors or omissions" (Supplemental Tool, p. 7). Defensibility is not a prudish academic standard, but the contemporary product of decades of research in economics, business, finance, operations research and engineering to determine how best to make resource allocation decisions under uncertainty and constraints that maximize the benefits sought, in this case risk and fragility reduction. This is how these disciplines define rationality. Variations from these disciplinary norms can distort decision-making in ways that interfere with achieving the maximum benefits. Variations can be made (some are in this project's process design), but only with sound reasons, clear explanations and sensitivity to the direction and magnitude by which they may distort decision-making.

To assure defensibility, the project team defined the elements of a risk methodology based on the risk disciplines as they apply to the policy guidance and the conditions and constraints of the targeted users. Then, to identify candidate federally sponsored tools, the team conducted a series of meetings with federal agencies with responsibility for different aspects of CISR, especially the lifelines. They were asked to summarize their tools, methods or processes for lifeline CI risk and vulnerability analysis and near term plans in some detail. Altogether, 23 tools and processes were identified and all but one was reviewed in summary. Annex D.1 contains summaries of the tools examined.[25]

The approach was to characterize each tool based on presentations by agency representatives as supplemented by information drawn from agency websites. These were then compared with an initial CISR-RMP standard process developed from CISR policy guidance, conditions and constraints of potential users, the design objectives and contemporary risk analysis disciplines.[26] This approach is illustrated along the left side of Attachment 1, reproduced here for convenience, in sections corresponding to the major phases of the NIPP 2013 CI Risk Management Framework.

D.1 Defensibility: A Discipline-Based Risk/Fragility Analysis Process Criteria Set

This initial, discipline-based standard for the present project (columns 1 and 2, respectively, in Attachment 1) argues that consistent definitions of key terms, common, ratio-scale modes of measurement, a common initial threat/hazard set and consistent, comparable results are essential for rational choices in setting priorities or allocating resources to reduce risks and/or fragility.

In ***Phase 1, Set Goals and Objectives,*** the standard requires defining and weighting the decision-makers' goals and objectives using a formal method such as Multi-Attribute Utility Theory or Analytical Hierarchy Process (AHP). While advocates for each of these methods strongly disagree with one another, reasonable arguments for both are available. In application, AHP seems easier for novices to grasp quickly and use immediately. For the CISR-RMP, we have added convening and organizing a regional coalition or public-private partnership and adapting a standard information sharing and protection agreement—both necessary for analysis of interdependencies and collaboration on CISR investments. For convenience, we have also included hazard description in this phase because the hazards that "keep you

[25] Limitation: these are cursory characterizations only, so bear some risk of misinterpretation.
[26] In addition to DHS publications cited in Section 3, numerous risk methodology sources consulted. See the Bibliography.

awake" are at least implicit in CISR goals and objectives. Policy calls for "all-hazard" risk analysis, so all categories of threat and hazards are listed in a standard set. This set would be structured so that the defined hazards are mutually exclusive (they do not overlap) and collectively exhaustive (all possible events are included when "no significant negative event" is assumed to complement the list of possible negative events included). The standard set is simply a starting point, as inapplicable hazards are deleted and unlisted local ones are added, but necessary to assure comparability and utility in interdependency analysis. Deleted hazards are assumed to have a likelihood of zero, so the list remains collectively exhaustive.

In ***Phase 2, Identify Infrastructure,*** specific systems, facilities and assets (collectively, "assets") are defined as critical to the extent they are necessary for the infrastructure to perform the organization's basic mission to meet demand for infrastructure services. Usually these are conceived as subsystems of the system that performs the core mission, with the subsystems made up of assets and flows. In the ideal, all such assets would be included in the analysis, but few CIs or local communities have the analytical resources for this, so the assets are screened and ranked by initial, gross estimates of the consequences of their loss under a given negative event.[27] The most important assets are then arrayed in a matrix against the threats and hazards, and the threat-asset pairs with the greatest impact (based on very crude, quick, even ordinal rankings) are selected for detailed analysis. These threat-asset pairs are the scenarios that are the object of the rest of the analysis.

In ***Phase 3, Assess and Analyze Risk***, technical specifications are essential. The disciplines would argue that uncertainties are very large and consequential for CISR risk analysis, so the key terms in the risk and fragility equations should be estimated as probability distributions and combined by Monte Carlo simulation, accounting for correlations and dependencies among terms; interdependencies should be modeled through a system-of-systems approach with all properties and functions defined with full uncertainties and again modeled by Monte Carlo simulation with correlations. Once improvement options are defined, alternative portfolios (collections of options) would be chosen by formal portfolio analysis, in which all possible portfolios and their uncertainties are analyzed to determine which lie along an "efficient frontier" of portfolios that maximize benefits at all levels of uncertainty. The decision-makers select among these portfolios the one that best fits their tolerance for uncertainty. This is the approach used very successfully in financial, pharmaceutical and international oil and gas firms. Very few CIs or local governments, however, have this level of expertise or understanding; indeed, very few organizations of any kind can fully meet this standard. Proposing it, even with outside expertise to perform it, would be intimidating and likely poorly understood by the users this project is targeting—and certainly would not lead to wide-spread adoption and integration with other business processes.

[27] Some risk professionals would argue that all assets involved in meeting the organization's mission must be assessed for all threats and hazards. In light of the limitations on personnel and analytic capacity, it is preferable to focus on the most important threat-asset scenarios to a futile attempt to be comprehensive.

Attachment 1. Detailed Technical Criteria vs. Federally Sponsored Lifeline Risk/Resilience Manangement Methods

NIPP 2013 Phase		CISR-RMP Design Objectives	Full Ratio Risk & Resilience						Conditional Ratio Risk					Ordinal Risk				
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
		Sponsor	OR/Econ/ Engg	DHS/IP/S&P CISR-RMP		DHS/S&T	AWWA	EPA/IP/ AWWA	USACE	FEMA	DoT/FHWA		DHS/TSA	USCG	DHS/IP	DoE	DOT/FHWA	
		Method/Tool	Discipline Ideal	Minimum Require-ment	Currently Available	Nashville Feasibility Pilot (1)	J100-15 In Progress	J100-10	Dam Security Tool/CRM(2)	THIRA	CAPTA	Component-Level: Bridges	Component-Level: Tunnels	MSRAM	VCAT (withdrawn)	State Energy Assess. (3)	VAST (4)	Vulner. Assessm't Framework
1. Set Goals and Objectives	1.	1. Goals & Objectives -- means for users to define and weight																
	2.	Convene & organize regional coalition or public-private partnership		🟦	🟦													
	3.	Adapt Common Information Sharing & Protection Protocol		🟦	Current Need													
	4.	Goal Setting & weighting																
	5.	a. Formal goal weighting (Multi-Attribute Utility Theory or Analytical Hierarchy Process)		🟦	🟦	🟦												
	6.	b. Informal but explicit goal statement required	🟦	🟦	🟦		🟦	🟦	🟨	🟦	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
	7.	c. Assumed to be risk and/or fragility reduction							🟨	🟦	🟦	🟦	🟦	🟦	▨	▨	▨	▨
	8.	2. Threats -- explicitly included																
	9.	a. Standard, including																
	10.	i. Terrorism	🟦	🟦	Current Need	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		
	11.	ii. Crime & Vandalism	🟦	🟦	🟦	🟦	🟦	🟦	🟨		🟨			🟨				
	12.	iii. Episodic natural hazards, e.g., storms	🟦	🟦	🟦	🟦	🟦	🟦		🟦	🟦			🟨			🟦	🟦
	13.	iv. Slowly evolving climate change, e.g., sea level rise, drought	🟦	🟦	🟦	🟦	▨			🟦	🟦			🟨			🟦	🟦
	14.	v. Cyber attack	🟦	🟦	🟦	🟦	▨	▨	🟨	▨	▨			🟨				
	15.	vi. Dependency	🟦	🟦	🟦	🟦	🟦	🟦		▨				🟨				
	16.	vii. Proximity	🟦	🟦	🟦	🟦	🟦	🟦						🟨				
	17.	viii. Age/wear/accidents	🟦	🟦	Current Need		🟦		🟨		▨			🟨				
	18.	ix. Product/service contaminated	🟦	🟦	🟦	🟦	🟦	🟦						🟨				
	19.	b. Local additions acceptable	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟦				🟨				
	20.	c. Required but no standards set								🟦						🟦		
2. ID Infra-structure	21.	3. Asset Identification																
	22.	a. Devolved from mission, function	🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟦				🟦	🟦	🟦	
	23.	b. Screened for criticality		🟦	🟦	🟦	🟦	🟦	🟦		▨				🟦	🟦	🟦	🟦
	24.	c. Required, but no standard ID process								🟦		🟦	🟦	🟨				
3. Assess and Analyze Risk (Partial)	25.	4. Risk/Resilience Analysis																
	26.	a. Risk = f(T, V, C), & fragility metrics each *estimated as distributions*, combined thru Monte Carlo simulation	🟦	Future Strategic Enhance-ments														
	27.	b. Dependencies modeled as system-of-systems, with uncertainties	🟦															
	28.	c. Portfolio modeling to find efficient combinations from correlations	🟦															
	29.	d. Post-event analysis-based real-time resource allocation	🟦	Future														

LEGEND	Suspected	Not Suspected		
Unknown	🟨	⬜		
	Fully Present	Partially Present	Missing	
Ratio Scale	🟦	▨	Current Need	Future Need
Ordinal Scale	🟩	▩		

Attachment 1 is continued on the next page.

Notes: (1) AWWA J100-10 was the risk tool used in the Nashville Feasibility Pilot.

(2) Common Risk Model for Dams addresses human malevolent threats only. It is a conditional risk method applied in two different ways. For a single dam, threat likelihood is set to 1.0 for all scenarios, but if the analysis is for a set of dams, the likelihood of thre adversary selecting any particular dam is is estimated based on its asumed relative attractiveness based on Likelihood of Success (Vulnerabiity) and Consequences. The assumptioon is also that at least one dam will; be attacked, so the calculated risk is still conditional, but incorporating adversary choice moves it one step closer to full risk.

(3) DOE's State Energy Assessment Initiative is more a meta-analysis of needs & requirements.

(4) VAST is designed to be used with Vulnerability Assessment Framework.

Attachment 1 (Continued). Detailed Technical Criteria vs. Federally Sponsored Lifeline Risk/Resilience Manangement Methods

NIPP 2013 Phase		Sponsor Method/Tool CISR-RMP Design Objectives	Full Ratio Risk & Resilience						Conditional Ratio Risk					Ordinal Risk				
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
		Sponsor	OR/Econ/ Engg	DHS/IP/S&P CISR-RMP		DHS/S&T	AWWA	EPA/IP/ AWWA	USACE	FEMA	DoT/FHWA		DHS/TSA	USCG	DHS/IP	DoE	DOT/FHWA	
		Method/Tool	Discipline Ideal	Minimum Require-ment	Currently Available	Nashville Feasibility Pilot (1)	J100-15	J100-10	Dam Security Tool/CRM(2)	THIRA	CAPTA	Component-Level: Bridges	Component-Level: Tunnels	MSRAM	VCAT (withdrawn)	State Energy Assess. (2)	VAST (3)	Vulner. Assessm't Framework
3. Assess and Analyze Risk (Continued)	30.	e. Risk = f(T, V, C), each *estimated as points*		🟦	🟦	🟦	🟦	🟦	▨	▨	▨	▨	▨					
	31.	i. T = Threat Likelihood as absolute probability		🟦	🟦	🟦	🟦	🟦	▨					🟨				
	32.	ii. V = Vulnerability as conditional probability		🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	▧	▧	▧	▧	▧	▧	▧
	33.	iii. Co = Consequences to owner	🟦	🟦	🟦	🟦	🟦	🟦	🟦									
	34.	-- Liabilities: Human casualty & other	🟦	🟦	🟦	🟦	🟦	🟦	🟦			🟨	🟨	🟨	🟨	🟨	🟨	🟨
	35.	-- Direct dollar losses to owner	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	36.	iv. Cr = Consequences to the region & nation	🟦	🟦	🟦	🟦												
	37.	-- Human casualties (incl. VSL)	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	38.	-- Loss of Gross Regional Product	🟦	🟦	Current Need	▨	▨	▨		🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	39.	-- Environmental impacts	🟦	🟦	🟦	🟦				🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	40.	-- Symbolic/psychological/confidence	🟦	🟦	🟦	🟦				🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	41.	-- National security	🟦	🟦	🟦	🟦				🟦	▨	🟨	🟨	🟩	🟨	🟨	🟨	🟨
	42.	f. Fragility or other outage or continuity metric	🟦	🟦	🟦	🟦	🟦	🟦		▨								
	43.	g. Dependencies modeled as system-of-systems, deterministic	🟦	🟦	Current Need	▨	🟨			▨								
	44.	h. Calculate risk & fragility to both enterpirise and regional public	🟦	🟦	🟦	🟦	🟦	🟦										
4. Implement Risk Management Activities	45.	5. Risk-Based Decision-Making																
	46.	a. Sorts risks to accept, transfer, manage	🟦	🟦	🟦	🟦	🟦	🟦										
	47.	b. Requires definition of options for managing	🟦	🟦	🟦	🟦	🟦	🟦	▨	🟦				🟨				
	48.	c.Estimates benefits based on risk analysis	🟦	🟦	🟦	🟦	🟦	🟦	▨			▧	▧	▧	▧	▧	▧	▧
	49.	d.Requires estimation of costs	🟦	🟦	🟦	🟦	🟦	🟦	▨	🟦				🟨				
	50.	i. Life-cycle costs	🟦	🟦	🟦	🟦	🟦	🟦	🟨					🟨				
	51.	ii. Budget requirements	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟨	🟨	▧	🟨	🟨	🟨	🟨
	52.	e.Joint benefits analysis	🟦	🟦	🟦	🟦	🟦											
	53.	f. Specific decision-rules for selecting options	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟨	🟨	🟨	🟨	🟨	🟨	🟨
	54.	g Sensitivity analysis of major uncertainties	🟦	🟦	Current Need		🟦	▨		🟦								
	55.	h. Routine management control systems to monitor costs and implementation milestone	🟦	🟦	🟦					🟦								
	56.	i. Post-event analysis-based real-time resource allocation	🟦	Future														
5. Measure Effectiveness	57.	6. Performance Evaluation																
	58.	a. Inputs & process assessment	🟦	🟦	🟦													
	59.	b. Outputs assessment	🟦	🟦	🟦													
	60.	c. Risk analysis based outcomes assessment, with exercises & actual events	🟦	🟦	Current Need													

LEGEND

	Suspected	Not Suspected		
Unknown	🟨			
	Fully Present	Partially Present	Missing	
Ratio Scale	🟦	▨	Current Need	Future Need
Ordinal Scale	🟩	▧		

Notes: (1) AWWA J100-10 was the risk tool used in the Nashville Feasibility Pilot.

(2) Common Risk Model for Dams addresses human malevolent threats only. It is a conditional risk method applied in two different ways. For a single dam, threat likelihood is set to 1.0 for all scenarios, but if the analysis is for a set of dams, the likelihood of thre advesary selecting any particular dam is is estimated based on its asumed relative attractiveness based on Likelihood of Success (Vulnerabiity) and Consequences. The assumptioon is also that at least one dam will; be attacked, so the calculated risk is still conditional, but incorporating adversary choice moves it one step closer to full risk.

(3) DOE's State Energy Assessment Initiative is more a meta-analysis of needs & requirements.

(4) VAST is designed to be used with Vulnerability Assessment Framework.

Strategically, this level of sophistication should be deferred at present, while acknowledging its desirability for a future version. Elements of this approach, however, can be introduced *over time* as expertise and the desire for more advanced tools is expressed by user organizations. The alternative is to use single-point estimates of the key terms *in ratio scale metrics* combined by standard mathematical functions. [28] Analysts estimate threat likelihood, vulnerability, consequences to the owner and to the region, and the duration and severity of outages for each threat-asset pair; and calculate *baseline* risk and fragility.

Many terrorism risk analysts stress the ability of an intelligent adversary to react to and counter security initiatives so that estimating the likelihood of attack on a specific threat-asset pair requires a more sophisticated approach such as game theory. Even if the historical record were not too thin to permit frequency analysis, some risk analysts say that the adaptability of an intelligent, knowledgeable and motivated assailant can overcome many or most countermeasures—to an extent that the concept R = T×V×C may be invalid for terrorism risk (Cox, 2008b; Bier, 2005; Bier and Azaiez, 2009). They recommend use of a variation of game theory or related techniques. We reject this notion for two reasons: (1) the current state of the art is immature enough that even those who agree that game theory should be used do not agree as to how, and (2) game theory analysis is very difficult to perform even by experts, so has little role in a pragmatic methodology for municipal workers and CI engineers, operators and managers. If such an approach is to be put to use, it should be part of a national effort to develop sound, but simple procedures for local officials and CI personnel to use.

Note in Attachment 1 that the elements of classic security risk as required by the disciplines and the minimum requirement for the desired CISR-RMP are listed individually and that risk to the owner and to the regional public are both required. Most risk analyses by default assume the interests of either the owner (as in business risk analysis) or the public (as in policy analysis benefit/cost analyses). Because the CISR-RMP must support both the decisions by enterprise leaders and representatives of the public, both are addressed in the required CISR-RMP. They differ in the definition of consequences and outages and, possibly, the decision-relevant metrics (many enterprises use net revenue and return-on-investment, while most governments use net benefits and benefit/cost analysis). In addition to taking only one relevant perspective, many risk analysis methods leave out one or more critical dimension of risk, most often the likelihood of the threat or hazard event, but sometimes even the vulnerability of the asset to the event. Included in this phase are the criteria of at least one metric of fragility (or other indicator of resilience), and the deterministic system-of-systems modeling of interdependencies among the lifelines.

A variety of complementary models can be useful in Phase 3 (as well as Phases 4 and 5) but are *not* required to make rational choices—and may, at first, complicate the process enough that it is rejected wholesale by potential users. Many lifelines maintain computer models of their systems for use in planning and managing operations and development. These can be especially helpful in tracing the

[28] Many risk professionals in the respective disciplines would be professionally opposed to using point estimates when the uncertainties are as high as in all-hazards CI risk analysis, arguing that capturing these uncertainties is essential to understanding risks and risk-reduction benefits. We concur over the long term, but recognize that so few potential users are familiar with probability distributions and Monte Carlo simulation that their inclusion would severely limit the use of the process. As a strategy, introducing risk analysis with simple point estimates allows greater sophistication to follow. In Brashear's experience, analysts who become comfortable with very basic analytic methods begin to request upgrades when they are ready for them. For example, analysts who find point estimates difficult because of uncertainties usually ask to estimate them as ranges. From there, advancing to full probability distributions is a short step.

internal dependencies of process workflows to estimate the full consequences of an asset's failure. Front-line managers, engineers and operators who manage the operations of such systems typically have sophisticated mental models of how their systems operate. Such models are usually accurate and precise enough to support risk analysis at this level. It usually facilitates discussion, however, to prepare flow charts of the basic processes and subsystems, even if only based on these mental models.

Other models assist in specifying the nature of current and future threats, e.g., climate change models, while others help in estimating consequences, e.g., "plume" models of toxic gas releases into the atmosphere. Some complementary models return specific damage estimates based on the specifications of the threat or hazard and properties of the assets, e.g., blast models. These models are *not* required because they are usually complex, require a great deal of data and personnel time, and can be costly to use, even if the software is provided free of charge. When the risk is especially large or critical, these models are invaluable in building confidence in the estimates.

Phase 4, Implement Risk Management Activities, starts with the decision about which risks and fragilities the decision-makers choose to accept as they are, to transfer through insurance, or to actively manage by designing and evaluating options. Options are defined and designed to enough detail to support cost estimation and to specify which risk/fragility elements would be changed and by how much. Risk analyses for both the enterprise and the regional public are conducted *assuming* the option is implemented. The difference in risk and fragility with the option and without it is the gross benefit of the option. A joint-benefits analysis sorts out options that benefit more threat-asset pairs than just the one each was designed for and combines the total benefits (adjusting out any double-counting).

This is followed by a net benefits analysis (gross benefits less lifecycle costs, both in discounted present values[29]) and specific decision-rules are applied to preliminarily select options within available budgets. The selected options are subjected to sensitivity analysis of both the risk without the option and with it to see whether plausible uncertainties would change the selection. This sensitivity analysis process partially offsets the disadvantages of using point estimates instead of probability distributions. This continues until the selected options are those that, even considering uncertainties within a plausible range, promise the greatest net benefit within the budget constraint.

If the initial setting of goals and objectives had additions beyond security and resilience (e.g., economic growth, social or geographic equity), these are incorporated into the final selection of options. The selected options are detailed, implemented, and monitored according to the organization's routine management controls. In the future, this CISR-RMP may be able to allocate flexible resources in real time for managing a crisis.

Phase 5, Measure Effectiveness, interprets the inputs, processes and outputs measured in Phase 4 according to the enterprise's standard accounting, project management and output/sales measurement processes. These are interpreted as to the extent the options were implemented as planned. For *outcomes* measurement, the process is to re-estimate risk and fragility after an appropriate amount of time, taking into account any events that actually happen (locally or in other locations) and the results of tabletop and red team exercises designed to test the effectiveness of the options as implemented. Objectivity in this

[29] A present value is the "time value" of a stream of future cash flows (or their equivalent, e.g., benefits) that is discounted to the present by a discount factor that reflects the greater value of near term over the longer term. It has the effect of making options of differing durations comparable in time, e.g., options with a duration of one, ten and fifty years can be directly compared if all are in present values. The discount rate in the private sector is usually linked to the cost of capital or strategic aspirations, while in the public sector, they are typically set by policy, with the bond interest as a minimum.

risk/fragility analysis would be enhanced by the use of analysis teams other than those who conducted the original baseline and options valuation risk/fragility analyses and/or providing quality assurance reviews. Based on any or all of these interpretations, corrective actions are taken.

Note that vulnerability and resilience are also often assessed using multi-question indicators, often tied to "best practices" or explicit standards. Frequently, they are used in benchmarking to compare the local situation with others. Several of these are in extensive use, such as IP's Infrastructure Survey Tool and the National Institute of Standards and Technology is following this approach in developing its *Community Resilience Planning Guide* (NIST, in preparation), so they were included in the summary review. None of these measures risk or benefits of investments or programs to advance CISR or support outcomes assessments, but rely on the decision-maker to determine whether to comply with the best practice or standard.

D.2 Review of Federally Sponsored Risk Analysis Tools

To provide an efficient way to describe the diverse approaches, methods, models and tools, it is useful to characterize them along a rough continuum from approaches that fully estimate risk and fragility or resilience in fully documented, technically defensible, repeatable and transparent ways, through essentially non-risk methods to models that complement risk analysis by providing needed elements, but do not produce risk or resilience estimates themselves. The methods, processes and tools examined can be ranked in terms of rigor in six categories along the following continuum:

1. Full ratio scale risk *and* fragility or other ratio metric of resilience,
2. Full ratio scale risk (without a ratio resilience metric),
3. Conditional ratio scale risk,
4. Ordinal scale risk,
5. Indices and indicators of vulnerability and/or resilience, and
6. Complementary models to assist in risk analysis.

The first three categories are listed across the top of Attachment 1. Indicators and complementary tools were left out of the table because they meet virtually none of the criteria. They are not designed to analyze risk or evaluate options except in the broadest qualitative way. All the individual tools available before this phase of the project was completed are summarized in Annex D. For the purposes of the CISR Risk Management Process, only the first two categories can fully meet the requirements defined to this point because they are the only ones using ratio metrics of risk and fragility. Only ratio-scale estimates can be used in all the necessary calculations – baseline, option valuation and performance assessment – and avoid decision distortions in the cases of very large consequences and very low likelihoods.

Categories of methods that do not meet this criterion, however, can contribute useful insights. Partial ratio scale risk tools can add the missing elements to become full ratio scale risk tools. Ordinal risk assessments introduce their users to the broad concepts of risk analysis and their results can be used to identify and rank assets and threat-asset pairs for full ratio-scale risk analysis. Users of ordinal scale tools can readily be trained to employ ratio scales because the underlying ideas are understood. Indicators can identify areas for further analysis and can be a rich source of options for improving security and resilience that can be analyzed using a full ratio-scale risk method to establish whether they justify their costs.

This summary reviews tools based on presentations by federal employees and supplemented by information provided on agency websites. Of the twenty-four tools:

- Only one process—shown in three forms as columns 4-6 of Attachment 1, ANSI/AWWA J100-10, its update (J100-15, in preparation) and regional application (Nashville Feasibility Pilot, which used J100-10), can be characterized as full ratio risk and resilience, estimating both R = f(T, V, C) where the function is the product and the variables are point estimates using ratio scales, and *fragility*, defined as the product of outage (average unmet daily demand times the duration of the outage) and the same vulnerability and threat likelihood as the associated risk, or F = f(T, V, O), also a ratio scale. Other than a number of multi-variate indices of resilience, this was the only risk-related, ratio metric of resilience we found among the various tools reviewed. J100-10 is currently being updated as ANSI/AWWA J100-15 for release later in 2015 or early 2016. The updated version corrects several minor errors; deletes the "bins" for estimating vulnerability and consequences and the use of conditional risk (assuming 1.0 as probability of terrorist events); adds the threat of an asset's failing due to wear, fatigue or aging, and methods for including ice storms and wildfires to the original set of natural hazards – earthquakes, flooding, hurricanes and tornados, all of which were updated. J100-10 was the risk/fragility tool used in the 2011 field pilot in Metropolitan Nashville and Davidson County, Tennessee to test its generality and initiate modeling od interdependencies. Although J100 was originally developed for water and wastewater systems, the approach and its immediate predecessor are regarded as general to any system having physical assets. The approach has now been successfully used in a variety of fields other than water/wastewater, including chemical manufacturing, oil refining, LNG terminals, nuclear power plants, nuclear waste storage and transport, dams and navigational locks, college and university campuses, electricity distribution, emergency communications and dispatch, fire suppression, emergency medical, police emergency operations, landfills, highways and bridges. [30]
- Five of the reviewed processes are partial ratio risk, quantifying consequences and vulnerabilities in the risk equation – USACE's Common Risk Method – Dams (CRM-D), FEMAs Threat and Hazard Identification and Analysis (THIRA), DOT's Costing Asset Protections for Transportation Agencies (CAPTA) and Component-Level Risk Management for Bridges and TSA's Component-Level Risk Management for Tunnels. The missing element in all cases was threat likelihood. The content and precision specifications for measuring consequence and vulnerability varied widely from very broad descriptors to relatively detailed directions for the process. The main problem with leaving likelihood out of the calculations is that it forces decision-makers to attempt to mentally adjust for consequences of events that are orders of magnitude different in impact. Mentally differentiating between an event expected once in ten years and once in a hundred thousand years exceeds human capacity, whereas calculated expected values using likelihood of each is not.
- Five are ordinal risk methods—the U.S. Coast Guard's MSRAM; DHS/IP's VCAT, which, as noted has been discontinued; DOE's State Energy Assessment Initiative; DOT's VAST, FHWA's Gulf Coast 2 (more a project than a tool, so not shown on the chart), Vulnerability Assessment Framework,

[30] Disclosure: One of the authors of this report, Brashear, led the project that updated RAMCAP for the last time (ASME-ITI, 2009) developed RAMCAP for the water sector (ASME-ITI, 2007b), the predecessor to J100, and has served as a member of the J100 (AWWA, 2010) Standards Committee since its inception. He also developed an extension to J100 that allowed it to be used in a *regional* portfolio approach (Brashear, 2009) and in the regional context with interdependencies in the 2011 the Nashville Feasibility Pilot (Brashear, *et al.,* 2011).

and Component-Level: Bridges; and DHS/TSA's Component Level: Tunnels. These generally include at least threat likelihood (sometimes breaking out vulnerability) and consequences, but because of the coarse categories and unbounded upper end of consequences and the lower end of likelihood, are unable to be used to calculate benefits or discriminate among options. A number of cleaver attempts have been made over the years to correct this limitation, but none has succeeded.

- Three were index methods consisting of lengthy questionnaires about vulnerabilities, protective measures in place, etc. They included Baseline Assessment for Security Enhancement (BASE) for Mass Transit (DHS/TSA), BASE for Highway Vehicles (DHS/TSA), and Pipeline Corporate Security Review (DHS/TSA). Federal employees with related experience apply most of these. Each consists of several areas of interest, each of which is addressed with a series of questions. Scores are weighted sums in each area, presented as a comparison of individual entities with benchmarks of other entities in the industry.

In addition to the tools explicitly reviewed, a few other federal index tools are worth mentioning because they were discussed with local and federal respondents or were included in the 2015 review of DHS risk tools by GAO (2015).

- Although not presented for discussion, DHS/IP's Infrastructure Survey Tool (IST) used in the voluntary Regional Resilience Assessment Program and Site Assistance Visits is a voluntary assessment taking up almost 300 pages, using more than 1500 variables covering six components and 42 subcomponents administered by trained Protective Service Advisors from the Protective Security Coordination Division of DHS/IP. Results in all four cases (including the IST) are presented as index scores and comparative benchmarks, with the implication that areas of lower scores need to be raised. The language used to discuss these is that a lower score on an item represents a "gap" or "vulnerability" to be remedied.
- The Federal Protective Service (FPS) employs a "Modified IST" to review vulnerabilities of federal buildings (National Academies, 2010).
- The new NIST Cybersecurity Framework is also an index type tool, guiding users to specific, mostly voluntary standards to use to raise scores.
- NIST is developing a voluntary Community Resilience Planning Guide as this is written, but early indications are that it will, like the Cybersecurity Framework, be a voluntary standards-referenced indicator system, with detailed standards for each of several infrastructures, but no formal risk analysis to value compliance. The NIST draft has been criticized for the absence of a risk analysis component, resulting in the presumption that all the standards listed should be met.

These seven index tools are not risk analysis, by any definition, although these survey-based indicators are often discussed in qualitative risk and vulnerability language.

Three additional tools in this survey were supplemental tools—EPA's WHEAT, DoT's CMIP and FHWA's Circular 25 – help to estimate future hazards or damage as a function of asset properties and the specific stresses of defined threats and hazards; these are representative of a much larger number of such tools.

Several federal employees stated that there was a broadly held opinion that, given the nearly two decades since the need for risk analysis to guide resource allocation for critical infrastructure security was articulated, the current state of the risk analysis tool development is relatively immature. Only one of the tools presented called for full ratio risk analysis attempted to quantify resilience on a ratio scale. Even granting the USACE dams tool, two tools seems an extremely low number considering the fully articulated disciplinary standard is well more than 60 years old and the millions of dollars that have been invested in developing and applying these tools. This review has considered the lifelines only, so there may well be full risk and resilience tools available in non-lifeline CIs and in other areas. It is important to note that these are the only tools identified within this study that can be used to calculate the information required for the benefit/cost and return-on-investment analyses required for rational resource allocation.

The other tools do bring some value, although fully rational, quantitative decision guidance is not among them. Both partial and ordinal risk methods convey key concepts of risk analysis, so it is a relatively modest amount of adaptation to advance to full ratio metric risk/fragility analysis. For users of partial risk methods, their users have only to acquire ratio-scale estimates of threat likelihood to be able to perform a more useful risk analysis. The lack of threat likelihood information for human threats is attributable to the unwillingness of the intelligence and law enforcement communities to put forward quantitative, ratio-scale estimates. This is a significant policy issue for DHS to address. Many users of partial risk methods express interest in obtaining and using this information to make natural hazard risk comparable with man-made risk to improve their decisions.

In the case of the ordinal risk tools, the gap is larger, requiring changing from using comfortable but overly compressed ordinal scales. “Very high” estimates of consequences and “very low estimates of probability – the cases where risk analysis is most needed – may contain orders of magnitude differences even if the scales levels are consistently defined. That risk analysis concepts have been introduced and used, however, suggests that steps toward greater rigor, precision and consistency might be seen as improvements in what users are already doing. The remarks among the potential users that more specific guidance would be welcomed supports this view.

The indicator systems present a much more difficult challenge in moving toward full risk management. This general approach is widely accepted by professional security and law enforcement managers and many emergency managers. They are simple (if lengthy) and provide concrete, specifics as to what should be done. Some, perhaps many, users of these tacitly believe that the numerical indices can stand in lieu of risk analysis. The potential for distorting decisions here is that the implied guidance that money should be spent to “close the gap,” to bring the user’s organization “up to standard” or to meet “peer” scores, with no way to value the advocated step.

By the nature of the index and indicator tools, it is not possible to say whether real risks are reduced, whether the implied risk is worth reducing, or if the implied actions are worth their cost. These tools, however, do contribute to broadening the understanding of users to the full scope of possible vulnerabilities and they contain numerous ideas for options that might be employed should specific risks be identified. According to GAO (2015), in Fiscal Years 2011 through 2013, PSAs performed 3,255 assessments, the FPS an additional 1,458 and TSA performed 545 – a relatively large number of foregone opportunities for true risk analysis. During the same period, the Coast Guard directly performed 93 risk analyses and oversaw up to 3500 self-analyses using ordinal risk MSRAM.

Also notable was that the tools of all types with greatest “market penetration” were those implemented through active technical assistance and/or quality control, ranging from the fully articulated implementation organization used by the Coast Guard with MSRAM to FEMA’s THIRA, with its broad guidelines and loose association with FEMA grants. With MSRAM, the organizational system is appended to a military command-and-control system. The indicator tools used by TSA, IP and FPS are also supported by a significant number of trained DHS personnel who have established constructive relationships with local infrastructure owners and operators. THIRA, the partial risk tool by FEMA with essentially complete market penetration for its target audience, is supported by annual training programs and is required of all states and UASI regions that desire to participate in certain FEMA grant programs, although the amount and purposes of the grants are not tied to THIRA results. This suggests that active, supported federal involvement is necessary to move technical CISR risk assessment tools of any type into widespread use by targeted users – but that it clearly can be done.

Annex D.1 Report of a Limited Survey of Federal Processes, Methods and Tools for Risk/Resilience Management at Regional and Local Levels

Introduction. A portion of the Critical Infrastructure Security and Resilience Risk Management Process (CISR-RMP) project is the characterization of current and near-term processes that critical infrastructures (CIs) used in decision-making about reducing risks and enhancing resilience. The priority is the lifeline CIs – water/wastewater, transportation, energy and telecommunications. Many of the relevant processes have been sponsored by or required by federal agencies. In January 2015, we conducted a series of meetings to summarily survey what the federal CISR community is currently supporting and has in development for the near term for use by local and regional lifelines and local governments and regional partnerships.

With the assistance of IP/S&P and IP/SOPD, we invited all known federal offices that might be sponsoring or encouraging use of specific processes, methods or tools to address man-made and/or natural hazards (including those associated with climate change). Special efforts were made to reach out to the Sector Specific Agencies specified in NIPP 13. A general meeting was held on January 20, 2015, at the National Institute of Building Sciences. Subsequent meetings were held on January 28 at the Transportation Security Administration headquarters with several transportation agencies, January 29 at the office of Chris Duvall with DHS/Cyber Security & Communications, February 13 with Dan Schmelling of EPA's Water Division, and May 19 with Yasmin Seda-Sanaberia and J. Darrell Morgeson.

At each of these, the conversations followed the same general outline (Annex 1). At the first and second, agency representatives briefly presented tools currently in use, being developed, and in one case, a tool that had been removed from active use. The presentations used in these meetings may be found in Attachment A to this report, submitted as a separate file. At the third meeting, a more ranging conversation was held, supported by extensive printed material describing the methods used in the cyber and communications area. In the fourth, we discussed the recent updates of an EPA risk tool and one of its key subordinate models.

This appendix summarizes the tools that were examined. They are evaluated and discussed at length in Section 5 of this report.

January 20 Meeting. Six approaches were presented and discussed by the 31 individuals shown in Appendix 2. The presentations are provided in the Attachment, so they are only briefly summarized here, along with notes and high points from the discussion.

1. Federal Highway Administration (FHWA). Two tools were presented by the FHWA contractor, ICF International. (See Attachment > Jan 20 > Snow DHS Workshop on Risk and Resilience Tools.) Both dealt with climate change threats in particular.

a. DoT CMIP (Coupled Model Intercomparison Project) Climate Data Processing Tool – a *complementary* model by the definitions above – is a user-friendly, Excel-based tool that downscales local climate projections from the Coupled Model Intercomparison Project Phases 3 and 5(CMIP3 and CMIP5) using an initial downscaling by the U.S. Bureau of Reclamation's Downscaled CMIP3 and CMIP5 Climate and Hydrology Projections (DCHP) (http://www.fhwa.dot.gov/environment/climate_change/adaptation/adaptation_framework/modules/user_guide/cmip_user_guide.pdf). It takes the user's selection among 21 optional climate projections and downscales local projections for areas as small as 56 square miles (7.5 miles by 7.5 miles). Such downscaled data are vital to identifying present and future threats arising from climate change. It provides the results of each model including, their mean and confidence limits for a variety of temperature and precipitation descriptors.

The discussion related to the continuing scientific debates and uncertainties and to certain technological limits to the model itself. One participant stated what appeared to be a broad consensus: "I accept its results. It allows us to move forward on the risk side with a fully defensible, best-available science-based estimate. Otherwise, we can't move forward."

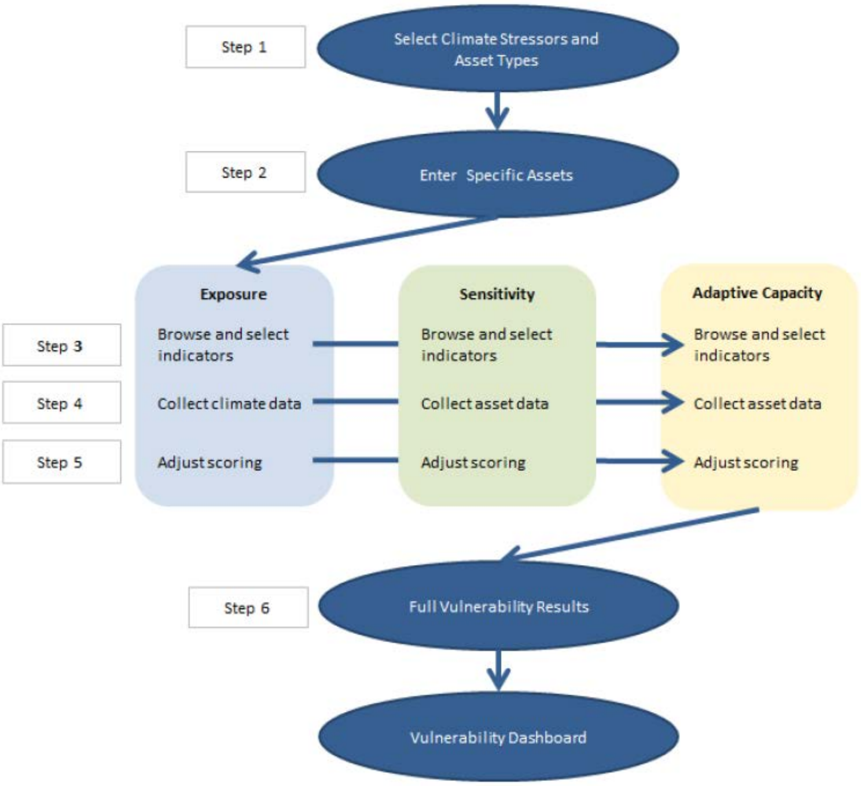


Figure A. USDoT/FHWA Vulnerability Assessment Scoring Tool (VAST)

b. Vulnerability Assessment Scoring Tool (VAST, Figure 1) – an *ordinal risk* approach – is also a user-friendly, Excel-based tool that looks at the impact of climate change on local transportation assets. The VAST presentation is contained in the previously cited link in the Attachment. The tool is available at http://www.fhwa.dot.gov/environment/climate_change/adaptation/adaptation_framework/. Designed to help local decision-makers and their staffs decide how to allocate their resources, the tool estimates Vulnerability by deciding, first, which assets and climate-related stressors are most important to worry about, specifying each in detail. Then, specific Vulnerability is estimated as a user-weighted combination of the components: Exposure (specific nature of the stressor), Sensitivity (specific condition of the asset) and Adaptive Capacity (cost of improvement, length and duration of detour around the asset). Individual indicators are scored in a 1-4 ordinal scale and combined by user-supplied weights to Component scores, which are themselves combined by user-supplied weights for an overall Vulnerability Score. The results are displayed in the form of a matrix of the elements and combined Vulnerability score by asset, with the improvement costs, with the most vulnerable highlighted in red.

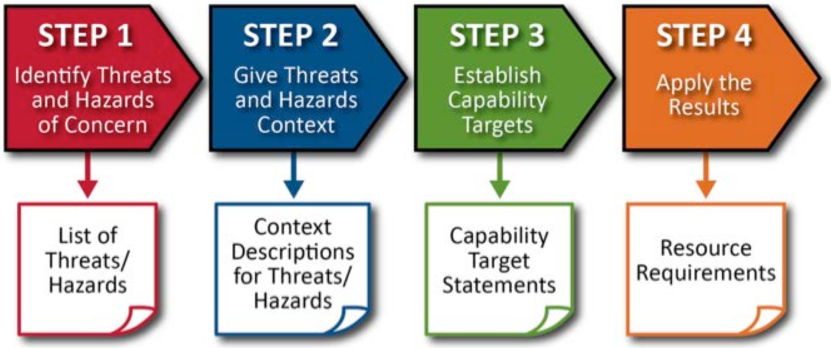

STEP 1
Identify Threats and Hazards of Concern
STEP 2
Give Threats and Hazards Context
STEP 3
Establish Capability Targets
STEP 4
Apply the Results
List of Threats/ Hazards
Context Descriptions for Threats/ Hazards
Capability Target Statements
Resource Requirements

Figure 2. FEMA Threat and Hazard Identification and Risk Analysis

Several states and metropolitan transportation planning organizations have adopted VAST for making resource trade-offs.

2. Federal **Emergency Management Agency** (FEMA) *Threat and Hazard Identification and Risk Analysis* (THIRA, Figure 2) – a *partial risk* process (see Attachment > Jan 20 > THIRA Overview NPPD 20150112)—is the analysis guiding FEMA’s implementation of Presidential Policy Directive 8 (PPD-8) to strengthen national preparedness for disasters at state, regional and local levels. The scope is the “whole community,” which usually means Urban Area Security Initiative (UASI) metropolitan regions and states, both of which are required to file THIRAs to be eligible for certain FEMA grants (although these filings are not used in allocating the grant funds).

The Process consists of four steps (Figure 2): (1) Identify Threats and Hazards of Concern – enumeration; (2) Give Threats and Hazards Context – specification of enough details to enable estimation of the severity of the impact on the community relative to 31 standard Core Capabilities; (3) Establish Capability Targets – defining the levels and requirements for each core capability that the community believes are needed to manage the worst of the threats affecting that capability (usually in performance terms); and (4) Apply the Results – estimation of the specific resources (as defined in the National Incident Management System standard naming conventions) needed for each core capability and programmatic planning for managing the worst-of-the-worst events.

The hazards are those of concern to the community, so they vary from place to place. They may include natural events, terrorism, industrial accidents and any others of concern to the users. The impacts can be described in any terms, but tend to focus on human casualties and physical losses. As a partial risk method, THIRA asks for locally defined vulnerabilities and consequences, but, while identifying hazards and threats, their likelihood is neither estimated nor considered. The users are almost universally emergency management professionals at the state and local levels. Of the 31 core capabilities, only the 13 most closely related to emergency management and early-stage recovery have been required to be included to date.

3. DHS Office of Infrastructure Protection (IP) *Chemical Security Assessment Tool* (CSAT, Figure 3, see Attachment > Jan 20 > VCAT Overview Workshop Info sharing risk tools) – an *ordinal risk* process –

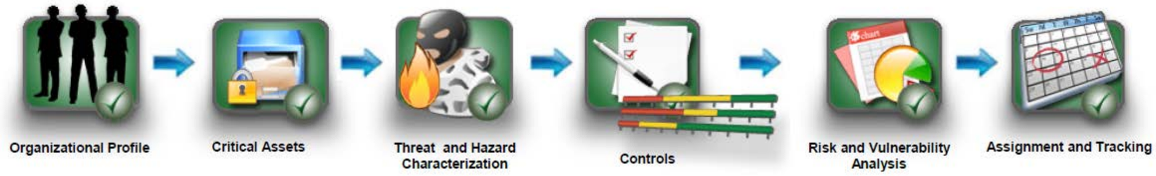


Figure 3. DHS/IP Voluntary Chemical Assessment Tool (VCAT)

was developed for use by chemical facilities that failed to pass the “top screen” based on the magnitude and criticality of possible consequences to be required to implement the Chemical Facility Anti-Terrorism Standards for chemical facilities. For these smaller and less critical facilities, the *Voluntary Chemical Assessment Tool (VCAT)* was developed as a software suite based on the commercially available software *CounterMeasures*® (Alion Science and Technology Corporation), which had been “validated” by the U.S Strategic Command.

The process is fully automated and designed for use by in-house teams, who are asked to make a series of ratings. The “profile” is a description of the site, node or facility overall. Potentially critical assets are inventoried and scored on a five-by-five matrix of the “value of the asset to an adversary” versus “impact on the facility’s ability to function.” Hazard frequency is rated on a five-point scale ranging from “More than once per year” > “Once a year” > “Once every 5 years” > “once every 20 years” > “Once every 100 years or less (or more).” Hazard severity is rated in a five-by-five matrix of “Intent” defined as the level of the adversary’s motivation, and “Capability” based on judging the likelihood of the adversary’s having the capability developed and having it in place. Controls are recorded as measurable observations based on rules and regulation compliance, administrative and technical procedures, and preventive, corrective and detective countermeasures. The program combines these judgments into an overall risk score (subdivided by break-outs by levels of control through existing countermeasures, those proposed, and residual risk). The most important vulnerabilities, threats and critical assets are also displayed. A “cost-to-benefit analysis” is provided based on estimated countermeasure cost in dollars and benefits derived from numerical analysis of the rankings. It is unclear how benefits are calculated given that the underlying data are ordinal and open-ended.

The method had more than 500 users by 2013 and was endorsed by at least three major chemical industry associations before it was “decommissioned” to save costs to DHS; it was replaced by the Infrastructure Survey Tool, administered as part of the Enhanced Critical Infrastructure Protection by federal Protective Service Advisors.

4. Department of Energy (DoE) *State Energy Assessment Initiative* (see Attachment > Jan 20 Presentations > Creating a Culture of Risk Assessment brochure 01072015) – an *ordinal risk* method – is being developed in-house by DoE staff for use by a combination of state-level staff and DoE experts. Its purpose is “to better understand potential impacts to energy infrastructure.” The Initiative is being carried out in collaboration with the National Association of State Energy Officials (NASEO), the National Association of Regulatory Utility Commissioners (NARUC), the National Conference of State Legislatures (NCSL), and the National Governors Association (NGA). Its goals are to “increase States’ awareness of risk to energy systems to help them better prepare for disruptions and to make more informed decisions; inform and assist States on available analytical capabilities and resources for identifying and evaluating energy infrastructure risks; and provide a suite of scalable, easily-applied analytical tools, methods, and processes to enable States to better assess risks to energy systems and assets." These goals are to be advanced by meeting four objectives: "1. Determine State energy risk assessment needs; 2. Assess current practices in State-level energy risk analysis; 3. Identify tools, methods, and processes to evaluate risk related to energy assets and systems; and 4. Engage with key stakeholders (across entire risk analysis development cycle)." The process identifies threats and hazards (likelihood is not mentioned), rates assets by vulnerability and consequences, which are assigned weights by algorithm. DoE experts assign Criticality scores based on importance in assuring energy continuity. Risk is calculated based on these rankings and expressed as a numerical score. Resilience is not explicitly estimated, while interdependencies are mentioned, but the approach is not elaborated. The approach has been used in two pilot projects that evaluated major NFL stadiums.

5. DHS/IP, Environmental Protection Agency (EPA) **and American Water Works Association** (AWWA) *Standard J100-10 Risk and Resilience Management of Water and Wastewater Systems* (J100, see Attachment > Jan 20Presentations > J100 Summary Updated 01-20-15)—a *full risk and resilience analysis* process—originated in the DHS/IP Risk Analysis and Management for Critical Asset Protection (RAMCAP) program, which developed a highly simplified, fully quantitative risk analysis process that was generic to all or most infrastructures for consistency and comparability within and across sectors and communities. This basic process was then tailored to the technologies, cultures and special issues in each sector, while maintaining the standard definitions, process and metrics to assure comparability of results, regardless of sector. The approach was extensively and successfully tested in each of seven diverse critical infrastructures – nuclear power, nuclear waste, chemical manufacturing, oil refining, liquefied natural gas terminals, dams and locks, and water and wastewater systems. The basic system was itself updated three times to meet IP's evolving mission, moving from a terrorism focus to all-hazards, from simply risk to risk and resilience.

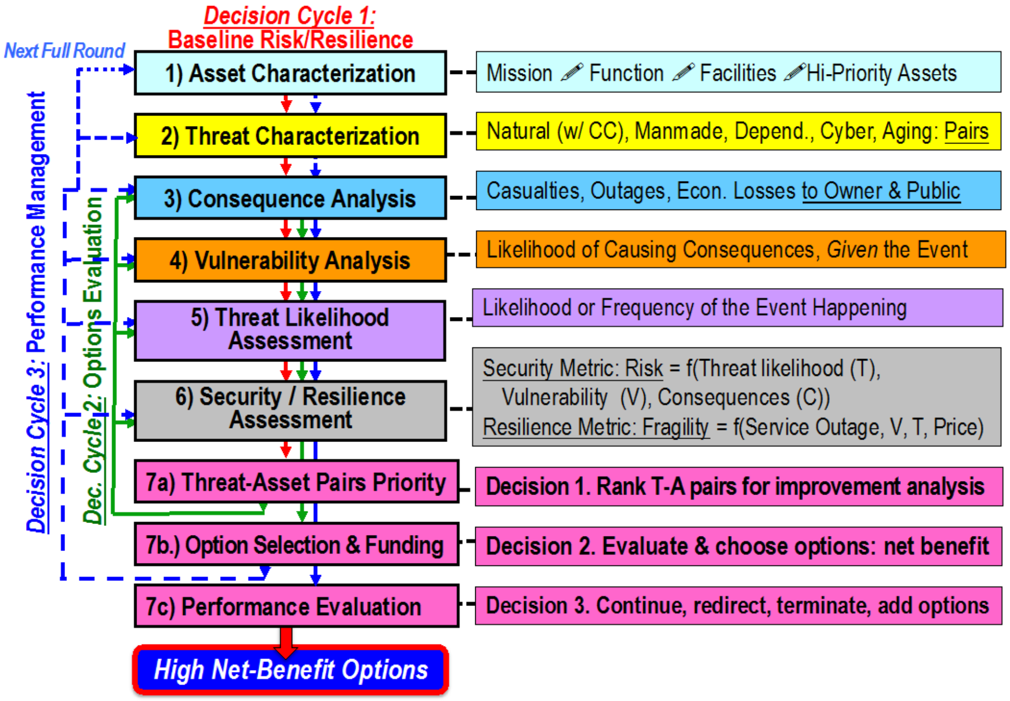

Decision Cycle 1:
Baseline Risk/Resilience
Next Full Round
Decision Cycle 3: Performance Management
Dec. Cycle 2: Options Evaluation
1) Asset Characterization
2) Threat Characterization
3) Consequence Analysis
4) Vulnerability Analysis
5) Threat Likelihood Assessment
6) Security / Resilience Assessment
7a) Threat-Asset Pairs Priority
7b.) Option Selection & Funding
7c) Performance Evaluation
High Net-Benefit Options
Mission ✐ Function ✐ Facilities ✐Hi-Priority Assets
Natural (w/ CC), Manmade, Depend., Cyber, Aging: Pairs
Casualties, Outages, Econ. Losses to Owner & Public
Likelihood of Causing Consequences, Given the Event
Likelihood or Frequency of the Event Happening
Security Metric: Risk = f(Threat likelihood (T), Vulnerability (V), Consequences (C))
Resilience Metric: Fragility = f(Service Outage, V, T, Price)
Decision 1. Rank T-A pairs for improvement analysis
Decision 2. Evaluate & choose options: net benefit
Decision 3. Continue, redirect, terminate, add options

Figure. 4 ANSI/AWWA Standard J100-10 Risk and Resilience Management of Water and Wastewater Systems

The water sector determined to develop the American National Standard now called ANSI/ AWWA J100-10 as a vehicle for updating their 2003-2005 vulnerability assessments required by the Bioterrorism Act of 2002. DHS has designated the standard under the SAFETY Act. EPA, the Sector Specific Agency for the water sector under the NIPP, a National Laboratory and several engineering firms have developed software packages that implement the standard. At least the EPA tool and one of the proprietary tools have also been designated under the SAFETY Act. The basic process was also successfully feasibility tested in a significant metropolitan area as the primary risk method in a regional risk/resilience analysis that included water, energy, emergency communications and dispatch, emergency medical care, fire suppression, law enforcement, and roads and bridges, along with their interdependencies.

J100 (Figure 4) is designed for use by in-house engineering and operating personnel in support of utility managers' budgeting decisions. It includes a standard starting set of all hazards, including many of the effects of climate change. It addresses dependencies as threats of shortages of key inputs – energy, chemicals, personnel, etc. Both physical and system control and data acquisition (SCADA) assets are included. Improving security is defined as reducing Risk (R = T x V x C) and improving resilience is defined as reducing Fragility (Fragility = T x V x Service Outage x Price, where Service Outage = units demanded/day x number of days of outage Price is the pre-disruption price of the product or service). Both are estimated from the perspectives of the system owner *and* of the community it serves, respectively, to identify major areas of externalities and other market failures for attention by both owners and the community in collaboration.

The analysis proceeds in three decision cycles: (1) Baseline risk and resilience estimation – the "cost of doing nothing"—leading to the decision as to which risks justify developing options; (2) Options evaluation—defining security and resilience options and evaluating the extent to which they reduce T, V, C of SO, thereby reducing risk and fragility – leading to the decision as to which to include in the appropriate budgets; and (3) Performance management – using the same definitions and methods (complemented by exercises and actual field experience when possible) to monitor what is working for effective management.

The J100-10 Standard, available from AWWA, has been accepted by the Government Coordinating Council and the Sector Coordinating Council as the water industry standard. Several hundred copies of J100 have been sold, primarily to the larger utilities and the engineering firms that support the sector. AWWA has scheduled release of the update (J100-15) in late 2015. The automated version of J100 sponsored by EPA, the Vulnerability Self Assessment Tool (VSAT), Version 6.0, is available free of charge at http://water.epa.gov/infrastructure/watersecurity/techtools/vsat.cfm. Usefully, it is supported by a supplemental consequence estimation tool, Water Health and Economic Analysis Tool (WHEAT, http://water.epa.gov/infrastructure/watersecurity/techtools/wheat.cfm), that estimates ratio scale values for fatalities and injuries, financial costs to the utility and economic impacts on the community of the loss of an operating water system asset, water contamination and release of toxic gas. According to EPA, they plan to keep VSAT current as the J100 standard is updated.

January 28 Meeting. At IP's request, the Transportation Security Administration arranged for a number of the agencies responsible for the respective subsectors (”modes") of transportation to prepare summaries of their methods and processes for managing risk and resilience and to present them in highly summarized form (the hand-outs of which are included in the Attachment under "Jan 28.") The participants in that meeting are also listed in Appendix 2.

1. U.S. Department of Transportation (DOT) *Costing Asset Protections for Transportation Agencies* (*CAPTA*, See Attachment > Jan 28 > CAPTA Info)—a *partial risk* method—is a consequence-based risk management approach to capital budgeting that departs from traditional risk management strategies. It includes asset and hazard identification (both natural and man-made) and estimation of consequences (and implicitly vulnerability, with and without mitigating countermeasures) and the costs of the countermeasures in support of operating and capital budget decisions. It does not attempt to assess the likelihood of threat or hazard taking place, but assumes that if a decision maker perceives the possibility of a threat or hazardous event (assuming the event is sufficiently severe), the decision maker should consider alternatives for avoiding or minimizing consequences. The consequence-based approach focuses on how the asset has been adversely affected, not on why or how it happened. It may be employed by a range of agencies responsible for risk management across transportation modes in an all-hazards environment: Regional entities, such as port authorities, toll authorities, and transit authorities; State agencies, such as DOTs and state emergency management agencies; and Local agencies, such as Departments of Public Works and County Highway Departments. Infrastructure project designers and planners, transportation project resource managers, those responsible for transportation infrastructure security are all intended users. Its use is voluntary and its documentation is readily available by Internet, so no data are available as to the number of users. While many natural hazards are considered, climate change *per se* is not.

2. DOT/ Federal Highway Administration (FHWA) and DHS/TSA *Component-Level Risk Management for Bridges* (FHWA), *Tunnels* (DHS/TSA), respectively (see Attachment > Jan 28 > Ernst Response…)—both *partial risk methods* are virtually the same except as noted. These tools are designed to assist bridge/tunnel owners, designers, planners and project developers to consider terrorist risk. Natural hazards, including those associated with climate change are not explicitly treated. Dependencies and interdependencies are not included. The emphasis is on physical assets, with the inclusion of cyber assets when operating centers are among the assets being analyzed. “Quantitative relative risk” is evaluated as a function of threats, vulnerabilities and importance for all components that ensure structure stability and function. Each component is evaluated for base risk and mitigated risk and strategies are then evaluated for cost. Comparing cost to relative risk reduction provides a cost to benefit measure. For tunnels, casualty risks are also estimated as base and mitigated levels. It is unclear whether threat likelihood is included or casualty risks are converted to dollars or used in benefit/cost analysis. State DOT’s and their consultant partners have used this method during development for several significant bridge projects. FHWA and DHS both use this method for bridge assessment. State examples are CA, TX, KY, and NY. DHS has used the tunnel risk analysis method for its assessments.

3. DHS/TSA *Baseline Assessment for Security Enhancement* (BASE) for mass transit and highway vehicles and *Pipeline Corporate Security Review* for pipelines—all three use *indicators* approaches—provide voluntary guidance tailored for mass transit and passenger rail, with parallel tools for highway vehicles (busses, trucks) and pipelines. In all three cases, structured interview guides consisting of more than 100 questions each around broad security-related issues (e.g., 17 for mass transit, 20 for highway vehicles) identified by security experts as contributing to security. The focus is on those assets with greatest criticality, here defined as the impact on continuity of function and volume of use. TSA inspectors, working with the owner’s personnel, administer the spreadsheet instruments to qualified operators who volunteer. There are about 300 TSA inspectors engaged in this work for some portion of their time. The resulting information is returned to TSA for analysis. TSA sends the owners an executive summary with scores in each area (displayed with a red-yellow-green scheme) and recommendations for improving these scores by reference to the respective guidelines. Supplemental conferences and technical assistance are offered to owners requesting help.

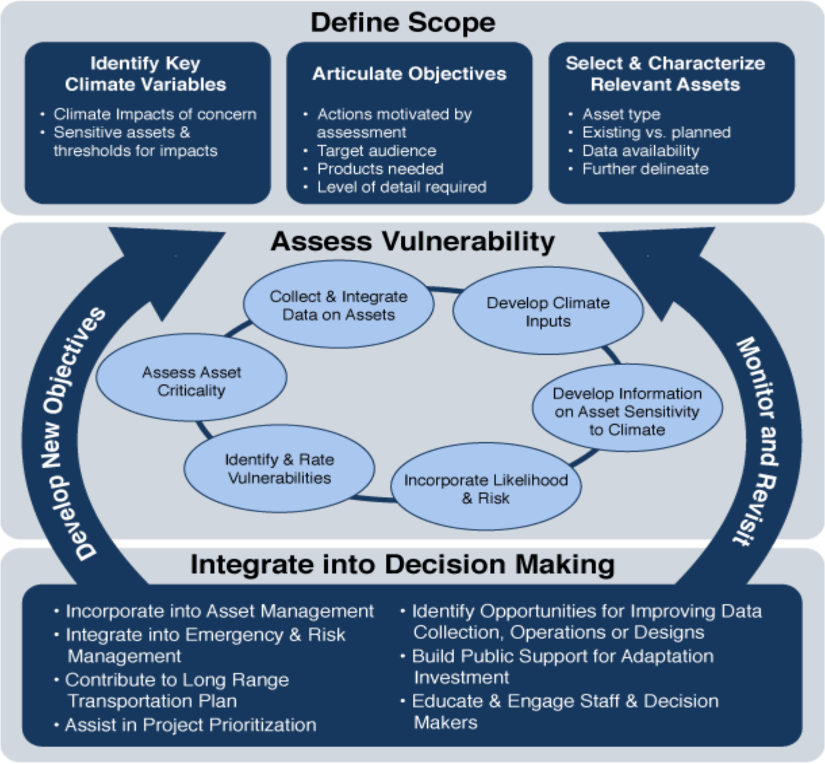

Define Scope
Identify Key Climate Variables
• Climate Impacts of concern
• Sensitive assets & thresholds for impacts
Articulate Objectives
• Actions motivated by assessment
• Target audience
• Products needed
• Level of detail required
Select & Characterize Relevant Assets
• Asset type
• Existing vs. planned
• Data availability
• Further delineate
Assess Vulnerability
Collect & Integrate Data on Assets
Develop Climate Inputs
Develop Information on Asset Sensitivity to Climate
Incorporate Likelihood & Risk
Identify & Rate Vulnerabilities
Assess Asset Criticality
Develop New Objectives
Monitor and Revisit
Integrate into Decision Making
• Incorporate into Asset Management
• Integrate into Emergency & Risk Management
• Contribute to Long Range Transportation Plan
• Assist in Project Prioritization
• Identify Opportunities for Improving Data Collection, Operations or Designs
• Build Public Support for Adaptation Investment
• Educate & Engage Staff & Decision Makers

Figure 5. FHWA Vulnerability Assessment Framework

Note: DHS/TSA also contracts with the U.S. Army Corps of Engineers to conduct in-depth vulnerability assessments of particularly important tunnels and bridge-tunnel combinations. A Tunnel Risk Assessment Methodology Paper will be one of the products synthesized from the series of field assessments.

4. **FHWA**'s work on analyzing climate change effects on transportation assets and resilience to them consists of several related efforts, including a series of 22 climate change resilience pilot projects and four cooperative projects. The most recent count of agencies that have completed climate vulnerability assessments includes 24 state DoTs and 30 Metropolitan Planning Organizations (see Attachment > Jan 28 > bcrt and http://www.fhwa.dot.gov/environment/climate_change/index.cfm). FHWA has four related efforts relevant to the present project (see Climate Change Tool Information and the same Website):

a. Gulf Coast Phase 2 Project (GC2)—an *ordinal risk* methodology—is an in-depth analysis of all modes of transportation in the Mobile, Alabama, metropolitan region. It builds on the larger lessons learned in the GC1 study of the Gulf Coast from Mobile to Houston, Texas. Its methodology roughly follows the Framework, discussed next, so it serves as a pilot and demonstration of the feasibility and practicality of the approach.

b. FHWA Vulnerability Assessment Framework (the FHWA Framework)—an *ordinal risk* methodology—is illustrated in Figure 5. The Framework is designed for use by planning, engineering and asset management practitioners at State Departments of Transportation (DOTs), Metropolitan Panning Organizations (MPOs) and federal Land Management Agencies (FLMAs). It covers surface transportation systems and assets, including roads, bridges, culverts, operational infrastructure (e.g. maintenance facilities, traffic signals), ports, pipelines, and airports.

Assets are selected for inclusion based on a multi-variate scoring approach; climate variables are selected by location and broad regional projections; and objectives are set locally. The actual "Assess Vulnerability" function employs the DoT CMIP and VAST processes described above. The basic R = f(T, V, C) concept is used, but risk is treated more qualitatively rather than "calculated" or "measured." Many areas use climate "scenarios" to represent likelihood, and evaluate vulnerability and consequences by applying procedural tools (FHWA Framework), or spreadsheet tools (GC2). Areas applying these tools have scoped and evaluated alternative solutions to make assets and systems more resilient. In some applications, a type of economic analysis was done to compare costs and benefits, though most stop short of this type of analysis. Interdependencies are not included. As shown in the decision function at the bottom, it is seen as contributing to an array of regional and local decisions. Several agencies around the U.S. have used/applied the tools and methods. Most of the agencies involved in the 19 FHWA Climate Resilience Pilot Program are using the Framework, and many are using the GC2 tools/methods. At least one agency is actively using the methodologies in HEC-25.

c. Hydraulic Engineering Circular Volume 25: Highways in the Coastal Environment (HEC-25) (see Attachment > Jan 28 > Climate Change Tool Information, http://www.fhwa.dot.gov/engineering/hydraulics/pubs/07096/07096.pdf)—a *supplemental tool*—is an engineering guide to data sources and calculation methods to implement the FHWA Framework and to go beyond that in sophistication by replacing the ordinal judgments about consequences of specific events with ratio scale values and incorporating more mathematical rigor.

Note: FHWA also publishes guidance and suggestions as to useful security and resilience design concepts for use by this same audience, e.g., "Considering Security and Emergency Management in the Planning of Transportation Projects" (see Attachment > Jan 28 > ConsideringSecurityAndEM.)

5. U.S. Coast Guard (USCG) *Maritime Security Risk Analysis Model (MSRAM*, see Attachment > Jan 28 > MSRAM_brochure)*)*—an *ordinal risk* method—is a terrorist risk analysis process (Figure 6) that is applied annually by the Coast Guard to support a variety of management decisions at strategic, operational and tactical levels. Its application across the country has resulted in a national database of more than 7000 assets (e.g., vessels, facilities, infrastructure) and 17,000 scenarios (threat-asset pairs). Its level of sophistication is the risk novice to allow widespread use with a practical amount of in-service training and supporting information. Its application is a "bottom-up" process with rigorous, multi-tiered "top-down" review to encourage realism and consistency.

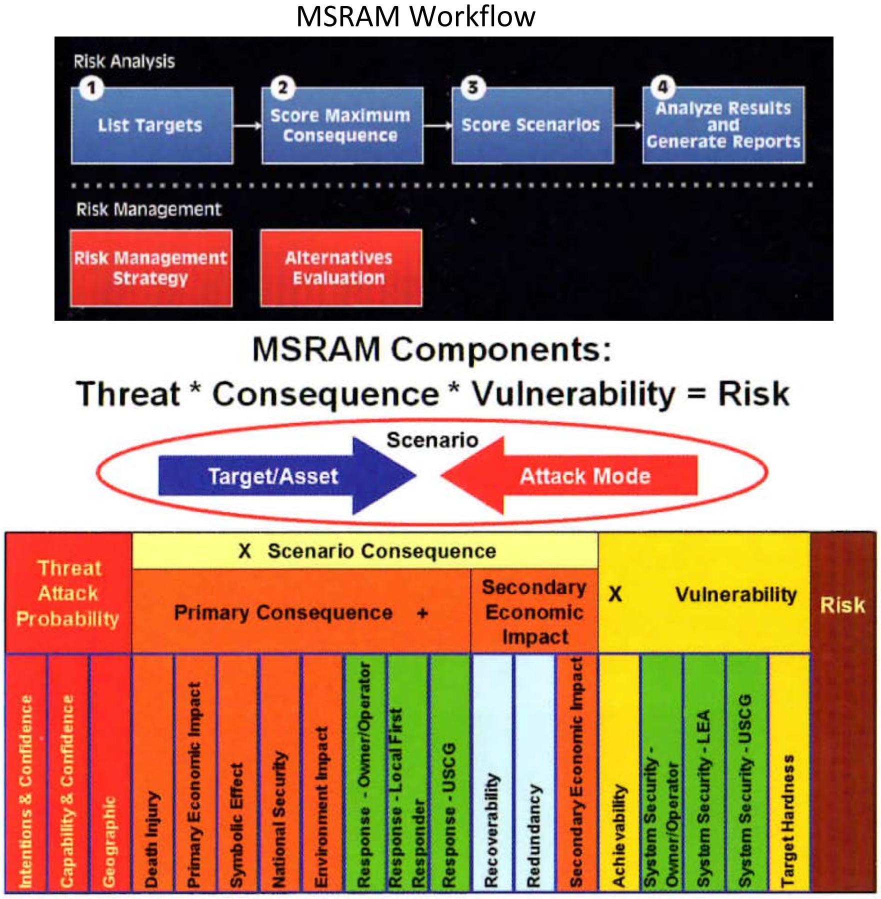


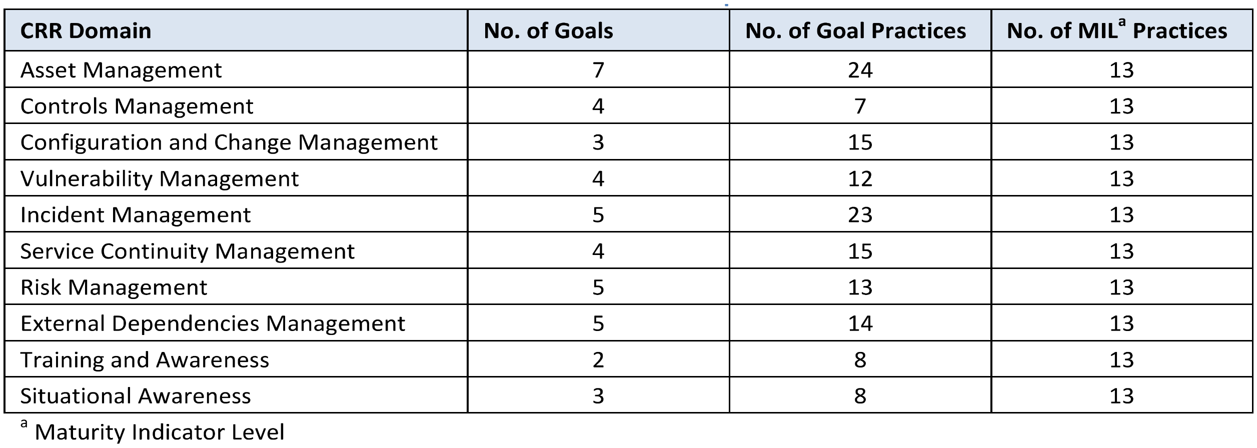
Figure. 6. U.S. Coast Guard Maritime Security Risk Analysis Model (MSRAM)

Analysts are supported by scenario-specific benchmarks, factor scoring tools, access to the national database for analogous information, a reference library and a centralized help desk to support the accuracy, consistency and comparability of the results. The reviews bring expertise and experience to identify outliers, to challenge estimates, and assist the analysts in best use of the supplemental tools and information. The USCG analysts, experts, reviewers and decision-makers apply the process annually, working in close collaboration with owner/operators, local emergency response and law enforcement though Area Maritime Security Committees in areas of operations, largely ports. It obtains quantitative estimates of threat likelihood through collaboration with the intelligence community.

MSRAM's output includes risk-ranked lists of targets and scenarios; counts of targets at similar levels of risk; geographic information system layers displaying the location, nature and magnitude of the respective risks; comparisons of risk with and without government contributions; risk reduction value to owners, local law enforcement, first responders and the USCG. These outputs are used to identify the highest risk targets and scenarios, geographic density of risk, estimates of USCG risk-reduction performance over time, regulatory development, grant allocation, budget proposals, exercises and training, prioritizes issues for port-wide risk management, directs intensive risk management for very high-risk targets.

Communications and Cyber Security. In a brief conversation with Christopher Duvall, Office of Communications and Cybersecurity on January 29, this survey was extended to risk/resilience tools and processes in the communications and information technology sectors. All the cybersecurity methods discussed use the *indicator approach*, keyed to established standards.

The telecommunications industry actively cooperates and coordinates with the federal government through several mechanisms such as the National Coordinating Center for Communications (NCC), formed after the breakup of the AT&T monopoly to continue the industry-federal cooperation. The NCC now includes representatives of more than 50 major companies in the industry and twenty-four federal agencies, operating as a branch of the National Cybersecurity and Communications Integration Center (NCCIC). Given this active level of cooperation, no federal agency has initiated a risk analysis process or tool, except for the extensive cybersecurity process discussed below. This project was unable to obtain what proprietary processes or tools are in use by communications companies.

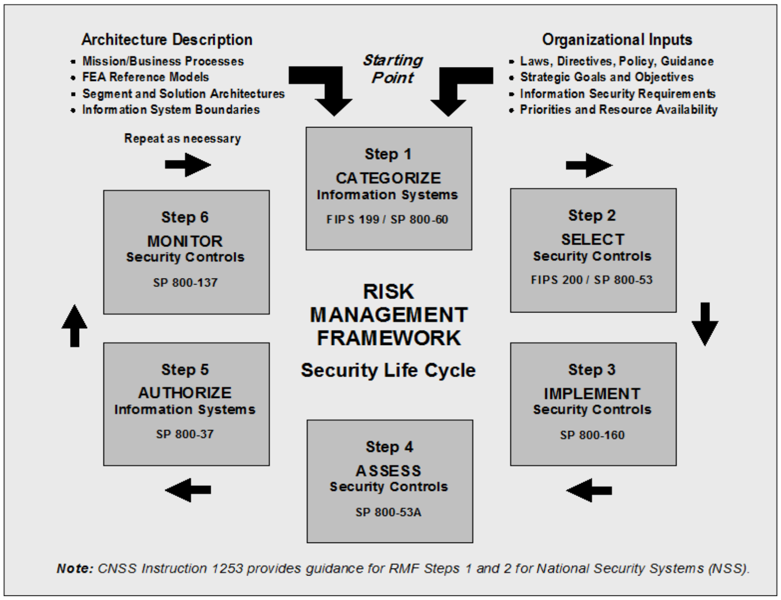


CRR Domain	No. of Goals	No. of Goal Practices	No. of MIL[a] Practices
Asset Management	7	24	13
Controls Management	4	7	13
Configuration and Change Management	3	15	13
Vulnerability Management	4	12	13
Incident Management	5	23	13
Service Continuity Management	4	15	13
Risk Management	5	13	13
External Dependencies Management	5	14	13
Training and Awareness	2	8	13
Situational Awareness	3	8	13

[a] Maturity Indicator Level

Figure 7. NIST Cybersecurity Framework Architecture

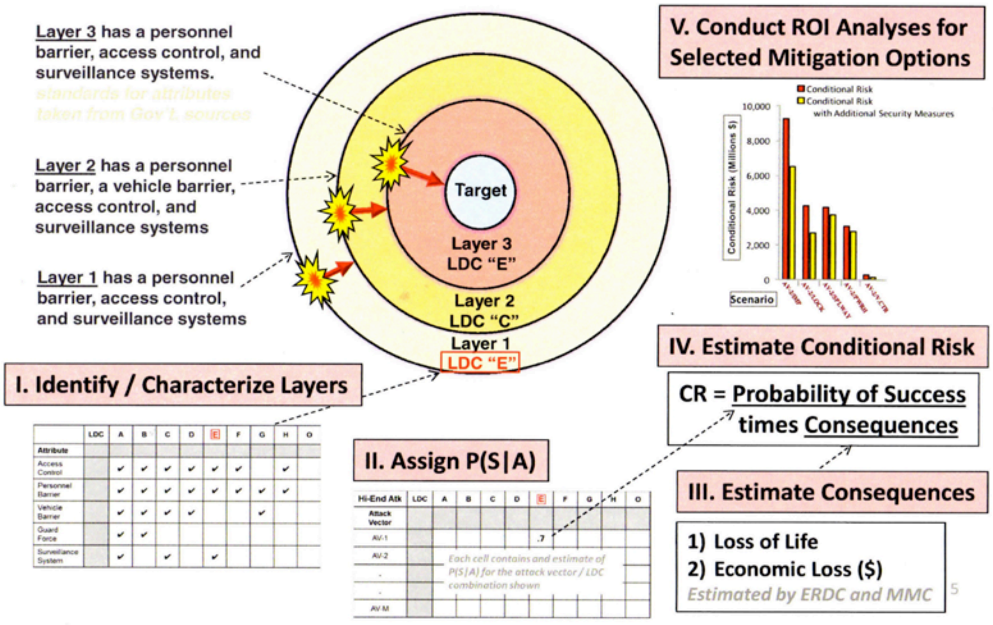
Presidential Policy Directive 21 and Executive Order 13636 set in motion development of a national Critical Infrastructure Cybersecurity Framework, which has now been completed by a collaboration of industry and federal agencies coordinated and documented by the National Institute of Standards and Technology (NIST). The Framework operates as a voluntary indicator-style risk management approach based explicitly on established standards and best practices. It consists of the ten domains shown in Figure 7. There are a number of "goals" and "goal practices" for each domain that, when implemented, move the user organization to higher levels of "maturity" (measured as "Maturity Indicator Levels") as a secure system.



Note: *CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).*

Fig. 8. NIST SP 800-53 (Rev. 4) Risk Management Process

One of the domains in the Framework is "Risk Management," which refers extensively to the Special Publication NIST-SP-800-53, Revision 4 as the operative standard. Figure 8 shows the workflow shown in that standard. Given the particulars of the system architecture and the organization it serves, the process is largely one of selecting the appropriate security controls based on standards, implementing them and managing them. The underlying standards are updated regularly based on actual experience.


Layer 3 has a personnel barrier, access control, and surveillance systems.
standards for attributes taken from Gov't sources
Layer 2 has a personnel barrier, a vehicle barrier, access control, and surveillance systems
Layer 1 has a personnel barrier, access control, and surveillance systems
Target
Layer 3
LDC "E"
Layer 2
LDC "C"
Layer 1
LDC "E"
I. Identify / Characterize Layers
II. Assign P(S|A)
III. Estimate Consequences
1) Loss of Life
2) Economic Loss ($)
Estimated by ERDC and MMC
IV. Estimate Conditional Risk
CR = Probability of Success times Consequences
V. Conduct ROI Analyses for Selected Mitigation Options
Conditional Risk
Conditional Risk with Additional Security Measures
Conditional Risk (Millions $)
10,000
8,000
6,000
4,000
2,000
0
Scenario
5

	LDC	A	B	C	D	E	F	G	H	O
Attribute										
Access Control		✓	✓	✓	✓	✓	✓		✓	
Personnel Barrier		✓	✓	✓	✓	✓	✓	✓	✓	
Vehicle Barrier		✓	✓	✓	✓			✓		
Guard Force		✓	✓							
Surveillance System		✓		✓		✓				

Hi-End Atk	LDC	A	B	C	D	E	F	G	H	O
Attack Vector										
AV-1						.7				
AV-2										
.										
.										
AV-M										

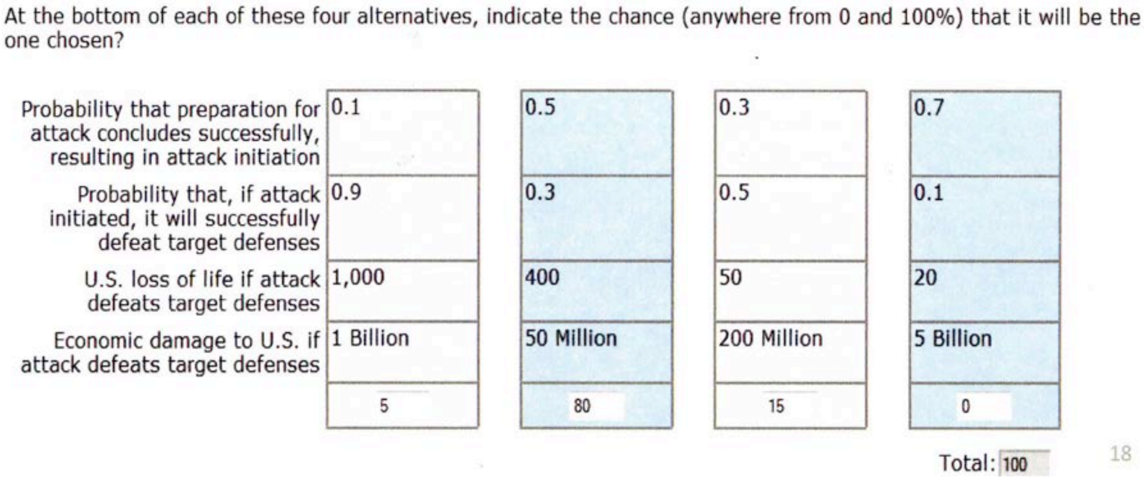
Each cell contains and estimate of P(S|A) for the attack vector / LDC combination shown

Figure 9. U.S. Army Corps of Engineers Common Risk Method – Dams

The U.S. Army Corps of Engineers (USACE) has developed the Common Risk Method – Dams (CRM-D) for dams security using the R=T×V×C formulation, point estimates, and a partial portfolio approach. The output is conditional risk, assuming threat likelihood is 1.0 for the individual facility level (Figure 9) and a somewhat more comprehensive approach for multi-facility trade-off decisions. Threats are limited to man-made. Vulnerability analysis uses the concept of layers of defense: up to five specific defensive layers may be present, placing the facility in a specific layer-of-defense class (LDC), which relates to a standardized conditional vulnerability. Multiplying this vulnerability by consequences (estimated elsewhere and input to the CRM-D) yields a conditional risk, given that an attack takes place at the subject facility. Risk mitigation options are evaluated using a sort of cost-effectiveness analysis (here called "ROI," or return-on-investment analysis), although the resulting benefit values are necessarily overstated by the amount of the threat likelihood. This allows rudimentary trade-offs if one is willing to as highly uncertain. Because it only includes man-made threats, it introduces less distortion that it would in an all-hazards approach. It does not set an actual dollar value of benefits of the mitigation options.

For higher level, multi-facility analysis, the likelihood of selection of each specific facility, *given* that one will be attacked, is included in the analysis. This Adversary Value Model (Figure 10) is based on expert judgment of a variety of experts, whom are asked to allocate a total of 100 percent likelihood of selection of a dam across a collection of dams. It is assumed there will be an attack and that all attack modes are equally likely. This method is similar to the "proxy" method in AWWA J100-10, but limited to the target selection given that there will be an attack on one of the specific collection of dams. As with the single facility, a partial return-on-investment analysis of risk mitigation options across the set of dams is possible within these assumptions.

These can then be arrayed as a likelihood-by-consequences display (Figure 11). It should be stressed that the probability of attack in Figure 11 is a conditional likelihood of the facility's selection given that one attack on the collection of dams will occur annually and that the assailant escapes pre-attack detection and interdiction and has detailed knowledge of the likelihood of attack's being successful (the vulnerability) and the consequences of the specific attack.



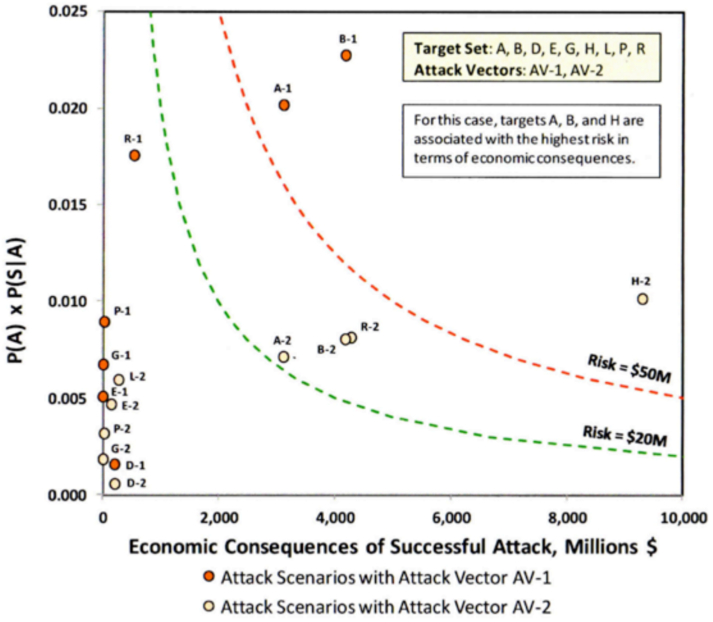
At the bottom of each of these four alternatives, indicate the chance (anywhere from 0 and 100%) that it will be the one chosen?

Probability that preparation for attack concludes successfully, resulting in attack initiation	0.1	0.5	0.3	0.7
Probability that, if attack initiated, it will successfully defeat target defenses	0.9	0.3	0.5	0.1
U.S. loss of life if attack defeats target defenses	1,000	400	50	20
Economic damage to U.S. if attack defeats target defenses	1 Billion	50 Million	200 Million	5 Billion
	5	80	15	0

Total: 100

18

Figure 10. USACE Common Risk Method



For this case, targets A, B, and H are associated with the highest risk in terms of economic consequences.

Figure 11. USACE CRM-D Display of Conditional Likelihood and Economic Consequences

Annex D.2 Standard Questions for Federal Tool Developers

- What is the name of the method or tool and who developed it?
- Who is the intended user, both type of organization and type of individual employee(s) or subject matter expert?
- What classes of hazards or threats are addressed? Is climate change included?
- Are interdependencies with other systems included, e.g., supply chain, infrastructures, etc.?
- What types of assets of systems are included? Physical? Cyber?
- How are risk and resilience measured or estimated? What, if any equations are used, e.g., Risk = Threat Likelihood x Vulnerability x Consequences?
- Does the process or tool evaluate risk-reduction or resilience-enhancement alternatives explicitly? If so, what form does this analysis take and how is this value expressed, e.g., benefit/cost ratio, return on investment?
- What is the direct output of the analysis? Please show examples as screen shots or reports.
- How widely used is the process and by what types of organizations?
- How would we go about obtaining a copy of the process or tool for review?

Annex D.3 Participants in Survey

January 20

Alice Lippert, DOE
Amy Rue, DHS
Andrew Janca, FEMA
Ann Kosmal, GSA
April Salas, DOE
Brian Beisheim, FEMA
Brian Scully, DHS
Chris Coleman, DHS
Dan Schultz, DHS
Enrique Matheu, DHS
Eric Rollison, DOE
Jerry Brashear, NIBS/Brashear Group
John Snyder, DOT/ICFI
Josh Borenstein, USDA
Sam Higuchi, NASA
Laura Wolf, HHS
LeeAnne Jackson, FDA/HHS
Matthew Weese, DHS
Michael Bowen, DHS
Mike Savonis, DOT/ICFI
Nathan Tatum, HHS
Nohemi Zerbi, DHS
Obi Ikeme, DHS
Paula Scalingi, NIBS/ Scalingi Group
Richard Alt, DHS
Susan Stevens, DHS
Jim Chung, USDA
Joe Reale, USDA
Bill Cummins, DHS
Michael Runestad, DHS
Todd Spangler, DoD

January 28

Brian Conaway, TSA
Gerald Delrosario, USCG
Gitanjali Borkar, DoT
Jim Taylor, TSA
Jerry Brashear, NIBS/The Brashear Group
Joseph Dove, TSA
Libby John, TSA
Ruben Yabut, DoT
Ryan Owens, USCG
Tim Reilly, TSA

Other

Christopher Duvall, DHS
Yasmin Seda-Sanaberia, USACE
Dan Schmelling, EPA
J. Darrell Morgeson, IDA

Appendix E.
CISR Risk Management Process Design

In developing design objectives, the project team reviewed the national goals and overall design objectives drawn from the policy guidance of the NIPPs and related CISR documents, considered the stakeholders' objectives and constraints, reviewed the key decisions implied by these objectives and their requirements, and then laid out a series of specific design objectives. These are presented in more summarized form in sections 5 and 6 of the body of the report.

E.1 Overall Design Principles

The overall Design Principles are enunciated in the NIPP and DHS doctrine, stating that an acceptable CISR-RMP must be:

- Practical and as simple as possible so that both the process and its results may be fully understood by non-professional analysts and decision-makers and can be carried out by extant staffs of lifelines, local governments and partnerships if they so elect.
- Holistic relative to unity of effort in engaging and coordinating all the lifelines, local governments and P3s initially and other groups later, e.g., other CIs, business and industry and civil society;
- Documented and transparent so that the method, data, assumptions and judgments may be examined, critiqued and adjusted as necessary;
- Reproducible so that analytic reliability (analyst-to-analyst repeatability), consistency and comparability can be established and maintained across analysts, time and organizations;
- Adaptable relative to changing conditions and customizable as to security and resilience enhancement options; and
- Defensible so that it is free of defects relative to the relevant professional disciplines and areas of uncertainty in the results can be readily identified and examined.

To these, we added: Integratable with existing business processes to encourage regular consideration of security and resilience in routine management decision-making. The CISR-RMP must be compliant with the Critical Infrastructure Risk Management Framework as explained in NIPP 2013 and detailed in the Supplemental Tool and meet the "NIPP Core Criteria for Risk Assessment" provided in NIPP 2009, Appendix 3A, which is reproduced verbatim as Appendix 2 to this report. This last set of requirements is included because it is both fully consistent with the later documents and in some cases, more specific as to the desired metrics and directions. Where any exceptions are taken from these guidelines, they are explained and justified.

E.2 The CISR Risk Management Process Goal

The CISR Risk Management Process Goal follows from the policy guidance of the PPDs and the latest NIPP:

Goal: Rational regional CISR management: resource allocation and evaluation. The goal of a CISR Risk Management Process is *to enable localities, lifelines, and other critical infrastructure and service* *providers to cooperatively assess all-hazards risk of loss and disruption to services, to rationally allocate available resources to initiatives that advance CISR as much as possible under constraints, and to evaluate the effectiveness of these initiatives*.

This report defines "rational" resource allocation as obtaining the maximum net benefits (i.e., maximum reductions in risk and/or fragility) to the owners and the community within available financial and analytical resources and other constraints. Rationality here is understood to be, in the phrase coined by Herbert Simon (1957), "bounded rationality"—goal-directed and "optimizing" but only within human limits, available information and processing capacity. True optimization is unfeasible in this area, due to the need to balance priorities, major uncertainties, limited analytical resources and political realities. Rational resource allocation, on the other hand, means to allocate available resources to options projected to yield the highest levels of net benefit possible given these and financial constraints. Generally, that requires fully quantitative methods leading to net benefit/cost or return-on-investment analysis, both of which require that risk, resilience and the benefits of improving them be measured using ratio scales, preferably converted to dollars. Rationality in management of CISR also requires regular and systematic performance evaluation of outcomes of options chosen, resourced and implemented, with appropriate actions based on the evaluations.

E.3 Design Objectives

The desired CISR management process should include the following minimum functions and features, as integrated into a whole that meets the policy guidance and NIPP analytical principles. These functions and features meet the design objectives— organization, cooperation and a simple but substantively rigorous process:

a. Methods for assembling and motivating lifeline operators and senior management, state and local officials and P3s (where they exist) to commit personnel time and information to a regional CISR management process. This process, with suitable safeguards, will entail each member conducting its own thorough CISR analysis and sharing limited information about their risks with those with whom they are interdependent and local government. Information sharing must be done according to an enforced, formal, legally vetted protocol to protect against unauthorized use or release of data. This function may include workshops, tabletop exercises and organizing P3s where they do not already exist.

b. A systematic methodology to articulate and prioritize (apply logically consistent weights to) locally defined goals and objectives relative to resilience, security and other important goals of the organization, agency, partnership or community, e.g., environmental sustainability, social and spatial equity, economic growth and development. Usually this entails use of Multi-Attribute Utility Theory (MAUT) (Keeney and Raiffa, 197) or Analytic Hierarchy Process (AHP) (Saaty, 1980).

c. Clear definitions of all important terms and their measurement in ratio scales.[31] Ratio scales of measurement are defined as having equal intervals (i.e., the distance between 1 and 2 is the same as the distance between 99 and 100) and a true zero (the absence of the quantity). These scales permit the full range of mathematical functions (e.g., can be added together or divided legitimately) and are

[31] Restricting the key terms of the risk/fragility analysis may be the most controversial aspect of the CISR-RMP design. There are a number of reasons for this that are explained in context.

clear in their meaning across users, systems, and organizations. In this case, the minimum requirement for risk/fragility analysis is that ratio scales.

Ratio-scale metrics are contrasted with interval scales (equal intervals, but no true zero, such as measurements of temperature in Fahrenheit or Centigrade) and ordinal scales (direction of magnitude, but neither equal intervals nor zero), and nominal scales (categorization without direction) (Stevens, 1946). Interval scales are seldom seen in risk analyses because essentially all the relevant variables -- threat likelihoods, vulnerabilities, most consequences, benefits and costs – all have a natural zero points and can be measured using equal intervals. Nominal scales are used only to classify, so are not useful in risk measurement except for incidental classifications, e.g., man-made versus natural hazards.

Many risk methods, however, in an attempt to simplify, use ordinal scales, such as low-medium-high-very high or green-yellow-red. Even when these are "quantified" by converting these to, say a 1-4 or 1-10 scale, or more gradations are used, they are fundamentally still ordinal scales. There is no assurance that all the intervals are equal and there is no true zero point. Only by *assuming* equal intervals and zero can ordinal scales be used for statistical calculations of means, standard deviations, etc., or used in benefit/cost or return on investment calculations. Ordinal-scale methods for CISR run significant risk of distorting decisions because they necessarily compress the scale of measurement where both consequences and likelihoods vary by *several orders of magnitude*. This is especially the case in the very largest consequences and the very smallest likelihoods – that is, where very unlikely events have disastrous consequences, the case where the most discriminating risk analysis pays off the most – ordinal scales collapse vastly different quantities into single categories – consequences in the "greater than" top category and likelihood at the "less than" bottom category.

Ordinal scales are often displayed as matrices of likelihood vs. consequences, usually with colors – "heat charts" – indicating urgency for attention or action, but not permitting calculation of value for resource allocation beyond possible movement among categories. With ordinal risk, calculating benefits as the difference between the risk with and without an improvement option cannot meaningfully be done, nor can the difference be divided by costs as in a benefit/cost ratio.

L.A. Cox calls these methods "worse than useless…[even] worse than random" (Cox, 2008a). D.W. Hubbard summarizes his review of ordinal risk analysis in the words of a security expert and client: "Garbage times garbage is garbage squared" (Hubbard, 2009, p. 131). Although very widely done, using ordinal scales in risk analysis (beyond initial screening) must be seen as a "significant error" relative to the standards of NIPP 2013, its Supplemental Tool and the specifics provided in NIPP 2009 (see Appendix A).

In the early phases of a risk analysis, however, it is often useful to "pre-screen" or "top-screen" assets or threat-asset pairs to focus analytic attention on the most important. Ordinal scales can be a quick and efficient means for doing this.

d. Measurement of threat likelihood, vulnerability and consequences consistent with directions in NIPP 2009, Appendix A, except for the allowance for using "conditional risk" (assuming threat likelihood is 1.0) for man-made threats. No conditional risk can be acceptable because of the orders of magnitude differences among man-made and all other hazards. These definitions are consistent with the DHS Risk Lexicon (2010) and broadly understood.

e. An explicit, detailed management process engineering step-by-step description of the flow of information, analyses (including minimum requirements for the tools to carry them out) and decisions from the beginning of one pass through the process – including all three key decision cycles (below) to the beginning of the next, the objective being to raise the levels of security (reduce risk) and resilience (reduce fragility). Risk and fragility are the core measurements of the process and their reduction constitutes the benefits of the options that lowered them. The three key decision cycles are methods for estimating the levels of risk and fragility under the three conditions required for rationality as defined above:

   i. *Baseline risk/fragility estimation* assumes that no action is taken to mitigate risk and/or fragility. Expected[32] risk and fragility levels permit identifying and prioritizing which specific assets or facilities and which specific threats will be included in more detailed analysis and provides the baseline for comparisons with conditions as modified by CISR improvement options. These risk levels may be interpreted as the "expected cost of inaction."

   ii. *Option valuation* re-estimates risk and fragility assuming specifically defined mitigation options are implemented. The difference between risk and fragility levels with the option(s) in place and the baseline without them is the expected benefit of the option(s). This difference can be interpreted as "expected savings" of lives, dollars, etc. This analysis allows rational resource allocation by selecting the options with greatest benefits, net of the costs of the options.

   iii. *Effectiveness assessment* is measurement whether the options that were selected were implemented as planned and whether they actually achieved their outcomes objectives. Comparing this level of risk and fragility with the first condition describes how much CISR has been improved and comparing them to the second set describes how well the options performed relative to their specific improvement objectives.

   This process must be simple and intuitive enough that existing employees of the lifelines and local governments can carry out the process themselves, as opposed to outside risk experts, with a modicum of training and technical assistance if they so choose. It must be kept simple so that its results can readily be explained to busy decision-makers and their questions can be answered definitively and quickly.

f. A key design objective is to make the estimates of risk, fragility, benefits and costs consistent and directly comparable across sectors. In the words of the NIPP Supplemental Tool, "Common definitions, scenarios, assumptions, metrics and processes can ensure that risk assessments contribute to a shared understanding among critical infrastructure partners." (2013, p. 7.) This shared understanding enables:

   - Comparing across divisions of a large organization for rational resource allocation,
   - Measuring progress of project and local programs over time and against objectives,
   - Enabling the cross-infrastructure information sharing for necessary for interdependency analysis,

[32] "Expected" here and in the following is used in the statistical meaning of "probability weighted," e.g., the expected value of something is its value times its likelihood or frequency of occurring, not that it is anticipated. Technically, it is the arithmetic mean of the distribution of an uncertain value of the something, or its long-term average.

- Facilitating higher level budget and rate-setting authorities to better understand and appreciate investments in CISR,
- Allowing community representatives to understand the analytical results in context,
- Permitting functional aggregation: asset to facility to system to regional system-of-systems,
- Supporting mathematical aggregation for upward reporting for state and federal program management and other cross-cutting uses (e.g., aggregating across jurisdictions, by types of hazards, etc.) for policy-making and R&D planning,
- Providing a basis for allocating and managing state and federal grants to advance CISR,
- Permit reporting of progress by national CISR programs, and
- Possibly, providing a scale for bond-rating agencies, insurers and re-insurers and future infrastructure banks and other investors to provide incentives or make investments.

To meet the overall goals and objectives of the CISR-RMP it is necessary to adopt fully quantitative (ratio scale) measures for risk, fragility, benefits and costs, generally all converted to dollar amounts, but, in the case of human casualties, also reported in natural terms to keep them foremost in decision-makers deliberations. Consequences not conducive to quantification such as psychological impacts, confidence in governments, environmental impacts are described in ordinal scale terms for display in decision-making, with later ratio quantification desirable.

g. Methods for analyzing risk and resilience of cyber and physical-cyber systems used by the lifeline CIs, especially in operational controls.

h. Means of defining dependencies and interdependencies of individual CI systems with other CIs and regional interactions to identify and quantify the risks and fragility they impose and the means to explicitly integrate them into the risk/resilience analyses of each CI and the consideration of the regional coalition.

i. Models or procedures to estimate the impacts of disruptions to lifeline CIs on regional economic activity (gross regional product) and, ideally, on individual industries, wages, jobs and local income and sales taxes. Ideally, this model would use the estimated fragilities and interdependencies as input and return the desired regional scale metrics.

j. Means for generating options for consideration in reducing risk and/or fragility. This could include best practices in the industry, engineering or architectural solutions, new security protocols, added surveillance equipment, etc. These should be well enough defined to support estimates of the changes in threat likelihood, vulnerability, consequences and/or outages that the options would cause and to estimate the life-cycle and initial budget costs. Costs should be adjusted to after-tax terms for for-profit organizations.

k. Methods for calculating the value of options that can be integrated with the users' standard approaches to planning and budget decision-making. Options are best valued as net benefits – gross benefits (the reduction in risk and/or fragility attributable to an option) in dollars less life-cycle costs, both in present value dollars[33]—because that is the amount the organization or region is better off. In addition, some decision-makers are interested in the efficiency by which the benefits are created. In this case, the benefit/cost ratio (B/C) or the return on investment (RoI) is useful, especially as a "tie-breaker" between options with comparable net benefits. It is an error to allocate resources only by efficiency measures unless there is no resource constraint; to do so may lead to decision-makers to overlook the most valuable, if less efficient, options.

l. Means for displaying results for decision-makers at each point where decisions are called for. "Dashboards" have come to mean virtually any computer-monitor summary of results and options for decisions. Designing these displays requires great care because it is difficult to make decisions if too much detail is shown. If possible, capabilities should be designed in to permit the "drill-down" (to display underlying detail) and the "what-if" (quick, preferably real-time analyses to allow decision-makers to experiment before taking decisions). These features are not simply conveniences, but can be essential to building decision-makers' confidence in the process.

m. Means of monitoring the implementation of the programs and investments selected for cost, schedule, process operations, and the quantity and quality of outputs for accountability.

n. Methodologies for evaluating not only the outputs of the chosen programs and investments but their direct and impact *outcomes* – how much the programs and investments have actually improved the levels of resilience and security – that is, reduced fragility and risk – and how well they performed relative to their projected benefit objectives, with corrective actions as required. This would include analysis of actual events that occur, various exercises and analytical processes to gauge progress.

o. Systematic processes for aggregation, summarization and visualization of analytical results and decision options to support explanations and decision-making by senior executives and representatives of the general public; and for reporting to higher levels of the organization and/or higher levels of government, with appropriate safeguards for privacy and sensitive, confidential and classified information; this information would provide "bottom-up" data for addressing regional and National issues to complement the conventional "top-down" national reviews.

p. Provisions to routinely address both owners' and communities' security and resilience, respectively, to support recognition and discussions of shared benefits, externalities, public goods, regional development, etc.

Typically, critical infrastructure risk analysis follows one or the other of two disciplines: the first, as taught in business schools, is an application of operations research to the microeconomics of the firm. It seeks to find the set of options that will most benefit the firm, after costs, so it acknowledges only the cash flows captured by the firm – direct losses, direct costs of repair or replacement of damaged assets, direct liabilities for casualties, lost revenue while down, etc., as appropriate for a firm. The other is an application of welfare economics that seeks to minimize the lost welfare to the public at large, so it looks to the public benefits of risk and fragility reduction – impacts on the regional economy, lost jobs and wages, all human casualties, longer term impacts, etc. The mathematics of the

[33] Present value dollars are cash or cash equivalent in- or out-flows that occur in the future, discounted to their value at present based on the time value of money. Discount rates can vary for a number of reasons, but should not be less than the borrowing costs of the enterprise. Discount rates should *never* be used as a surrogate for risk.

two is identical, but they focus on very different decision-makers and recognize consequences as appropriate to the respective decision-makers.

Lifeline infrastructures, however, bear the public trust of providing life-essential services to the community as well as sustaining themselves financially, so they should examine not only the risks, fragilities, benefits and cost to their enterprise, but also to the community as a whole. Moreover, because lifelines are ubiquitous, they benefit directly and indirectly from operating in a more secure and resilience region. Both sets of calculations should be presented in protected form so that the community can identify where the CIs cannot be expected to invest but where benefits to the public are substantial. For these, the community may provide incentives or seek outside funds.

q. Inclusion of all types of risk management options, including risk acceptance, risk transfer (e.g., insurance), all phases of primary preparedness (prevention, protection, mitigation, response and recovery), and all resilience strategies (e.g., robustness, redundancy, resourcefulness and rapidity), land-use zoning, building codes, growth and economic development plans and innovative architecture, engineering and construction practices.

r. Where feasible, integration of risk/resilience management with other, routine management processes, such as contingency planning, formal asset management, capital planning and budgeting and operational planning and budgeting. Such integration reduces the marginal cost of conducting the analysis and encourages routine risk/resilience decision-making in the context of the routine business functions.

These features together describe a complete and effective management process for managing lifeline critical infrastructure and regional security and resilience. Many other features can contribute to the process by such things as a fully integrated, seamless and automated process, integrated models that project threat conditions over time at specific locations, callable data bases of useful statistics, models that increase the accuracy of estimates of the variables going into calculations of risk and fragility, explicit treatment and display of uncertainties, geospatial information systems (GIS) displays and analysis, best practice surveys of CISR improvement options, etc. While each of these may very well improve quality or efficiency of the process, they are *not* essential to rational CISR management. Their contributions can be gauged only in the context of the overall management process and the extent to which they might cause different options to be selected from those selected by the process without them.

It is important to consider the preceding design objectives as parts of an integrated system, a management process that flows from initial organization through to the continuing evaluation of measures taken to advance CISR and the start of a new analysis cycle. Minimum workable elements in each, integrated through a comprehensive field-based process will move the NIPP approach from five chevrons with explanations to a complete system in which the elements are expected to be iteratively reviewed, enhanced and upgraded routinely. It is vastly more important to get the process working as a system that can mature over time than it is to perfect individual elements above a minimally workable level. As this construction proceeds, the priorities for improving elements and the specifications for those improvements and/or new elements will become evident and can then be addressed.

E.4 CISR Risk Management Process Design

Figure E.1 expands on Figure 4 from the body of the report and is, itself, expanded still further in Attachment 2 (repeated from the body of the report at the end of this appendix). Each shows the same process at different levels of detail. There is a one-to-one correspondence among these figures and figures 3 through 5 in the body of the report. In all, the upper, green portion is the process as carried out by individual enterprises, whether they are private corporations, a public utility authority or a government agency charged with a CI or emergency mission, or non-CIs if they desire to participate. The number of such enterprises would vary based on the nature of the region and the willingness to participate. The blue portion of the figures is the process as carried out by a voluntary regional coalition made up of the participating enterprises and the local governments at the governance/executive management level. In the absence of a volunteer coalition, local governments or councils of governments may be able to carry out many of these functions, but the active participation of the lifeline CIs should be the top priority of any jurisdiction initiating a CISR program. The general flow of the process within any level in the charts is top-to-bottom and left-to-right; these flows are implied (not connected by arrows) to keep the figures legible. The few explicitly shown flows between phases or levels are necessary instances of information sharing. Although not part of the project's statement of work, a higher level of government—state, federal or a combination, shown on the orange field – that would set policy and facilitate the process was presented in section 5.D. of the body of the report.

This Appendix sketches the design of the CISR-RMP for the enterprise and regional levels only. A CI or other organization, local government or a civic association can initiate the process. This discussion outlines the primary elements in each of the NIPP 2013 "chevrons." These elements are usefully thought of as "phases" in the process, made up of "steps" which are summarized in Figure E.1, with some combining and abbreviating and fully displayed in Attachment 2. While this process is expressly designed for critical infrastructures – especially the lifelines – local governments and regional CISR P3s, virtually any organization seeking to advance its security and resilience could use it. If successful with its intended user organizations, the process could be used in a regional program that includes other elements of the community, e.g., business, industry, civil society, schools and hospitals. In the following, the word "enterprise" should be read to indicate any organization undertaking to participate in a rigorous security and resilience enhancement program through this process. They may be CIs or non-CIs, public or private, for profit or not-for-profit. It is useful to start the description with the regional level.

In the discussion below, the order follows a general left-to-right sequence, but moves between the enterprise and regional levels in an order that follows the primary workflow.

R1. Regional Goals & Objectives organizes the stakeholder coalition (or uses an existing P3 or cross-sector collaborative body) – through a series of meetings (in person and virtual), tabletop exercises and other activities, determines multi-stakeholder requirements for information sharing, including protection of sensitive and proprietary data, regional goals and objectives and the threats and hazards the coalition is most concerned about. Creation or leveraging of an existing public-private-non-profit partnership or other collaborative mechanism may prove the most expeditious approach to forming an able and vigorous P3. The mere existence of a P3 directed toward regional security and resilience by reducing vulnerability to interdependency is often its own incentive to participate.

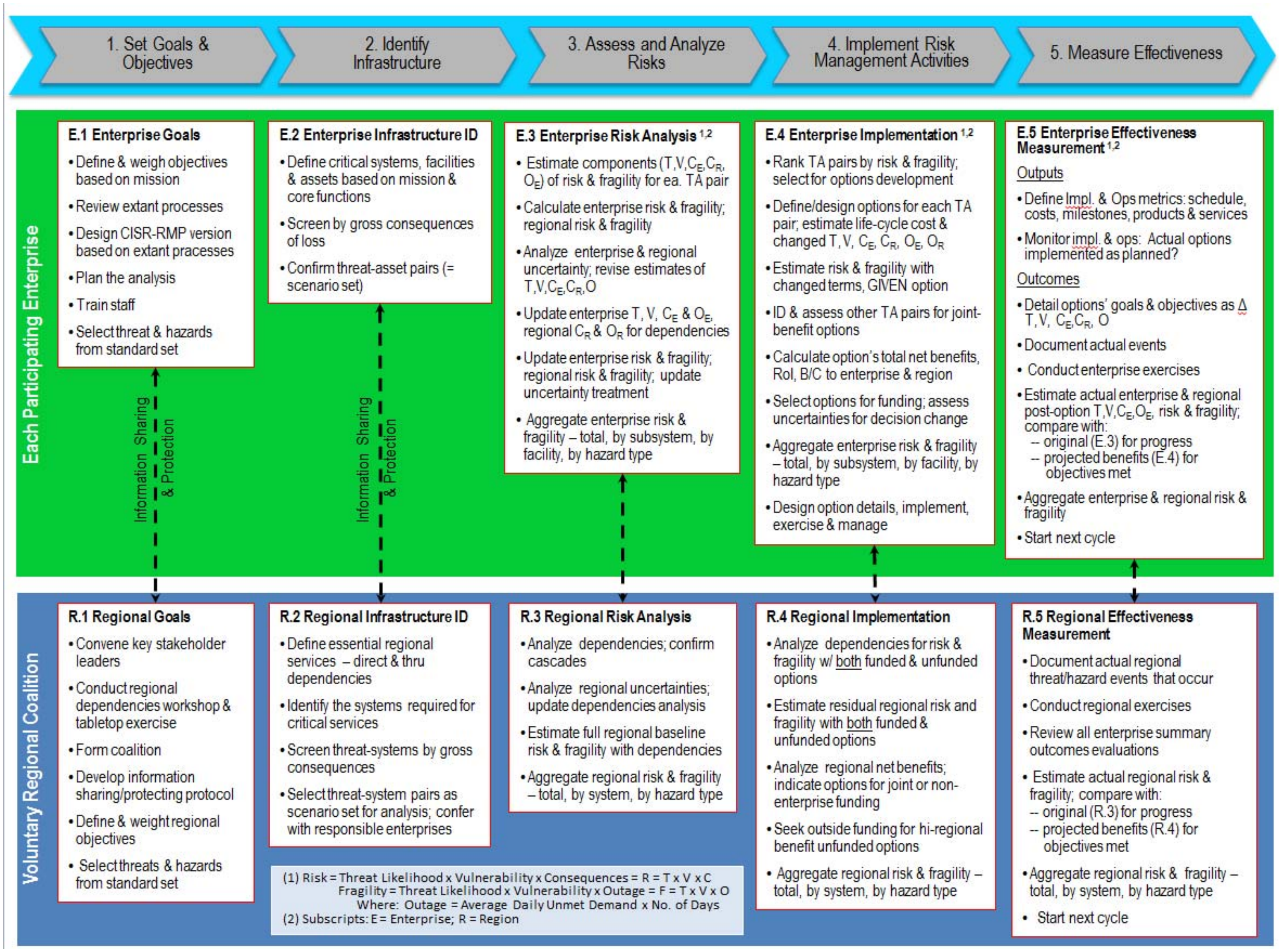
Convene key stakeholder leaders – This first step brings together a core group from among senior operators and managers responsible risk, emergency management, or continuity for the lifeline CIs and local governments in the region, representatives of key state agencies, significant community groups and federal agency representatives from DHS/IP and FEMA, but possibly also DoE, EPA, NOAA and USGS. Local emergency managers must be included, but should seldom lead the effort because they tend to focus on emergency preparedness to the exclusion of all other options – and to be deferred to by others in doing so. At this point, it is important to keep the scope of possible actions as broad as possible. The meeting is to outline the overall approach and invite participation in a workshop on CI dependencies and interdependencies.

Conduct one or more regional interdependencies workshop & tabletop exercise – A larger group including key staff to these executives becomes involved in the planning and carrying out of regional interdependencies workshops and ultimately whole-region tabletop exercises. The point of these is to demonstrate the near universal vulnerability to dependency on the goods and services from outside most organizations and the extent to which CI or supplier interruptions in services are passed on to their customers and their customers' customers through cascading impacts. Having experienced the complexity and counter-intuitive connections of interdependencies, local leaders become typically very interested in taking proactive steps to reduce these impacts. If regional stakeholders do not already have an existing coalition, as they realize that they have experienced only one or two of potentially hundreds of such events, they will see the need for an active, sustainable P3.

Form the coalition – This step consists of formally or informally organizing the coalition or P3, the members of which will be expected to conduct their own security/resilience analysis, to share some of the information through negotiated and secure channels, and to contribute staff time and/or funds to the expenses of the coalition. As the P3 is being formed, it is useful to define the geographic boundaries of the region. The service areas of the respective CIs included will influence this definition. The U.S. Census defines metropolitan and micropolitan areas based on the counties where the commuting patterns of working people are most intense. While not absolutely necessary, aligning the geographic boundaries of the community to be analyzed with county borders makes a great deal of useful information available because it is collected and stored by county.

Develop an information sharing/protecting protocol – A formal, legally vetted information sharing and protection agreement binding all organizations and individuals involved directly with handling or using risk and fragility data will be necessary if the information about dependencies and interdependencies is to be shared. To discover and address a risk of a supplier's disruption requires at least knowledge of the circumstances that brought it about (the threat event and likelihood to the supplier) and the supplier's estimated outage severity and duration. This is extraordinarily sensitive information for a number of valid reasons. It will not be shared without a clear, secure information sharing process and significant penalties for unauthorized releases. Well-defined and enforced protocols for cross-sector two-way information sharing and data handling in support of regional interdependencies analysis and community decision-making are essential to obtaining the participation of the respective lifelines. This entails bringing together local and state agencies with and lifelines and other critical infrastructures to agree on *formal*, legally vetted procedures and mechanisms for sharing agreed types of data and for handling sensitive and proprietary information. A "tiered" system can enable disseminating appropriate levels of information and risk assessment results among lifelines, with partner localities, and the public to incentivize and promote

Figure E.1. NIPP 2013 Framework & CISR Risk Management Process -- Enterprise & Region



1. Set Goals & Objectives

2. Identify Infrastructure

3. Assess and Analyze Risks

4. Implement Risk Management Activities

5. Measure Effectiveness

Each Participating Enterprise

E.1 Enterprise Goals

- Define & weigh objectives based on mission
- Review extant processes
- Design CISR-RMP version based on extant processes
- Plan the analysis
- Train staff
- Select threat & hazards from standard set

E.2 Enterprise Infrastructure ID

- Define critical systems, facilities & assets based on mission & core functions
- Screen by gross consequences of loss
- Confirm threat-asset pairs (= scenario set)

E.3 Enterprise Risk Analysis [1,2]

- Estimate components (T,V,C_E,C_R, O_E) of risk & fragility for ea. TA pair
- Calculate enterprise risk & fragility; regional risk & fragility
- Analyze enterprise & regional uncertainty; revise estimates of T,V,C_E,C_R,O
- Update enterprise T, V, C_E & O_E, regional C_R & O_R for dependencies
- Update enterprise risk & fragility; regional risk & fragility; update uncertainty treatment
- Aggregate enterprise risk & fragility – total, by subsystem, by facility, by hazard type

E.4 Enterprise Implementation [1,2]

- Rank TA pairs by risk & fragility; select for options development
- Define/design options for each TA pair; estimate life-cycle cost & changed T, V, C_E, C_R, O_E, O_R
- Estimate risk & fragility with changed terms, GIVEN option
- ID & assess other TA pairs for joint-benefit options
- Calculate option's total net benefits, RoI, B/C to enterprise & region
- Select options for funding; assess uncertainties for decision change
- Aggregate enterprise risk & fragility – total, by subsystem, by facility, by hazard type
- Design option details, implement, exercise & manage

E.5 Enterprise Effectiveness Measurement [1,2]

Outputs

- Define Impl. & Ops metrics: schedule, costs, milestones, products & services
- Monitor impl. & ops: Actual options implemented as planned?

Outcomes

- Detail options' goals & objectives as Δ T,V, C_E,C_R, O
- Document actual events
- Conduct enterprise exercises
- Estimate actual enterprise & regional post-option T,V,C_E,O_E, risk & fragility; compare with:
  - -- original (E.3) for progress
  - -- projected benefits (E.4) for objectives met
- Aggregate enterprise & regional risk & fragility
- Start next cycle

Information Sharing & Protection

Information Sharing & Protection

Voluntary Regional Coalition

R.1 Regional Goals

- Convene key stakeholder leaders
- Conduct regional dependencies workshop & tabletop exercise
- Form coalition
- Develop information sharing/protecting protocol
- Define & weight regional objectives
- Select threats & hazards from standard set

R.2 Regional Infrastructure ID

- Define essential regional services – direct & thru dependencies
- Identify the systems required for critical services
- Screen threat-systems by gross consequences
- Select threat-system pairs as scenario set for analysis; confer with responsible enterprises

R.3 Regional Risk Analysis

- Analyze dependencies; confirm cascades
- Analyze regional uncertainties; update dependencies analysis
- Estimate full regional baseline risk & fragility with dependencies
- Aggregate regional risk & fragility – total, by system, by hazard type

R.4 Regional Implementation

- Analyze dependencies for risk & fragility w/ both funded & unfunded options
- Estimate residual regional risk and fragility with both funded & unfunded options
- Analyze regional net benefits; indicate options for joint or non-enterprise funding
- Seek outside funding for hi-regional benefit unfunded options
- Aggregate regional risk & fragility – total, by system, by hazard type

R.5 Regional Effectiveness Measurement

- Document actual regional threat/hazard events that occur
- Conduct regional exercises
- Review all enterprise summary outcomes evaluations
- Estimate actual regional risk & fragility; compare with:
  - -- original (R.3) for progress
  - -- projected benefits (R.4) for objectives met
- Aggregate regional risk & fragility – total, by system, by hazard type
- Start next cycle

(1) Risk = Threat Likelihood x Vulnerability x Consequences = R = T x V x C
Fragility = Threat Likelihood x Vulnerability x Outage = F = T x V x O
Where: Outage = Average Daily Unmet Demand x No. of Days
(2) Subscripts: E = Enterprise; R = Region

resilience improvements. In metropolitan areas, regional fusion centers can be a focal point for this process, and leverage information-sharing procedures already developed with CI partners. *(Note: Best practices in information sharing protocols need to be identified and a model approach developed, ideally with federal assistance.)*

Define & weight regional objectives **–** Of the two most widely recognized and used methods for defining and weighting goals and objectives relative to one another, Multi-Attribute Utility Theory (MAUT) and Analytic Hierarchy Process (AHP), the latter is preferred because it is intuitively simpler to novice users; accepts values measured on ordinal, interval or ratio scales and converts them to ratio scales; allows cross-organizational comparisons; and links readily with budget optimization software. AHP deconstructs broad overall objectives into a hierarchy of lower level, more measurable objectives, and then establishes weights among them through a systematic pair-wise comparison process. This results in numerical weights that sum to unity. Addition or subtraction of new goals or objectives causes AHP to automatically adjust all others to maintain this total, making the process conducive to use in budget making. For all these reasons, AHP has been gaining in use and academic respectability, especially among engineers, although it remains controversial among micro-economists and decision scientists. The reasons for their reservations are technical an actually make AHP more useful in this context. The methodology is used by the regional coalition and by the enterprises, respectively, although, of course, the content may be quite different.

Select threats and hazards from a standard set – The methodology for this step is the same for enterprises and regional coalitions. For comparability to be assured, it is necessary to start with the same set of threats and hazards. The basic set would have been developed by DHS in consultation with other agencies and Sector Coordinating Councils. The criteria for inclusion should be that as a set, they constitute a mutually exclusive and collectively exhaustive set of events (given the assumption that "nothing major and negative happens" is the event that complements the named events). The threat and hazard events include man-made threats, including specific acts of terrorism, crime and vandalism; major natural hazards; technological accidents and asset deterioration due to age or usage loads in excess of design; proximity threats created by risky neighboring facilities; and dependency threats of outages for lack of utilities, employees or essential supplies.

Enterprises and coalitions begin with this basic set and may add or delete from it as needed to capture the threat and hazard conditions they face. Additions would mostly be for unusual local conditions (e.g., avalanche, mudslides, volcano eruptions) that might not be on the initial standard list because of their rarity. Deletions would mostly be for events that are impossible (e.g., submarine attack in a desert) or because they would have negligible consequences. The adapted list for the region and those for the enterprises should be as consistent as reasonable because the selected threats and hazards will play a large role in the interdependencies analyses later in the process.

NOTE: For natural hazards, DHS, in collaboration with the appropriate federal agencies and independent scientists, could develop a tool that would ease natural hazard characterization and improve consistency. In most cases, a federal or occasionally state agency keeps historical records of such major natural events such as earthquakes, hurricanes, wildfires, etc., differentiated by location with at least frequency and severity. A standard tool would take location as input and return a complete suite of standard natural hazards, with severity (load) levels and frequencies for each severity level. This tool could also allow a standard adjustment for climate change based on an approach similar to that used in U.S. DoT's CMIP climate change projection model, discussed earlier, for downscaling diverse large scale climate projections to local conditions. Climate change itself would be captured in terms of the specific threats relevant to the assets in the analysis, e.g., hurricane severity and frequency in the eastern U.S. and drought and heat in the west. The model would access the appropriate databases and make whatever standard calculations are necessary to make the information directly useful in conducting the analysis of these hazards, which historically have had impacts that dwarfed virtually all the others. Some gradually worsening climate change threats such as sea level rise and prolonged drought would require the analysis be conducted across time intervals and considered as a series.

E.1 Enterprise Goals and Objectives phase is very similar to the corresponding regional phase just discussed, consisting of planning and organizing the CISR management process for the enterprise, defining and weighing goals and objectives and selecting the threats and hazards to be included. The organizing and preparing is, of course, simpler in an organization where managers can assign personnel and other resources to the task. Many companies for whom real (i.e., non-financial) risk management is essential to their business model's viability, e.g., natural resources exploration and extraction, pharmaceuticals, have found it useful to establish a specialized unit to oversee, assist and maintain analytical quality and methodological consistency for comparability for decision-making. The personnel assigned to this unit are specially trained in depth in the methods to be used so that they can guide and help (and ultimately, approve) the risk analyses by engineering and operating personnel.

Phase E.1 differs from the R.1 in that it also includes a review of the enterprise's existing business processes with possible relevance to risk/resilience analysis – e.g., business continuity planning, asset management, capital development planning and budgeting, operations planning and budgeting. These processes are documented and analyzed for ways that they might be adapted toward the model CISR-RMP described here. The basic notion is to establish the model process in ways that are initially minimally disruptive and relatively easy to integrate fully with the existing processes to become an inherent part of the enterprise's routine. Instead of risk management being a periodic "special event," it becomes a continuing element in proper management.

E.2 Enterprise Infrastructure Identification *and* ***R.2 Regional Infrastructure Identification*** are very similar, except for the scale of the items being considered: the enterprise considers assets at a finer scale than the region. The enterprise begins with consideration of the vision and mission statement of the organization – the reason for its existence – and then identifies the core functions that are essential to this mission and the systems, facilities and assets essential to performing the function. The goals and objectives of the enterprise from earlier can assist in this task. The facilities and systems that are essential to carrying out the organization's core functions are the initial list of "assets" (used generically to include system, facility, machinery, personnel, etc.) to be considered for analysis. Both physical and cyber systems, especially those for process control and key business systems (e.g., billing and accounting), are included in this analysis. If the enterprise has previously used other risk or vulnerability approaches, their results can usefully cross-verify the list built from the core functions. Assets will be screened to a workable list in the next step, so at this stage, the user should be biased toward inclusion rather than exclusion of assets.

The regional coalition begins with considerations of the services that are essential to the survival and effective functioning of the regional community, both directly and indirectly. For example, a community would identify electricity distribution as essential directly, while electricity generation and transmission are essential indirectly. The previously defined regional goals and objectives should be consulted when defining the essential services.

This initial list is then “top screened” through a two-step process. This screening and the resulting shortlist of assets and threat-asset pairs are necessary to manage “analysis fatigue” that an overly long list of assets can cause. Too long a list runs the chance of overlooking major risks that happen to come up later in the analysis because the analysts are fatigued. The size of the list is a judgment made in consideration of the scale and complexity of the organization and its core functions and the number of analysts and amount of time available for the analysis. Detailed analysis can be tedious and difficult to do for long stretches of time without breaks. It is important to identify the most important assets and threat-asset pairs to take them up first. The basis for this selection is the grossly estimated consequences (which are later estimated more precisely) relative to human casualties, dollar losses, major disruption to the mission and core functions, and major disruption to customers’ functioning. Other gross criteria may be added if desired.

The first screening is simply to estimate the gross impact of loss of the asset regardless of cause. A simple, but precisely defined ordinal scale may be used, e.g., one (no impact) to ten (existential catastrophe). The intervals may be unequal and the top category may be open-ended, because no calculations will be made on these estimates – only selections for the next step. The point is to make these estimates fast and easy to make. In making these estimates, the analyst should consider the role each asset plays in the system of which it is part; a relatively inexpensive asset with no casualty possibility could be a single point of failure for a system essential to the organizations core functions. When completed for all assets on the initial list, the assets are ranked by the magnitude of impact and those at the top are identified for the second screening. The others are not completely dropped from the process, but deferred for the present. They may be added back to the analysis if they are later found to be important or in later iterations of the overall process**.**

The short list of assets is then arrayed in a matrix against the previously selected threats and hazards. In each cell of this matrix, an estimate is made using the same or a revised rough ordinal scale collapsed across the categories of impact. A quick estimate of the gross consequences is made for each cell of the matrix, i.e., each threat-asset pair. The threat-asset pairs are then ranked by the magnitude of impacts and those with the largest impacts are selected for further analysis. Those not selected are deferred and may be included later in the analysis if desired or addressed in a later iteration of the process.

The selected threat-asset pairs are the working list of scenarios to be included in the analysis. The list should be examined for two concerns. The first is that it includes the threat-system pairs identified as critical by the regional coalition in its parallel considerations. These should be harmonized so that the interdependencies analysis has all the needed information. The second issue is whether the set of scenarios can be regarded as mutually exclusive—i.e., each scenario is definably different from all others—and collectively exhaustive—i.e., collectively they exhaust the possibilities of negative events that could cause extraordinary disruption or damage, all others being managed as “routine.” Essentially, this is an assumption that all other events will be negative but routine, neutral or positive for the enterprise. These conditions are necessary for aggregation at any level because they avoid double counting and under counting.

At the regional level, the process is the same except that the process begins with essential services needed for the community to survive and advance its goals and objectives and then identifies the systems that provide those services. Lifeline CIs are always among them, but other systems may also be identified, e.g., major industries, major upstream dam, healthy and educated workforce. These systems are ranked using the same two-step process as the enterprise process and results in a rank-ordered set of threat-system pairs. The coalition then confers with the enterprises responsible for the operations of these systems to assure that they are included in the scenario sets the enterprises are planning to analyze.

E.3 Enterprise Risk Analysis is the first of three analyticcycles, the others being estimation of benefits and evaluation of actual performance outcomes. For each threat-asset pair, risk and fragility are calculated from estimates of threat likelihood, vulnerability, consequences to the enterprise and the region, respectively, and outages to the enterprise and region, respectively. It is convenient to estimate consequences first because part of the definition of vulnerability includes consideration of consequences.

- ***Consequences*** to the enterprise (C_E in Figure 1) include the costs of liabilities for human casualties (both employees and the general public); repair and/or replacement of damage to the asset and other restoration costs, revenue loss (net of variable operating costs), environmental restoration, penalties paid under service reliability contracts and for environmental damage, and any other cash outlay due to the threat event; and any other dimension of interest to decision-makers, e.g., loss of strategic opportunity, damage to brand or reputation. Taxable enterprises should adjust these elements to after-tax values. Consequences to the region (C_R) include loss of life and serious injuries (estimated in natural units, deaths and serious injuries and the corresponding “statistical value of life” as defined by the coalition based on federal guidelines) and lost economic activity (estimated as the reduction in gross regional product caused by the event and associated outages), and repair/replacement costs borne by all affected parties. The enterprise can make only a limited, initial estimate of consequences to the region at this point because dependencies on the interrupted service cannot yet be included. These estimates will be refined in collaboration with the regional coalition.

  The working assumption in making these estimates is the “worst reasonable case” assuming success of an adversary or the full impact of the specified natural hazard. Mathematical models of the system that predict the damage from asset properties and event severity (which may itself be the result of a threat model) can be very useful in making these estimates. Many organizations have developed such models or have planning and control models that can be used in consequence analysis. If these are unavailable or inconvenient, the judgment of the employees who engineer, operate and maintain these systems is a completely valid alternative because their “mental models” may be more accurate and more accessible than the mathematical models. Even if more formal models are used, their results should be “gut-checked” by the staff engineering and operating staff of the enterprise.

- ***Vulnerability*** is the conditional likelihood that, given that the threat event happens, that the estimated consequences will result. In the case of adversary attack, this is the likelihood that the attack will succeed. In the case of natural and accidental hazards, vulnerability is the likelihood that the full consequences will result from the event. Vulnerability estimation begins with a review of the facility location, setting, design and construction, systems and layout, including any existing security countermeasures or protective systems or can be facilitated and made more consistent by the use of any of several tools, including fault- or event-trees, path analysis, vulnerability logic diagrams, computer simulations, etc.

- ***Threat likelihood*** estimation is relatively simple for natural hazards. If the notional DHS tool were available, the analyst would simply provide the location and the standard set of threats, with frequency by severity level, would be returned. If the tool were not available, guidelines would enable the user to look up the same information on line. Likelihood of asset failure due to aging or use beyond design loads can be estimated by the enterprise's engineers and often is, routinely, as part of the growing number of formal asset management systems in use, especially among utilities. Estimating proximity and dependency threat likelihoods would depend on information sharing with neighbors and suppliers. For man-made, volitional threats such as terrorism, crime and vandalism, the enterprise should turn to federal and state law enforcement, intelligence and homeland security sources. Normal crime and vandalism statistics should also be used. DHS has long maintained that terrorism likelihood will be provided through one or another route. This has seldom been done beyond broad, verbal descriptions of possible threats to specific types of systems and facilities. Such assessments are not helpful in conducting a quantitative risk analysis. At the request of the actual users, AWWA's J100 standards committee developed a "proxy" method for grossly approximating the threat likelihood of specific terrorist attacks based on a RAND-Risk Management Solutions interpretation of historical data, local alternative targets and the consequences and vulnerability of the specific asset. Explicitly, this method is described as a very rough "stand-in" until better estimates become available.

NOTE: DHS has expertise and access to information that would permit it to prepare and provide quantitative terrorism threat likelihood estimates, with uncertainty bounds or distribution, to critical lifelines and local agencies with need to know. The reluctance of the intelligence community to provide such estimates to the detriment of rational CISR rational resource allocation is a condition DHS should no longer accept. If it declines, it should prepare or confirm a "proxy" method that could be standardized across CIs and local agencies. This at least would allow CI and local governments to make comparable assessments and put terrorism likelihood into the correct order of magnitude. In virtually all individual assets, the likelihood is so small that an error of one order of magnitude (e.g., from 1 in 100,000 to 1 in 1,000,000) will seldom change resource allocation decisions. As matter stand now, however, users either completely disregard terrorism risk or severely over-estimate its likelihood.

- ***Outage*** is a special case of consequences made important by the critical nature of lifeline infrastructures. Estimating them imposes no additional effort because their elements have already been estimated. To estimate lost gross revenue, required as part of estimating the financial losses to the enterprise, it is necessary to estimate the average daily unmet demand, the number of days of unmet demand and the pre-event price of the goods or services produced. The product of these three terms is the lost gross revenue and also outage in dollar terms; the product of the first two is outage in units. Outage to the enterprise (designated O_E in the Figures) is distinguished from regional outage (O_R) because O_R includes the additional outages created by interdependencies across all enterprises in the analysis as reflected in full-interdependencies lost gross regional product.

For risk analysis to truly guide operating and investment decision-making, it must be well understood and trusted by busy senior decision-makers, many of whom have little or no direct experience with risk analysis of real (i.e., non-financial) risk. In organizations unaccustomed to risk analysis, it is usually necessary to start with single point estimates of all terms and the simple product form of calculating risk or fragility to build understanding and confidence in the process. This may lead to a false sense of certainty and introduce some degree of error, but more sophisticated risk methods are poorly understood and are highly likely to result in rejection of the method or simply compliant "going through the motions" without affecting decisions at all. For these reasons, the initial implementation asks only for single point "best" estimates. Once the process has been used for a short time, it can move to estimating some or all of these variables as ranges and then in probability distributions, both reflecting uncertainties. Such estimates make for a better analysis because they explicitly account for and display the uncertainty in the estimates. The difficulty arises from the need to combine them by Monte Carlo simulation, of which very few senior managers have experience or understanding. It has been a frequent experience among risk consultants that as organizations use simpler methods in on-going organizational processes, they begin to request enhancements that almost always include explicitly analyzing and reporting uncertainty. In the meanwhile, sensitivity analysis and decision-reversal analysis may be used to address uncertainty.

The next step in this process is to calculate risk for the enterprise and region and fragility for the enterprise for each threat-asset pair, followed by a limited sensitivity analysis of major uncertainties for the threat-asset pairs with the greatest risk of fragility. These analyses may suggest additional data or side analyses to improve the estimates for these important threat-asset pairs. Once the estimates are as "firm" as they can be at this point, they pass to the regional level for dependency analysis.

R.3 Regional Risk Analysis begins with dependency analysis. This requires an analytical model that simulates the principle dependencies, interdependencies and cascading effects. Each enterprise identifies its critical assets where other CIs are essential to operations and would fail fully or partially if the other CI failed. This interest is threat specific. The supplier CI would provide the likelihood, severity and duration of interruption of supply under the same threat. This shared information is highly sensitive, requiring the strongest possible protections against unauthorized release and liability. It may be so sensitive that it must be submitted to a mutually trusted third party to handle the data. These data are inputs to a network or agent model that simulates the cascades of failures across CIs and across the regional geography. Although there are numerous "interdependencies models" in the literature, they are primarily the products of National Laboratories or universities and have seldom been made available to other users.

*This is the most important area for further research***.** There are several demonstrated approaches – network modeling, graph theory, GIS-based modeling, systems dynamics, agent-based models, input-output modeling, etc. Many of these require expertise and computing power beyond the resources available to localities and regional CIs. Few have been demonstrated for actual field use. The suggested field-based pilot suggests that the CIs and local governments may well have databases, models and various management processes that could be adapted to support a simplified approach.

Once the cascading failures have been modeled, a panel of engineers and operators experienced with these local CI systems reviews the results to confirm that the essential interdependencies and cascading hazards have been simulated. If not, the model is iterated with until the panel deems it acceptable to move to the next step. Then, the information about dependencies hazards is provided back to the individual enterprises for their use in updating their overall risk assessment.

The respective enterprises update their earlier estimates to incorporate the information about dependencies and interdependencies to reset their baseline risk and fragility for each threat-asset pair. These updated estimates are re-analyzed at the regional level using the dependencies model to set the regional baseline risk and resilience. At enterprise and regional levels, the revised estimates of risk and fragility are aggregated to a regional total, by CI system and relevant subsystems, by hazard type, possibly by geographic area, and other ways to aid in decision-making. The risk and fragility should be communicated to the senior executives of the coalition membership and the regional risk and fragility considered for public release.

E.4 Enterprise Implementation and R.4 Regional Implementation are the phases where the decisions to mitigate risk and fragility are made and carried out. It is the phase where the "business case" for risk- and fragility-reducing options is made and security and resilience are actually improved. The decision process is the decision to commit resources to specific options and the managed implementation and operations of the selected options.

The process begins with ranking and sorting the threat-asset pairs by their risk and fragility estimates. Those with small enough risk and fragility to be borne by the enterprise are simply accepted. Others can be transferred, at a price, by purchasing of insurance. While insurance can reduce the consequences of the hazard event to zero or whatever deductible is specified in the policy, it has no effect on fragility. Further, insurance policies are difficult to purchase for certain hazards such as terrorism, because underwriters lack an actuarial base of history on which to price the policy on actuarial analysis.

The threat-asset pairs remaining after acceptance and transferring risk require more active programs if risk and fragility are to be reduced. The value of these programs is the extent that their benefits exceed their costs. Most enterprises have standard metrics of value they are accustomed to, which determines the form of the business case, often net benefits analysis or return on investment analysis. These are only different in minor details, so here the language of net benefits analysis is used.

Design options are driven by the nature of the threat and the asset. They may include adoption of new procedures or industry best practices (often attractive options for cybersecurity), adding preventative and deterrence measures to reduce threat likelihood, adding protective measures to reduce vulnerability, revising the workflows or locations of facilities to reduce consequences and adding redundancies and mutual aid agreements to reduce fragility. Re-designing, rehabilitating and building new structures with designed-in security and resilience allow reduction of multiple elements. Note that in these examples, reducing one or more of the terms in the risk and/or fragility equations is the explicit purpose. One way to brainstorm for options is to ask how each element of risk and fragility could be reduced and define options based on the answers.

Option designs need to be detailed enough to estimate the amount that they will reduce the respective elements of risk and fragility and the amount they will cost over their useful lives. For options that are action programs made up primarily of people doing things that reduce risk or fragility, it is best to consider it an "annual" project, although it can be repeated for any number of years. If the threat or hazard is expected to change over time as some aspects of climate change are, it is useful to repeat the analysis for annual or multi-year blocks of time. In this case, the annual project becomes a non-capital multi-year project. Most of these projects will be considered by their enterprises as operating budget items.

More durable options with an investment phase and a multi-year operating phase will usually be considered capital budget requests. For these it is necessary to estimate its useful life for both benefits and costs. The benefits are projected from the start of full operations to the end of the useful life. They may be constant over time or may change from year to year with changes in the hazard or the effectiveness of the option. Costs are estimated on a “life-cycle” basis, including design and engineering, initial construction and procurement, operations and maintenance, periodic rehabilitation if needed, decommissioning, demolition and site restoration.

At the enterprise level, benefits of options are estimated based on risk, where all the consequences have been converted to dollars. Key components of these consequences, including lost gross revenue (i.e., fragility), deaths and serious injuries risk are recorded and displayed with the benefits in all decision. The benefits of an option are estimated by re-analyzing the threat-asset pair assuming the option has been implemented. If the option is well designed, some specific elements of risk and fragility will have been reduced by the option, so the risk and fragility estimates will be smaller than the original baseline estimates. For example, options may reduce consequences, outages, vulnerabilities, or, more rarely, threat likelihoods. The difference in risk or fragility attributable to the option is the gross benefit of the option. In multi-year options, both benefits and costs are expressed as net present values. To do this, both benefits and costs are projected over the life of the option (including its post-operations cleanup if any) and discounted back to the present using the enterprise’s standard discount rate (usually based on the enterprise’s cost of capital). Subtracting the present value of the life-cycle costs from the present value of the gross benefits yields the net present value of the benefits of the option, or its value to the enterprise.

It is common that an option designed for one threat-asset pair reduces risk or fragility for another pair. These joint benefit options are located by arraying threat-asset pairs versus options in a matrix and identifying such cases. The benefits of the joint benefit options must be carefully considered. Joint benefit options are analyzed for all the threat-asset pairs they seem to affect and the benefits are combined, with careful recognition that the combinations may be anywhere from as much as the sum of the benefits from all threat-asset pairs to as little as the value of the one with the greatest individual value.

Any option with a net benefit of less than zero (a gross benefit/cost ratio less than 1.0) is unlikely to be funded when resources are scarce, so its threat-asset pair is referred for additional option development. Where mutually exclusive alternative options have been defined for the same threat-asset pairs, the one with the greater value is preferred.

The remaining options from all enterprises are shared with the Regional Implementation phase, where they are analyzed for their impacts on interdependencies estimated as described in phase R.3, Regional Risk Analysis, and returned to the respective enterprises. The enterprises update their estimates for the new effects of interdependencies with the options.

The results of these analyses are displayed in a decision-relevant format – a “dashboard” with summary graphic displays of risks, fragilities, benefits, costs and other objectives and drill-down (finer detail) and “what-if” (rapid re-analysis) capabilities. The enterprise’s decision-makers are briefed and then select the options they will fund based on the full set of weighted objectives developed in phase E.1, up to their budget limitation. These selections are subjected to the form of sensitivity analysis known as robustness analysis. Uncertain variables are run to their extremes to see if the choices among options would change materially. For those that change, the decision-maker and analyst consider the likelihood that the variable will actually go to the point that would cause a change in selections.

The options choices made by the enterprises are shared with the regional coalition, where they *and the unselected options* are run through the regional interdependencies model and regional benefits are estimated. The benefits to the region of the enterprise's chosen options are calculated against the regional baseline estimated in phase R.3. The potential benefits to the enterprises' region of the *unselected* options as well as any uniquely regional options are evaluated from the regional public's perspective. In some cases, the incremental cost of unselected options to the enterprises might be small enough to voluntarily obtain its additional selection for the contribution to public benefit and positive image it could convey.

In other cases, the contrast of the enterprise's business case and the region's public benefit case will identify instances where the enterprise cannot justify the cost for sound reasons but the benefit to the region is compelling. For these cases, the coalition seeks to locate and/or attract funding. In some cases, it would be local – local government, business, industry or civil improvement groups would collectively benefit sufficiently to partner with the relevant enterprises and/or local government to provide incentives to make the project more justifiable for the enterprise. Given that the enterprise may share the results of its business case analysis, the regional coalition can calculate how much of an incentive is necessary to make the option competitive with those already selected by the enterprise. The amount of the incentive can vary from a small contribution to the full cost of the option, as needed to assure the option's inclusion in the enterprise's overall program.

In other cases, the coalition would seek funding outside the region – from the state, federal agencies, foundations, etc. Proposals for such funding would be well supplied with "hard" analytical justification, through all the analytical results available, so the coalitions using this approach should have better odds of winning grants than those that do not. Local enterprises, including local government agencies, would take responsibility for detailing, implementing, managing and exercising the programs based on all the selected options, regardless of funding source, because the regional coalition or P3 is unlikely to staff operational programs.

Note that this overall process produces rational resource allocations of both the enterprise and regional public's available resources while selecting the programs with the greatest net benefits to each.

At both levels, risk and resilience, without and with the new programs, are aggregated by total, system and subsystem, and hazard type. These are reported, with appropriate safeguards to the state and federal government agencies involved.

E.5 Enterprise Effectiveness Measurement measures both *outputs* and the *outcomes* of the CISR programs and reports them for accountability and progress reporting. Metrics are defined for both levels. For outputs measurement, the metrics are the typical ones used in project and program management – schedules, milestones with deliverables, costs and specific products and services delivered. These data are collected regularly as part of the enterprise's standard management information systems and is interpreted as whether the programs are being implemented as planned or being diverted by unexpected conditions or other impediments. The programs are managed day to day based on these metrics and the program plan.

Metrics for *outcomes* are program-specific. In each case, the option was chosen based on the net benefits it was projected to produce. These benefits were the result of reducing one or more of the elements of risk or resilience for the set of threat-asset pairs included in its benefits. These reductions are defined as the outcome objectives for measuring the overall goals of reducing risk and fragility. The specific projected reductions in threat likelihood, vulnerability, consequences (for all relevant dimensions—casualties, dollar losses, reduction in gross regional product), and outage duration or severity are the specific outcome measures when combined as calculated risk or fragility. Actual incidents of the threat or hazard are documented in detail as data about the levels of vulnerability, consequences and outages. In addition, exercises and drills are conducted both as training and to add data on these same elements. After a suitable amount of time (which will vary depending on the nature of the program), a separate analytical team from the analysts who conducted the initial risk and fragility analysis re-estimate the current levels of all elements and compare them to the previous estimates, noting the amount of progress made. These actual estimates are used to calculate risk and fragility for program level progress measurement. Two comparisons are useful:

- Comparison of actual with the original baseline estimated in phase E.3 to gauge actual progress in improving actual security and resilience;
- Comparison of actual with the projections estimated in phase E.4 to justify the programs to measure progress relative to the program's specific objectives.

NOTE: Because the programs' implementation has changed the actual situation, these new estimates of actual levels provide the baseline for the next complete cycle of risk/fragility analysis.

R.5 Regional Effectiveness Measurement also documents actual incidents in detail and conducts exercises and drills for training and to use as data for measure the effectiveness of the programs, but at a regional scale. Under the protections of the information sharing and protection agreement, the effectiveness evaluations performed by the enterprises are shared with the coalition. These are reviewed closely to define the level of actual implementation of the programs and then analyzed using the interdependencies model to estimate the actual levels regional risk and fragility. As with the enterprise effectiveness evaluation, these are used in two comparisons:

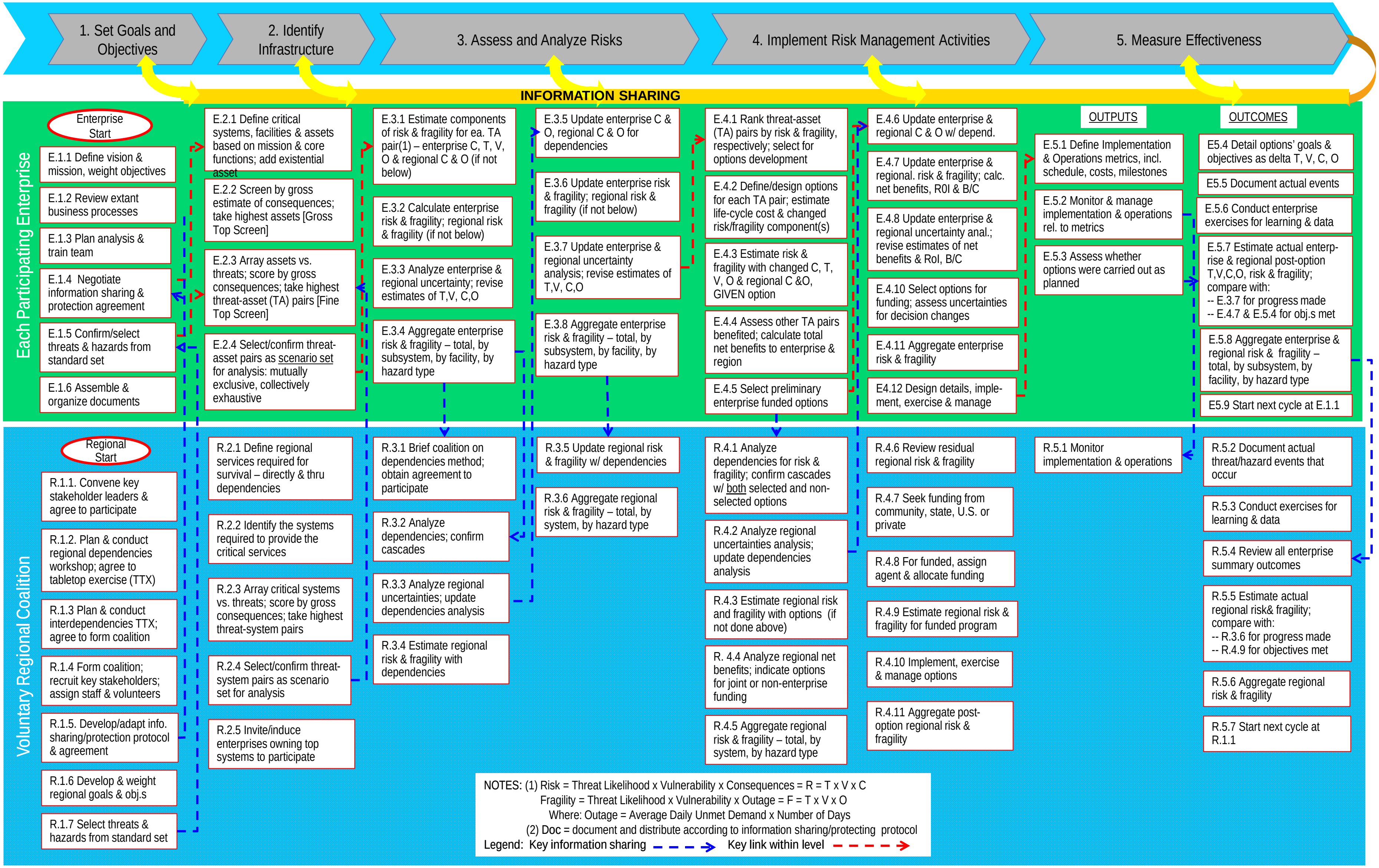
- Comparison of actual with the original regional baseline estimated in phase R.3 to gauge actual progress in improving regional security and resilience;
- Comparison of actual with the projections estimated in phase R.4 to justify the programs and any incentives to measure progress relative to the region's specific objectives.

The results of these comparisons are aggregated and summarized as regional totals, by major system, by hazard type and other useful subsets. This information is selectively released to sponsors of grants or incentives, the general public and state and federal authorities for use in their own policy and program planning and progress reporting to legislative bodies. Bond-rating services and insurance and re-insurance firms might provide preferential treatment to regional communities that conduct such programs, much as fire hazard insurance is keyed to specific conduct by fire departments.

As with the enterprise, the regional effectiveness assessment also establishes the new baseline for the next full cycle of the regional level of the CISR Risk Management Process.

Figure 5 shows the next more detailed level of the CISR-RMP for readers who wish to see it. We recognize that reading either figures or text is tedious and tiring. This level of detail (and for some tasks still finer) is needed if an actual management process is to be developed for testing.

Attachment 2. NIPP 2013 Critical Infrastructure Risk Management Framework and the CISR Risk Management Process



1. Set Goals and Objectives

2. Identify Infrastructure

3. Assess and Analyze Risks

4. Implement Risk Management Activities

5. Measure Effectiveness

INFORMATION SHARING

Each Participating Enterprise

Enterprise Start

E.1.1 Define vision & mission, weight objectives

E.1.2 Review extant business processes

E.1.3 Plan analysis & train team

E.1.4 Negotiate information sharing & protection agreement

E.1.5 Confirm/select threats & hazards from standard set

E.1.6 Assemble & organize documents

E.2.1 Define critical systems, facilities & assets based on mission & core functions; add existential asset

E.2.2 Screen by gross estimate of consequences; take highest assets [Gross Top Screen]

E.2.3 Array assets vs. threats; score by gross consequences; take highest threat-asset (TA) pairs [Fine Top Screen]

E.2.4 Select/confirm threat-asset pairs as scenario set for analysis: mutually exclusive, collectively exhaustive

E.3.1 Estimate components of risk & fragility for ea. TA pair(1) – enterprise C, T, V, O & regional C & O (if not below)

E.3.2 Calculate enterprise risk & fragility; regional risk & fragility (if not below)

E.3.3 Analyze enterprise & regional uncertainty; revise estimates of T,V, C,O

E.3.4 Aggregate enterprise risk & fragility – total, by subsystem, by facility, by hazard type

E.3.5 Update enterprise C & O, regional C & O for dependencies

E.3.6 Update enterprise risk & fragility; regional risk & fragility (if not below)

E.3.7 Update enterprise & regional uncertainty analysis; revise estimates of T,V, C,O

E.3.8 Aggregate enterprise risk & fragility – total, by subsystem, by facility, by hazard type

E.4.1 Rank threat-asset (TA) pairs by risk & fragility, respectively; select for options development

E.4.2 Define/design options for each TA pair; estimate life-cycle cost & changed risk/fragility component(s)

E.4.3 Estimate risk & fragility with changed C, T, V, O & regional C &O, GIVEN option

E.4.4 Assess other TA pairs benefited; calculate total net benefits to enterprise & region

E.4.5 Select preliminary enterprise funded options

E.4.6 Update enterprise & regional C & O w/ depend.

E.4.7 Update enterprise & regional. risk & fragility; calc. net benefits, R0I & B/C

E.4.8 Update enterprise & regional uncertainty anal.; revise estimates of net benefits & RoI, B/C

E.4.10 Select options for funding; assess uncertainties for decision changes

E.4.11 Aggregate enterprise risk & fragility

E4.12 Design details, implement, exercise & manage

OUTPUTS

E.5.1 Define Implementation & Operations metrics, incl. schedule, costs, milestones

E.5.2 Monitor & manage implementation & operations rel. to metrics

E.5.3 Assess whether options were carried out as planned

OUTCOMES

E5.4 Detail options' goals & objectives as delta T, V, C, O

E5.5 Document actual events

E.5.6 Conduct enterprise exercises for learning & data

E.5.7 Estimate actual enterprise & regional post-option T,V,C,O, risk & fragility; compare with:
-- E.3.7 for progress made
-- E.4.7 & E.5.4 for obj.s met

E.5.8 Aggregate enterprise & regional risk & fragility – total, by subsystem, by facility, by hazard type

E5.9 Start next cycle at E.1.1

Voluntary Regional Coalition

Regional Start

R.1.1. Convene key stakeholder leaders & agree to participate

R.1.2. Plan & conduct regional dependencies workshop; agree to tabletop exercise (TTX)

R.1.3 Plan & conduct interdependencies TTX; agree to form coalition

R.1.4 Form coalition; recruit key stakeholders; assign staff & volunteers

R.1.5. Develop/adapt info. sharing/protection protocol & agreement

R.1.6 Develop & weight regional goals & obj.s

R.1.7 Select threats & hazards from standard set

R.2.1 Define regional services required for survival – directly & thru dependencies

R.2.2 Identify the systems required to provide the critical services

R.2.3 Array critical systems vs. threats; score by gross consequences; take highest threat-system pairs

R.2.4 Select/confirm threat-system pairs as scenario set for analysis

R.2.5 Invite/induce enterprises owning top systems to participate

R.3.1 Brief coalition on dependencies method; obtain agreement to participate

R.3.2 Analyze dependencies; confirm cascades

R.3.3 Analyze regional uncertainties; update dependencies analysis

R.3.4 Estimate regional risk & fragility with dependencies

R.3.5 Update regional risk & fragility w/ dependencies

R.3.6 Aggregate regional risk & fragility – total, by system, by hazard type

R.4.1 Analyze dependencies for risk & fragility; confirm cascades w/ both selected and non-selected options

R.4.2 Analyze regional uncertainties analysis; update dependencies analysis

R.4.3 Estimate regional risk and fragility with options (if not done above)

R. 4.4 Analyze regional net benefits; indicate options for joint or non-enterprise funding

R.4.5 Aggregate regional risk & fragility – total, by system, by hazard type

R.4.6 Review residual regional risk & fragility

R.4.7 Seek funding from community, state, U.S. or private

R.4.8 For funded, assign agent & allocate funding

R.4.9 Estimate regional risk & fragility for funded program

R.4.10 Implement, exercise & manage options

R.4.11 Aggregate post-option regional risk & fragility

R.5.1 Monitor implementation & operations

R.5.2 Document actual threat/hazard events that occur

R.5.3 Conduct exercises for learning & data

R.5.4 Review all enterprise summary outcomes

R.5.5 Estimate actual regional risk& fragility; compare with:
-- R.3.6 for progress made
-- R.4.9 for objectives met

R.5.6 Aggregate regional risk & fragility

R.5.7 Start next cycle at R.1.1

NOTES: (1) Risk = Threat Likelihood x Vulnerability x Consequences = R = T x V x C
Fragility = Threat Likelihood x Vulnerability x Outage = F = T x V x O
Where: Outage = Average Daily Unmet Demand x Number of Days
(2) Doc = document and distribute according to information sharing/protecting protocol
Legend: Key information sharing – – – → Key link within level – – – →

National Institute of
BUILDING SCIENCES

1090 Vermont Avenue, NW Suite 700
Washington, DC 20005-4950
Phone: (202) 289-7800
Fax: (202) 289-1092
www.nibs.org