

Building Capacity for a Public/Private Program for Infrastructure Security in the National Capital Region

Executive Summary

Criterion 1: Program Overview

1. Statement of Need

National Needs – Critical infrastructure is a high priority of the national government. Critical infrastructure protection (CIP) is a national mandate, as demonstrated by the Homeland Security Act, Homeland Security Presidential Directive 7, the findings of the 9/11 Commission, the 9/11 legislation, federal investments in CIP analytic methods, and in other national policy statements. Specifically, national policy mandates ***public/private collaboration*** to implement a ***risk management*** approach.

Regional Needs – Critical infrastructure is a high priority of the jurisdictions and private sector in the NCR. In 2002 ***Eight Commitments to Action*** identified critical infrastructure protection as a high priority and provided guidance on the approach: “citizen involvement, collaborative decision-making, exercises that are inclusive of all levels of government, ...schools and universities, health care institutions, and other private and non-profit partners as appropriate.” The next year, the ***NCR Urban Area Homeland Security Strategy*** set as strategic objectives to “reduce the NCR’s vulnerability to terrorism” and “minimize the damage and recover from attacks that do occur” – both pointing to protecting critical infrastructure. In late 2003 and early 2004, the NCR initiated the ***National Capital Region-Critical Infrastructure Project (NCR-CIP)***, chartering a consortium of six NCR universities to address these needs. Phase I of that project is broadly to define specific critical infrastructure needs of the NCR and to develop a plan for meeting them.

With the goal to ***create a more resilient NCR by advancing critical infrastructure security at the asset, system and regional levels***, Phase I is assessing the state of security in each of eight infrastructure sectors and recommending specific steps to improve protection of their assets and systems while defining a preliminary framework to address ***regional*** CIP priorities. This framework consists of the organizational and decision-support analytic tools to rationally and transparently decide which CIP initiatives are worthwhile and who should pay their costs. The present proposal is for Phase II of the project, which is the initial implementation of that plan.

Specific Needs – Methods for public/private/non-profit collaboration to understand the risks to critical infrastructures and the value of risk reduction initiatives. Findings to date of NCR-CIP Phase I suggest the specific goals and objectives for Phase II. Central among the findings are the following regional needs:

1. Virtually all the critical infrastructures need to be addressed for the region to be as secure as needed because all are interrelated through dependencies in complex and non-intuitive ways.
2. Sector-level security needs to be improved in virtually all sectors currently being studied, to greater or lesser degrees, especially to counter the risks attributable to interdependencies.
3. Each sector must recognize and deal with risks and interdependencies as they set CIP goals and risk reduction programs for their assets and systems.
4. Sector-level CIP initiatives must be complemented by region-wide, multi-jurisdictional, public/private initiatives and integrated explicitly with the security strategies of the states,

the District, the counties and other municipalities – as well as the nation – for the region to reach the desired level of security and resilience.

The last of these is the most critical: establishing an overall management framework for coordination of NCR CIP initiatives at asset, system and region levels. It requires methods for:

- Defining and estimating the magnitude of risks to infrastructures;
- Evaluating the merits of risk-reduction programs and projects;
- Allocating resources to those with greatest value relative to their cost; and
- Deciding who should bear these costs – consumers or taxpayers, private or public sector, and if the latter, which among local, state or federal government.

Because as much as 85% of critical infrastructures are privately owned and operated, these methods need to include ways for firms to make the business case for investing in risk reduction, tailored expressly for use by individual firms and industries. In addition, because of the significance of the interdependencies that cause failures in one sector to spill over into others, these methods must be widely shared to allow multiple firms and jurisdictions to collaborate to find cost-effective solutions to regional CIP needs and must integrate with the state, local and national CIP programs.

2. Goals, Objectives and Specific Tasks

The overall goal for Phase II is to establish a metrics-based CIP management framework that provides the capacity for the NCR to develop an integrated strategy to share information, estimate risks to critical infrastructures, evaluate risk-reduction initiatives, invest in those initiatives with the greatest value, and evaluate their outcomes. Based on the findings of Phase I, Phase II will pursue this goal as three specific goals, each addressed by seven specific objectives, as summarized in Table 1 (with a summary schedule in Figure 1). This matrix of the tasks to achieve the goals and objectives illustrates the close integration of sector, region, and national levels. The table also shows the funding strategy: UASI funds are applied to the specific, high priority objectives of the NCR sectors and the NCR region, while this effort is leveraged to bring incremental funds into the region to build, generalize and validate the NCR methods as standard templates for use in other regions across the country.

The ***specific goals*** are:

- 1. Sector goal: Enable industry owners/operators to make the CIP business case and implement and evaluate risk reduction solutions in up to 15 sectors;***
- 2. Region goal: Enable achievement of regional CIP security and resilience based on analysis and equitable distribution of full regional benefits and costs of risk-reduction initiatives and their synergies with the strategies of the respective states, counties and cities; and,***
- 3. Nation goal: Leverage and integrate NCR regional CIP and national CIP developments (insofar as they benefit the NCR) and develop/test tools and templates for use in other regions.***

Achieving each of these goals requires meeting seven ***specific objectives***:

- 1. Assess the state of security of the remaining critical infrastructures*** by applying the approach developed in Phase I to agriculture and food, national monuments and icons, defense industrial base, information technology, government facilities, and commercial facilities – and ***integrate them with the eight assessed in Phase I.***
- 2. Increase awareness of CIP and the impact of interdependencies and integrate action plans*** by vetting the findings and recommendations of Phase I and conducting a series of

public/private table top exercises at sector and regional levels to define additional action steps.

3. *Initiate and facilitate **councils** for regional information sharing, deliberations, coordination and decision-making* as leadership partnerships at the sector, cross-sector, and regional public/private/non-profit levels.
4. *Provide analytic **decision support** – metrics, models, and methods – and facilitate planning and selection of risk reduction projects* by testing, adapting and/or developing methods suitable for each sector and regional decision-making.

Table 1. NCR-CIP Phase II Goals, Objectives & Key Tasks for Building Capacity for a More Secure and Resilient NCR

	<u>Proposed for UASI Funding</u>		<u>Proposed for Other Funding</u>
	<u>Sector-Level Tasks</u>	<u>Region-Level Tasks</u>	<u>National Integration Tasks</u>
Phase II Goals	<i>Enable owners/ operators to make the business case and invest in CIP</i>	<i>Enable achievement of regional CIP security and resilience and integrate with state, county and city strategies</i>	<i>Integrate national and NCR regional CIP and develop/test tools for use in NCR, other regions (likely DHS participants)*</i>
Objectives for Phase II			
1. Assess remaining critical infrastructure sectors	Assess state of security and advance recommendations for 6 new sectors	Integrate new sectors	Develop assessment templates (IP, ODP)
2. Increase awareness of value of CIP and role of interdependencies	Conduct table top interdependency exercises for each sector	Conduct multi-jurisdictional public/private CI interdependency exercise	Develop CI awareness exercise templates(IP, ODP)
3. Form councils to coordinate decision-making	Establish Sector Coordinating Councils (public and private, each sector)	Establish public-private Sector Coordinating Councils and NCR CIP Leadership Council	Link NCR regional organization template to NIPP (IP, ODP)
4. Provide analytic decision support	Field test asset risk management/ resource allocation tool and facilitate CI decisions CIP tool kit maintenance	Field test regional risk management/ resource allocation tools and facilitate CI decisions	Field test and evaluate tools for asset, system, and regional application (IP, S&T, ODP)
5. Facilitate implementation	Facilitate sector projects selected in 4 (funded subsequently)	“Red team” top regional priorities	Develop regional project implementation templates (IP, ODP)
6. Evaluate changes in NCR security/resiliency	Measure regional/sector baseline and change	Measure overall regional baseline and change	Develop evaluation templates (IP, ODP)
7. NCR-CIP program management	Develop and implement comprehensive management framework	Develop and implement comprehensive management framework	Develop and implement comprehensive management framework

*IP: Office of Infrastructure Protection; ODP: Office of Domestic Preparedness; S&T: Office of Science and Technology

5. *Facilitate **implementation** of the selected risk reduction projects*, starting with “red team” vulnerability assessments of the infrastructures of highest priority to the region. Note: Most

of the implementation efforts after these initial assessments are anticipated to be funded outside of the present proposal.

6. **Evaluate improvement and design enhancements** in *critical infrastructure security and resilience in the NCR* by empirically estimating baseline levels of key regional outcome metrics in Phases I and II for comparison to future re-measurement of the status of sectoral and regional resilience and security. Note that efficiency and output metrics are measured as part of the work toward each of the above objectives.
7. **Manage the NCR-CIP Phase II program** by applying prudent project management principles and methods.

Criterion 2. Management Overview

George Mason University (GMU) will continue to manage the University Consortium for Infrastructure Security (UCIP), which is made up six distinguished NCR institutions: **The University of Maryland, The University of Virginia, Howard University, Virginia Tech, James Madison University,** and GMU. This is the same team conducting NCR-CIP Phase I and represents a substantial proportion of the infrastructure and security academic expertise in the NCR.

Criterion 3. Fiscal Management

As shown in Table 2, the budget for the integrated Phase II program is \$6 million over 18 months. *This proposal seeks \$3 million from NCR UASI funds.* The other \$3 million will be sought from several offices of DHS and other federal agencies, most of which have meet with the team and express interest in collaborating with the NCR. However, *this project is designed to operate with only UASI funding, if required.*

Criterion 4. Evaluation

Evaluation of performance, effectiveness and results is central to the strategy for Phase II. Three types of evaluation will be undertaken. In ascending order of importance:

1. **Task Progress** – the extent to which the proposed activities are completed and delivered on schedule and in budget, basic project management supported by Microsoft Project and financial reporting.
2. **Task Effectiveness** – the extent to which the sets of related tasks achieve their objectives, e.g., sectors assessed, exercises conducted, councils organized, etc., the quality of those achievements as measured by satisfaction questionnaires and the comparison of conditions before and after the task performance.
3. **Results** – the extent to which the NCR is made more secure and resilient as results from the coordinated efforts of many actors in the regional scene, as catalyzed by NCR-CIP Phase II and supported by the public, private and non-profit sectors over a sustained period of time. A key objective of Phase II is to define metrics and study design for this evaluation and to *measure the baseline* against which future measures can be compared.

Conclusion

Phase II of NCR-CIP will build the capacity for a true public/private/non-profit partnership to evaluate and make the needed decisions and investments in critical infrastructure protection projects and programs – fully integrated with the national, state, county, city and private sector security strategies – to create *a more secure and resilient National Capital Region.*

Table 2. Distribution of Requested Funding by Funding Source, Goal, and Objective

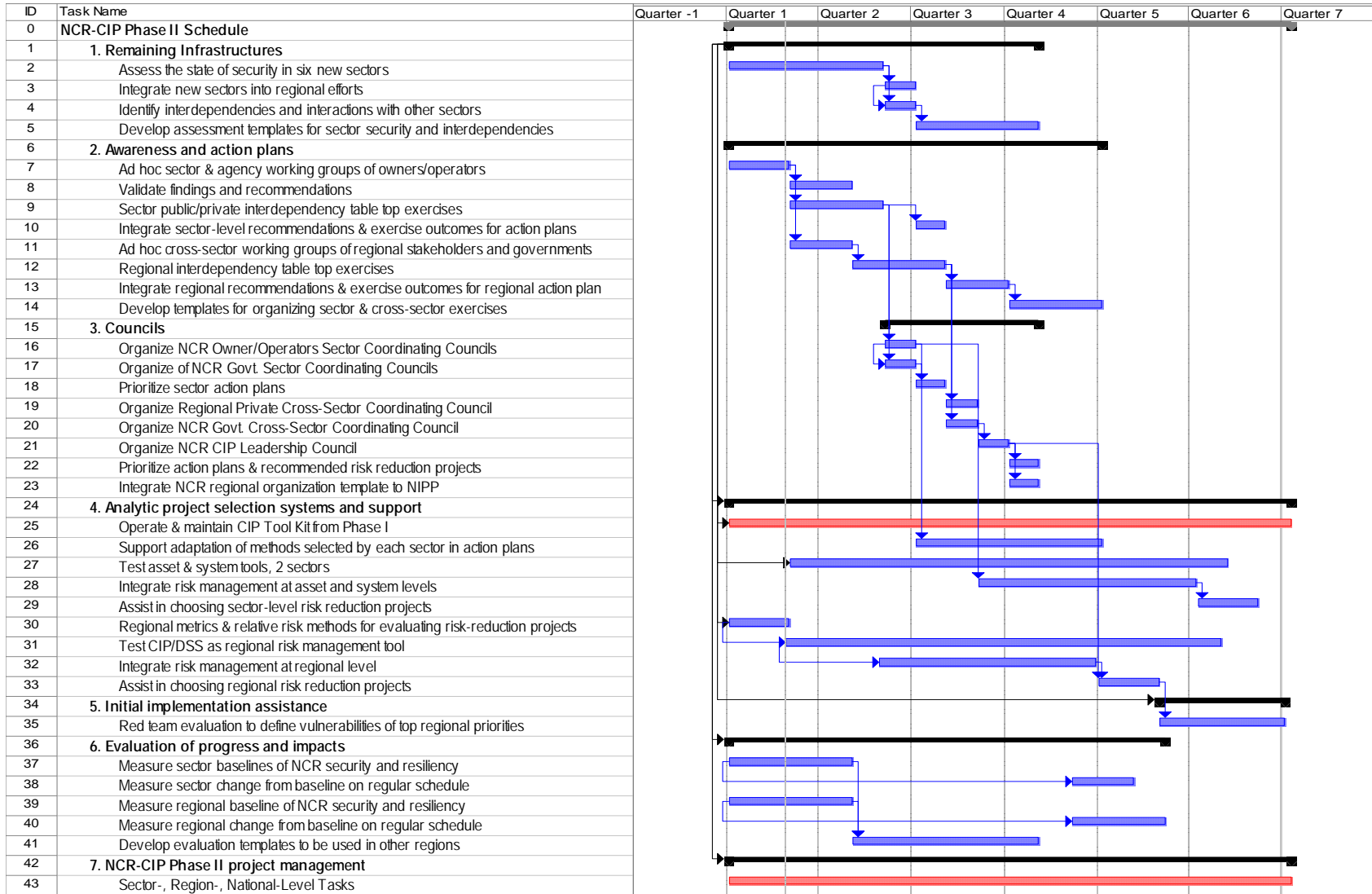
Proposed Funding Source	<i>Proposed for UASI Funding</i>				<i>Proposed for Other Funding*</i>	Total Program by Objective
	<u>Sector-Level Tasks</u>	<u>Region-Level Tasks</u>	<u>Evaluation Tasks</u>	Total UASI by Objective	<u>National Integration. Tasks</u>	
Goals Objectives	<i>Owners' CIP business case</i>	<i>Regional CIP investment</i>	<i>Efficiency effectiveness & outcomes</i>		<i>NCR-National CIP integration</i>	
1 Remaining sectors	\$ 500	**	**	\$ 500	\$ 80	\$ 580
2. Increase awareness	300	\$ 185	\$ 40	525	175	700
3. Form councils	145	35	40	220	80	300
4. Decision support	305	140	80	525	1,940	2,465
5. Facilitate implement.	***	335	***	335	600	935
6. Evaluate changes	135	135	25	295	125	420
Subtotal by Goal	1,385	830	185	2,400	3,000	5,400
7. Program management				600		600
Total by Goal	\$ 1,385	\$ 830	\$ 185	\$ 3,000	\$ 3,000	\$ 6,000

* Anticipated to be funded by the U.S. Dept. of Homeland Security, Offices of Domestic Preparedness, Infrastructure Protection, Science & Technology, and others.

** Included in Project Management.

*** Projects to be funded outside of present program as selected in tasks above.

Figure 1. NCR-CIP Phase II Summary Schedule





Building Capacity for a Public/Private Program for Infrastructure Security in the National Capital Region

A Proposal for Phase II of the National Capital Region Critical Infrastructure Project

*Submitted in Response to RFA #05 HSGP-UASI
to the*

Senior Policy Group of the National Capital Region

District of Columbia

*Robert Bobb, Deputy Mayor/City Administrator, Office of the Mayor
Barbara Childs-Pair, Director D.C. Emergency Management Agency, Office of the Mayor*

Maryland

*John W. Droneburg, Director Maryland Emergency Management Agency
Dennis R. Schrader, Director, Governor's Office of Homeland Security*

Virginia

*Janet Clements, Chief Deputy State Director, Virginia Department of Emergency Management
George W. Foresman, Assistant to the Governor for Commonwealth Preparedness*

U.S. Department of Homeland Security

Thomas J. Lockwood, Director, Office of National Capital Region Coordination

By the

University Consortium for Infrastructure Protection

*Managed by George Mason University
Critical Infrastructure Protection Program*





Office of Sponsored Programs

4400 University Drive, MS 4C6, Fairfax, Virginia 22030
Phone: 703-993-2988; Fax: 703-993-2296

February 28, 2005

Office of the Deputy Mayor for Public Safety and Justice
Attention: Leeann Turner
1350 Pennsylvania, NW, Suite 327
Washington, DC 20004

RE: RFA#05 HSGP-UASI

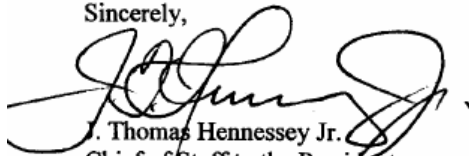
Dear Ms. Turner:

Enclosed please find a grant proposal submitted to the Office of the Deputy Mayor for Public Safety and Justice for Dr. John A. McCarthy, School of Law, George Mason University (GMU). GMU is a public institution of higher learning in the Commonwealth of Virginia.

The project is entitled *National Capital Region-Infrastructure Project Phase II: Building Capacity for a Public/Private Program for Infrastructure Security in the NCR*. Dr. McCarthy requests that the project begin June 1, 2005 and end November 30, 2006.

If you have any questions regarding the technical portion of this project, please feel free to contact Dr. McCarthy at 703/993-4840; questions regarding budget or university policies and procedures should be directed to Joanne Carter, Grants Administrator, Office of Sponsored Programs at 703/993-2976.

Sincerely,



J. Thomas Hennessey Jr.
Chief of Staff to the President
George Mason University

Enclosures

cc: J. McCarthy



CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Ms. Leeann Turner
Director for Homeland Security Grants Administration
Office of Deputy Mayor for Public Safety and Justice
1350 Pennsylvania Avenue, NW
Suite 327
Washington, DC 20004

Dear Ms. Turner:

It is with greatest pleasure that the University Consortium for Critical Infrastructure Protection (UCIP) submits this proposal to enhance the security and resilience of the National Capital Region (NCR) by ***“Building Capacity for a Public/Private Program for Infrastructure Protection,”*** in response to Request for Application (RFA)35 HSGP – UASI. It is **Phase II** of the **NCR Critical Infrastructure Project** currently being conducted by UCIP.

Six leading research institutions active in the NCR make up the University Consortium for Critical Infrastructure Protection -- **George Mason University (GMU), the University of Maryland, Virginia Polytechnic and State University (VA Tech), James Madison University, Howard University and the University of Virginia.**

While RFA guidance suggested each proposal should identify an appropriate Emergency Support Function (ESF) for application review, no existing ESF has comprehensive responsibility *for regional critical infrastructure protection in both public and private sectors*. This proposal is being submitted directly to the **NCR Senior Policy Group** for review, as suggested by the Office of National Capital Coordination of the U.S. Department of Homeland Security (DHS).

Please direct any inquiries directly to me (703-993-4840; jmccart5@gmu.edu) or my Associate Director for NCR Projects and UCIP manager, Jerry Brashear (703-993-9007; jbrashe2@gmu.edu).

Very sincerely,

A handwritten signature in red ink, appearing to read "John A. McCarthy".

John A. McCarthy
Director, Critical Infrastructure Protection Program
George Mason University School of Law

© George Mason University, 2005

CONFIDENTIAL. Distribution limited to NCR Senior Policy Group, NCR Chief Administrators Committee Officers Committee and Regional Emergency Support Committees of the Metropolitan Washington Council of Governments, the Washington , D.C., Office of the Deputy Mayor for Public Safety and Justice and their staff for purposes of evaluation only. No other use is authorized. Additional permissions for use must be requested by contacting Jerry Brashear, Associate Director, Critical Infrastructure Protection Program, George Mason University, at 703-993-9007 or jbrashe2@gmu.edu.

A. Applicant Profile

Project Title:

National Capital Region – Critical Infrastructure Project Phase II: Building Capacity for a Public/Private Program for Infrastructure Security in the NCR.

Emergency Support Function:

Senior Policy Group

Project Period:

18 months from commitment of funds – assume June 2005 start date

Project Synopsis:

Phase II of the National Capital Region Critical Infrastructure Project has the overall goal: *to build the capacity for information sharing and regional cooperation to enhance rational decision making for infrastructure risk reduction strategies*. It addresses this goal at sector, region (including integration with state and local jurisdictions) and nation levels through a fully integrated program jointly funded by the NCR UASI Grant Program and other sources, primarily DHS programs. At all three levels, work will be focused on six key objectives: (1) assess the state of security in the remaining critical infrastructure sectors, those not included in Phase I; (2) conduct awareness exercises focusing on the private sector and interdependencies, resulting in specific action plans; (3) facilitate the organization of councils for public/private/non-profit information and decision coordination; (4) test and develop analytic decision support tools and facilitate their use in selecting infrastructure protection measures; (5) facilitate testing and implementing the selected measures; and (6) evaluate output, progress and outcomes.

Implementing Jurisdiction:

University Consortium for Infrastructure Protection, managed by George Mason University

Agency Address:

Project Director:

John McCarthy
Director, Principal Investigator
George Mason University
School of Law
Critical Infrastructure Protection Project
3301 Fairfax Drive, MS 1 G 7
Arlington, VA 22201
703-993-4840 (office); 703-993-4847 (fax)
jmccart5@gmu.edu

B. Table of Contents

Sections	Page
Confidentiality Notice	iv
A. Applicant Profile	v
B. Table of Contents	vi
C. Proposal Summary	1
I. CRITERION 1 Program Overview.....	1
1. <i>Statement of Need</i>	1
2. <i>Goals and Objectives</i>	3
3. <i>Services to Be Provided</i>	4
II. CRITERION 2 Management Overview.....	5
III. CRITERION 3 Fiscal Management.....	5
IV. CRITERION 4 Evaluation.....	5
V. CONCLUSION.....	5
D. Project Goals, Objectives and Implementation Steps	6
I. OVERARCHING GOALS:	6
<i>Build Public/Private Decision and Coordination Capacity in the NCR</i>	6
II. SPECIFIC GOALS, OBJECTIVES AND IMPLEMENTATION STEPS:	6
<i>Comprehensiveness, Awareness, Organization, Decisions and Evaluation</i>	6
1. <i>GOAL 1. Enable owners/operators to make the CIP business case and implement & evaluate the CIP decisions in up to 15 sectors</i>	6
2. <i>GOAL 2. Enable achievement of regional CIP security and resilience based on full regional benefits and costs</i>	7
3. <i>GOAL 3. Develop, test, evaluate and document the NCR processes and tools for tailored application in other regions</i>	9
4. <i>GOAL 4. Assess efficiency and effectiveness of task performance and outcomes</i>	10
E. Project Description	11
I. RELATIONSHIP TO NATIONAL INITIATIVES.....	11
1. <i>National Importance of Critical Infrastructure Protection in the NCR</i>	11
II. REGIONAL PROTECTION PRIORITIES.....	13
1. <i>Needs and Guidance Driving NCR-CIP Phases I and II</i>	13
2. <i>Need for Decision-Making Organization and Tools Addressing Investments and Interdependencies</i>	13
III. SPECIFIC OBJECTIVES AND IMPLEMENTATION STEPS PHASE II.....	14
1. <i>Derived Directly from Homeland Security Policies, Needs and Findings of Phase I</i>	14
IV. EVALUATION.....	15
1. <i>Gauging the Effectiveness of Meeting Each Major Objective and Setting a Baseline for Future Region-Wide Assessments of Change</i>	15
V. PROGRAM INTEGRATION.....	16
1. <i>Phasing, Temporal Precedence Relationships and Resource Allocation</i>	16
F. Organization, Experience and Qualifications of Applicant	19

G. Staffing Plan.....	21
H. Project Budget and Budget Narrative.....	27
I. Certifications and Assurances.....	38
J. Appendices	
I – NCR Critical Infrastructure Needs, Tasks to Meet Them, and Evaluation of Effectiveness in Meeting Them	
II – Functional Organization Schemes for Regional-National Integration	
III – Resource Allocation by Provider	
IV – References	
V – Position Descriptions	
VI – Biographical Sketches	

List of Tables

Table 1	NCR-CIP Phase II Goals, Objectives & Key Services.....	4
Table 2	Distribution of Requested Funding by Funding Source.....	17
Table 3	Staffing.....	21

List of Figures

Figure 1	Figure 1. NCR-CIP Phase II Summary Schedule.....	18
Figure 2	NCR-CIP Phase II Organization.....	20

C. Proposal Summary

Building Capacity for a Public/Private Program for Infrastructure Security in the National Capital Region

(Overview of contribution to all 100 evaluation points)

Finally, the report does not provide the full picture of the challenge – the critical importance of integrating private sector initiatives as part of the larger effort. There are significant policy issues that are being considered within the context of the private sector’s role within the NCR and the commitment of public funds to address priority needs has been given careful attention. At the end of the day preparedness is not simply public sector readiness but the private sector as well. Report discussion should focus on planning processes and measurement criteria in the context of both public and private sectors

NCR Senior Policy Group comment; GAO 04-433, p.48

I. CRITERION 1: Program Overview (60 evaluation points)

1. Statement of Need (20 evaluation points; see also section E.)

National Needs – Critical infrastructure is a clear priority of the national government. Critical infrastructure protection (CIP) is a national mandate, as demonstrated by the Homeland Security Act, Homeland Security Presidential Directive 7, the National Infrastructure Protection Plan (NIPP), Federal investments in CIP analytic methods and in other national policy statements, including the 9/11 Commission report. Specifically, national policy argues for public/private collaboration and a risk management approach.

The National Capital Region (NCR) is a top national priority: it is the only region cited explicitly in the Homeland Security Act and the only region with a specially legislated Department of Homeland Security (DHS) office for coordination. This is justified by the fact that the NCR is a target-rich community: it is the very symbol of the United States in the eyes of world, the seat of the national government, headquarters of national defense as well as numerous international institutions. NCR sites were targeted on September 11, 2001, and in the anthrax attack. The NCR is also a major American region in its own right – its \$300 billion economy is the fourth largest in annual business and a major center of internet, telecommunications, information technology, biotech, and defense industries. As a major economic engine of two states and the District of Columbia, it is vital to the welfare of these states as well as the nation.

Regional Needs – Critical infrastructure is a clear priority of the jurisdictions and private sector in the NCR. In 2002 *Eight Commitments to Action* identified critical infrastructure protection as a high priority of homeland security strategy: “Infrastructure protection – work in partnership with the private sector to jointly identify and set protection priorities and guidelines for infrastructure assets and services in the NCR.” It also provided guidance on the approach: “citizen involvement, collaborative decision-making, exercises that are inclusive of all levels of government, . . . schools and universities, health care institutions, and other private and non-profit partners as appropriate.” The next year, the *NCR Urban Area Homeland Security Strategy* set as strategic objectives to “reduce the NCR’s vulnerability to terrorism” and “minimize the damage and recover from attacks that do occur” – both pointing to protecting critical infrastructure. In late 2003 and early 2004, the NCR initiated the *National Capital Region-Critical Infrastructure Project (NCR-CIP)*, a consortium of six NCR universities, to address

these needs. Phase I of that project was broadly chartered to define the more specific critical infrastructure needs of the NCR and to develop a plan for meeting them.

Under the goal to *create a more resilient NCR by advancing critical infrastructure security at the asset, system and regional levels*, Phase I is being conducted to assess the state of security in each of eight infrastructure sectors and recommend specific steps to improve protection of their systems while beginning to define a framework to address regional CIP priorities. This is especially to help in rationally and transparently deciding which CIP initiatives are worthwhile and who should pay their costs. The present proposal is for Phase II of the project, which is the initial implementation of that plan. This very need for more coordinated strategic planning and performance standards has been outlined by the GAO in May 2004 which states that the NCR does not have a set of accepted benchmarks and best practices to identify desired goals.

Specific Needs – Methods for public/private/non-profit collaboration to understand the risks to critical infrastructures and the value of risk reduction initiatives. Findings to date in Phase I of the NCR-CIP suggest the specific goals and objectives for Phase II. The critical infrastructure sectors in the National Capital Region vary widely in their approaches to vulnerability assessment and risk reduction. The area of greatest underestimation and underinvestment is interdependencies – the reliance on other sectors’ performance to continue to provide critical services. Owners and operators of CIs have not yet fully recognized, built, and acted on the business case for their own risk reduction – especially where the problem lies in other infrastructures on which they are dependent – and the NCR as a region lacks the planning, coordination and resource allocation framework to recognize, analyze and act on vulnerabilities that are not addressed by individual owners but are vital to the security, economic welfare, health and safety of NCR citizens.

Among the findings of Phase I are the following regional needs:

1. Virtually all the critical infrastructures need to be addressed for the region to be as secure as needed because all are related through dependencies in complex and non-intuitive ways.
2. Sector-level security needs to be improved in virtually all sectors currently being studied, to greater or lesser degrees, especially in steps to counter the risks attributable to interdependencies.
3. Each sector must recognize and deal with risk and interdependencies as they set CIP goals and risk reduction programs for their assets and systems.
4. Sector-level CIP initiatives must be complemented by region-wide, multi-jurisdictional, public/private initiatives and integrated explicitly with the security strategies of the states and the District for the region to reach the desired level of security and resilience.

Among the most pressing CIP needs in the NCR are establishing an overall management framework for coordination of NCR CIP initiatives, developing methods for defining and estimating the magnitude of risks to infrastructures, evaluating the merits of risk-reduction programs and projects, and allocating resources to those with greatest value relative to their cost. Because the vast majority of critical infrastructures are privately owned and operated, these methods need to include ways for firms to make the business case for investing in risk reduction. These methods need to be tailored expressly for the use by individual firms and industries. In addition, because of the significance of the interdependencies that cause failures in one sector to spill over into others, the need was for methods that are sufficiently widely shared to allow multiple firms and jurisdictions to collaborate to find cost-effective solutions to regional CIP needs.

2. Goals and Objectives (20 evaluation points; see also Section D)

The overall goal for Phase II is to establish a metrics based CIP management framework for the NCR which facilitates the capacity to share information, estimate risks to critical infrastructures, evaluate risk-reduction initiatives, invest in those initiatives with the highest priority, and evaluate their outcomes. Based on the findings of Phase I, this goal will be pursued at three levels:

- **Sector-level goal:** Enable **industry owners/operators** to make the **CIP business case** and implement and evaluate risk reduction solutions in up to 14 sectors;
- **Region-level goal:** Enable achievement of **regional CIP security and resilience** based on analysis and equitable distribution of **full regional benefits and costs** of risk-reduction initiatives and their synergies with the strategies of the respective states, counties and cities; and,
- **National-level goal:** Leverage and **integrate NCR regional CIP with national CIP developments** (insofar as they benefit the NCR) and develop/test tools & templates for use in other regions.

Achieving these goals requires meeting six **specific objectives**, which define the services to be provided, as described below:

1. Assess the state of security of the **remaining critical infrastructures** by applying the approach developed in Phase I to agriculture and food, national monuments and icons, defense industrial base, information technology, government facilities, and commercial facilities – and **integrate them with the eight assessed in Phase I.**
2. Increase **awareness** of CIP and impact of interdependencies and integrate action plans by vetting the findings and recommendations of Phase I and conducting a series of public/private table top exercises at sector and regional levels to define additional action steps.
3. Initiate and facilitate **councils** for regional information sharing, deliberations, coordination and decision-making at the sector, cross-sector, and regional public/private/non-profit leadership partnership.
4. Provide analytic **decision support** – metrics, models, and methods – and facilitate planning and selection of risk reduction projects by testing, adapting and/or developing methods suitable for each sector and regional decision-making.
5. Facilitate **implementation** of the selected risk reduction projects, starting with “red team” vulnerability assessments of the infrastructures of highest priority to the region. Note: most of the implementation efforts after these initial assessments are anticipated to be funded outside of the present proposal.
6. **Evaluate improvement** in critical infrastructure security and resilience in the NCR by empirically estimating baseline levels of key regional outcome metrics in Phases I and II for comparison to future re-measures as evaluations in the status of sectoral and regional resilience and security. Note that efficiency and output metrics are measured as part of the work toward each of the above objectives.
7. **Manage the NCR-CIP Phase II program** by applying prudent project management principles and methods.

3. Services to Be Provided (20 evaluation points; see also Sections D and E)

Table 1 summarizes the proposed work in a matrix of goals and objectives (Appendix I expands on Table 1 to detail the services to be provided at the level of specific tasks.) This format clearly illustrates the close integration of efforts and results at sector, region, and national levels.

Table 1. NCR-CIP Phase II Goals, Objectives & Key Services for Building Capacity for a More Secure and Resilient NCR

	<u>Proposed for UASI Funding</u>		<u>Proposed for Other Funding</u>
	<u>Sector-Level Tasks</u>	<u>Region-Level Tasks</u>	<u>National Integration Tasks</u>
Phase II Goals	<i>Enable owners/ operators to make the business case and invest in CIP</i>	<i>Enable achievement of regional CIP security and resilience and integrate with state, county and city strategies</i>	<i>Integrate national CIP developments with NCR regional CIP and develop/test tools for use in NCR, other regions(DHS offices with likely interest)</i>
Objectives for Phase II			
1. Assess remaining critical infrastructure sectors	Assess state of security and advance recommendations for 6 new sectors	Integrate new sectors	Develop assessment templates (IP, ODP)
2. Increase awareness of value of CIP and role of interdependencies	Conduct table top interdependency exercises for each sector	Conduct multi-jurisdictional public/private CI interdependency exercise	Develop CI awareness exercise templates(IP, ODP)
3. Form councils to coordinate decision-making	Establish Sector Coordinating Councils (public and private, each sector)	Establish public-private Sector Coordinating Councils and NCR CIP Leadership Council	Link NCR regional organization template to NIPP (IP, ODP)
4. Provide analytic decision support	Field test asset risk management/ resource allocation tool and facilitate CI decisions CIP tool kit maintenance	Field test regional risk management/ resource allocation tool s and facilitate CI decisions	Field test and evaluate tools for asset, system, and regional application (IP, S&T, ODP)
5. Facilitate implementation	Facilitate sector projects selected in 4	Facilitate regional projects selected in 4	Develop regional project implementation templates (IP, ODP)
6. Evaluate changes in NCR security and resiliency	Measure regional/sector baseline and change	Measure overall regional baseline and change	Develop evaluation templates (IP, ODP)
7. NCR-CIP program management	Develop and implement comprehensive management framework	Develop and implement comprehensive management framework	Develop and implement comprehensive management framework

Table 1 also shows the funding strategy: UASI funds are applied to the specific objectives of the NCR sectors and the NCR region, while this effort is leveraged to bring incremental funds into

the region to build, generalize and validate the NCR methods as standard templates and functionally equivalent variations for use in other regions across the country. This effort will also provide a test bed for technology that DHS has been developing to meet the needs of risk management of assets, systems and regions that are ready for testing under actual or simulated conditions that are close to actual, with real data, analysts and decision-makers. By design, the respective UASI and other DHS amounts are equal. As the other direct DHS projects are negotiating detail, this amount could vary.

II. CRITERION 2. Management Overview *(5 evaluation points; see also Sections F and G)*

George Mason University (GMU) will continue to manage the University Consortium for Infrastructure Security (UCIP), made up six NCR institutions (The University of Maryland, The University of Virginia, Howard University, Virginia Tech, James Madison University, and GMU. This team is the same team conducting NCR-CIP Phase I and represents a substantial proportion of the infrastructure and security academic expertise in the NCR. GMU's project management and reporting expertise has recently been upgraded.

III. CRITERION 3. Fiscal Management *(5 evaluation points; see also Section H)*

The budget for the integrated Phase II program is \$ 6 million over 18 months. This proposal seeks \$3 million from UASI. The other \$3 million will be sought from several offices of DHS and other federal agencies, most of which have met with the team and express interest in collaborating with the NCR. However, this project is designed to operate with only UASI funding, if required.

IV. CRITERION 4. Evaluation *(30 evaluation points; see also Sections D and E)*

Evaluation of performance, effectiveness and results is central to the strategy for Phase II. Four types of evaluation efforts will be undertaken. In ascending order of importance:

1. **Task Progress** – the extent to which the proposed activities are completed and delivered on schedule and in budget, basic project management supported by Microsoft Project and financial reporting.
2. **Task Effectiveness** – the extent to which the sets of related tasks achieve their objectives, e.g., sectors assessed, exercises conducted, councils organized, etc., the quality of those achievements as measured by satisfaction questionnaires, and the comparison of conditions before and after the task performance. (Appendix 1 details the evaluation tasks in relation to the programmatic steps.)
3. **Results** – the extent to which the NCR is made more secure and resilient will result from the coordinated efforts of many actors in the regional scene, as catalyzed by NCR-CIP Phase II and supported by the public, private and non-profit sectors over a sustained period of time. A key objective of Phase II is to define metrics and study design for this evaluation and to measure the baseline against which future measures can be compared.

V. CONCLUSION

Phase II of NCR-CIP promises to make great strides toward building the capacity for a true public/private/non-profit partnership to evaluate and make the needed decisions and investments in projects and programs – fully integrated with the national, state, county and city security strategies – to create a more secure and resilient National Capital Region.

D. Project Goals, Objectives and Implementation Steps

(Evaluation Points Addressed: Goals and objectives, 20; Services to be provided, 20; Evaluation, 30; for a total of 70 points)

I. OVERARCHING GOALS: *Build Public/Private Decision and Coordination Capacity in the NCR* (20 available evaluation points; see also Section C and E and below)

As described in Section C, the NCR-CIP project's overall goal is to contribute to the creation of a more secure, resilient National Capital Region by advancing critical infrastructure security at the asset, system and regional levels. Phase I is defining specific needs at each level. The ***overarching goal of Phase II***, proposed here, is ***to build the capacity to make and carry out the public/private coordinated decisions needed to create greater resilience and security within an accountable and transparent management framework***. It does this by *completing* the state-of-security assessments for the *sectors not yet assessed* and *establishing* for all sectors, and the region as a whole, the *awareness, organization and decision support tools* to enable the needed decisions to be made by the public and private sector leadership of the NCR. It then integrates these decisions with the policies and programs of the nation and the respective states, counties, and cities of the NCR.

These overarching goals directly contribute to the goals and strategy of the NCR. The ***Eight Commitments to Action*** identified critical infrastructure protection as a high priority strategy: "Infrastructure protection – work in partnership with the private sector to jointly identify and set protection priorities and guidelines for infrastructure assets and services in the NCR." It also stressed: "citizen involvement, collaborative decision-making, exercises that are inclusive of all levels of government, ... schools and universities, health care institutions, and other private and non-profit partners as appropriate." The ***NCR Urban Area Homeland Security Strategy*** set as strategic objectives to "reduce the NCR's vulnerability to terrorism" and "minimize the damage and recover from attacks that do occur" – both pointing to improving the resilience and security of critical infrastructure.

II. SPECIFIC GOALS, OBJECTIVES AND IMPLEMENTATION STEPS:

Comprehensiveness, Awareness, Organization, Decisions and Evaluation (Available evaluation points: Goals and objective, 20; Services to be provided, 20; Evaluation, 30; see also Sections C and E)

According to the format requirements in RFA #05 Appendix D, the following narrative description is in three-level outline form. The third level (implementation steps) is designated using letters and numbers because most tasks at the sector level apply to all sectors, individually. These are designated "S." For consistency, regional (R), evaluation (E) and national (N) tasks are similarly designated. A matrix overview showing how each step relates to goals, objectives and other tasks as well as overall integration can be found in Appendix I.

1. GOAL 1. Enable owners/operators to make the CIP business case and implement & evaluate the CIP decisions in up to 15 sectors

Objective 1.1. Assess remaining critical infrastructures and key asset sectors

S1.1 Evaluate the state of security in the sectors not yet analyzed; advance recommendations for tools, incentives and cooperative decision-making

Objective 1.2. Increase awareness of value of CIP and impact of interdependencies

S2.1 Form *ad hoc* working groups of owners/operators in each sector

- S2.2 Validate Phase I findings and recommendations with *ad hoc* sector groups
- S2.3 Plan sector-level public/private interdependency table top exercises (meetings and workshops)
- S2.4 Conduct sector-level public/private table top interdependency exercises
- S2.5 Conduct sector-level after-action reviews and make recommendations
- S2.6 Integrate Phase I sector-level findings and recommendations with recommendations from the sector exercise to form sector action plans and organization

Objective 1.3. Initiate and facilitate councils for deliberations, coordination and decision-making

- S3.1 Facilitate self-organization of NCR Owner/Operators Sector Coordinating Councils from the *ad hoc* sector working groups
- S3.2 Facilitate self-organization of NCR Government Sector Coordinating Councils (sector specialists from NCR jurisdictions, possibly to include CoG committees or R-Serfs)
- S3.3 Prioritize sector action plans from S2.6: including, possibly, standards, methods, incentives, governance, policy recommendations and risk reduction projects; decide which actions are to be carried out within the sectors and which are to be referred to the NCR CIP Leadership Council – responsibilities and budget for near-term, mid-term and long-term actions

Objective 1.4. Provide analytic decision support – metrics, models and methods

- S4.1 Assess, operate, maintain and enhance CIP tool kit from Phase I – online library, evaluation, and database of vulnerability and risk assessment tools and CIP literature
- S4.2 Support adoption/adaptation of methods selected by each sector in S3.3 action plans; introduce preliminary relative risk methods
- S4.3 Provide access to and support the database of S4.1 for the District of Columbia, State of Maryland and Commonwealth of Virginia to use as the basis of field tests
- S4.4 Field test ASME’s RAMCAP and Sandia’s tools at asset and system levels in each of three volunteer sectors
- S4.5 Leverage existing risk and decision support capabilities to developed risk visualization and communication tools for owner/operators of CIs
- S4.6 Integrate more advanced risk management at asset and system levels as they are demonstrated to be effective

Objective 1.5. Facilitate implementation of selected field pilot tests

- S5.1. through S.5.n **Implementation step 1 through n** To be defined in Phase I and above and selected in S3.3 and R3.4

Objective 1.6. Conduct evaluation of changes in NCR’s CIP security and resiliency

- S6.1 Establish an empirical baseline of NCR security and resiliency for the CI sectors – methods to be defined in Phase I
- S6.2 Measure change from baseline on regular schedule over time

2. GOAL 2. Enable achievement of regional CIP security and resilience based on full regional benefits and costs

Objective 2.1. Assess remaining critical infrastructures and key asset sectors

- R1.1 Integrate the new sectors into the regional efforts. Identify important interdependencies and interactions

Objective 2.2. Increase awareness of value of CIP and impact of interdependencies

R2.1 Form *ad hoc* cross-sector working group of owner/operators and public officials to plan interdependency table top exercises

R2.2 Determine community and non-profit stakeholders for table top exercise

R2.3 Plan cross-sectoral public/private/non-profit interdependency table top exercise (meetings and workshop)

R2.4 Conduct all-region public/private/non-profit interdependency table top exercise

R2.5 Conduct region-level after-action review and make recommendations

R2.6 Integrate Phase I region-level findings and recommendations with recommendations from the regional exercise to form the regional action plan and organizational design for a public/private/non-profit collaboration

Objective 2.3. Initiate and facilitate councils for deliberations, coordination and decision-making

R3.1 Facilitate self-organization of NCR Owner/Operators Regional Private Cross-Sector Coordinating Council from *ad hoc* cross-sector working group (possibly expanding from Board of Trade Emergency Preparedness Committee)

R3.2 Facilitate self-organization of NCR Government Cross-Sector Coordinating Councils from leaders, managers and sector specialists from NCR jurisdictions Council (possibly leaders from SPG, CAOs, Emergency Preparedness Council)

R3.3 Facilitate self-organization of NCR CIP Leadership Council from the NCR Owner/Operator Council and the NCR Government

R3.4 Prioritize cross-sector and regional action plans from R2.6 – responsibilities and budgets for near-term, mid-term, and long term actions; prioritize the recommended risk-reduction projects S3.3

Objective 2.4. Provide analytic decision support – metrics, models and methods

R4.1 Establish and validate metrics for valuing and evaluating risk-reduction projects using risk portfolio concepts, benefit-cost ratios, and other pertinent management metrics

R4.2 Support use of preliminary relative risk methods in Leadership Council resource allocation deliberations in the near term, awaiting more advanced methods

R4.3 Evaluate National Labs’ CIP/DSS, NISAC models, GIS-based methods and econometric approaches as tools for understanding and analyzing interdependencies and consequences of CI disruptions in the NCR

R4.4 Field test National Labs’ CIP/DSS (and possibly others) as risk management tool for cross-sector regional application

R4.5 Leverage existing risk and decision support capabilities to developed risk visualization and communication tools for regional decision makers

R4.6 Integrate more advanced risk management at system-to system and regional levels as they are demonstrated to be effective

Objective 2.5. Facilitate implementation of selected field pilot tests

R5.1 Conduct “Red Team” focused assessments and initiate risk reduction planning on top regional priorities

R5.2 through R5.n Implementation step 1 through n To be defined in Phase I and above and selected in R3.4

Objective 2.6. Conduct evaluation of changes in NCR’s CIP security and resiliency

R6.1 Establish an empirical baseline of NCR security and resiliency for the region as a whole – methods to be defined in Phase I

R6.2 Measure change from baseline on regular schedule over time

3. GOAL 3. Develop, test, evaluate and document the NCR processes and tools for tailored application in other regions

Note: () indicated initiative to be proposed to alternate entity for funding

Objective 3.1. Assess remaining critical infrastructures and key asset sectors

N1.1 Develop generic template for assessing the state of sector security and variations for adapting it to the respective sectors (Infrastructure Protection Directorate at the Department of Homeland Security (IP))

Objective 3.2. Increase awareness of value of CIP and impact of interdependencies

N2.1 Develop generic template and variations for organizing *ad hoc* sector-specific and cross-sector planning groups for awareness planning (IP)

N2.2 Develop generic template and variations for validating state of security evaluations (IP)

N2.3 Develop generic template for using table top exercises to raise awareness of interdependencies and action planning and organizing of public/private/non-profit partnerships (IP, Office of Domestic Preparedness (ODP))

Objective 3.3. Initiate and facilitate councils for deliberations, coordination and decision-making

N3.1 Define relationships of NCR councils and their counterpart NIPP Councils, especially at the leadership level (IP)

N3.2 Develop template and variations for organizing and chartering regional sector and cross-sector CIP organizations that can deliberate and make coordinated decisions, while retaining accountability (IP)

Objective 3.4. Provide analytic decision support – metrics, models and methods

N4.1 Evaluate the NCR CIP tool kit as an aid in supporting CIP planning for assets, systems, sectors and regions for use in other regions (IP)

N4.2 Apply as a case study preliminary relative risk methods for asset and regionally coordinated resource allocation (IP, Science and Technology Directorate (S&T))

N4.3 Expand scope and collaboration in R4.3 to serve as test bed evaluating and enhancing the interdependency and consequence estimation models for use in NCR and other regions (S&T, IP)

N4.4 Expand scope and collaboration in S4.3 to serve as test bed evaluating and enhancing asset and system risk management methods for use in NCR and other regions (S&T, IP, ODP)

N4.5 Expand scope and collaboration in R4.4 to serve as test bed for evaluating and enhancing regional risk management methods for use in NCR and other regions (S&T, IP, ODP)

N4.6 Expand scope of S4.5 and R4.5 to improve visualization and communication of CI risk and the value of CI risk reduction in resource allocation decision-making in NCR and other regions (IP, S&T)

N4.7 Develop a template and variations for integrating risk management into resource allocation decisions at the asset, system, multi-system and region level for use in the NCR and other regions (IP)

Objective 3.5. Facilitate implementation of selected field pilot tests

N5.1. through N5.n Implementation step 1 through n Field case studies in CIP for application to regions throughout the U.S. (IP and Sector Specific Agencies)

Objective 3.6. Conduct evaluation of changes in NCR's CIP security and resiliency

N6.1 Develop a template and variations for defining an empirical baseline for CIP evaluation – methods to be defined in Phase I (IP, S&T)

N6.2 Develop template and variations for empirically evaluating changes in asset and regional security and resilience over time (IP, S&T)

4. GOAL 4. Assess efficiency and effectiveness of task performance and outcomes

Objective 4.1. Assess remaining critical infra-structures and key asset sectors

E1.1 Present for acceptance by the SPG and CAOs that all remaining sectors have been assessed for state of security

Objective 4.2. Increase awareness of value of CIP and impact of interdependencies

E2.1 Assess *pre-exercise* level of awareness of cross-sector interdependencies among key leaders, managers and planners of owner/operators and public agencies

E2.2 Assess *post-exercise* level of awareness of cross-sector interdependencies among key leaders, managers and planners of owner/operators and agencies. Differences between pre and post evaluate effectiveness in raising awareness

Objective 4.3. Initiate and facilitate councils for deliberations, coordination and decision-making

E3.1 Assess *pre-organization* frequency of interactions and CIP decision-relevance of interactions among owner/operators within and across sectors and between them and public and non-profit stakeholders

E3.2 Assess *post-organization* frequency and CIP decision-relevance of interactions among owner/operators within and across sectors and between them and public and non-profit stakeholders. Differences between pre and post evaluate contribution of NCR CIP organization to CIP decisions

Objective 4.4. Provide analytic decision support – metrics, models and methods

E4.1 Document current methods for allocating resources to CIP used by NCR owner/operators, jurisdictions and cooperative regional organizations

E4.2 Evaluate effectiveness of relative risk methods in sector and regional resource allocation decision-making.

E4.3 Assess the applicability of field-tested methods for evaluating risk and valuing CIP assets and systems of the NCR

E4.4 Assess the applicability of CIP/DSS (and any other tested) to the multi-system and regional resource allocation decisions of the NCR

E4.5 Evaluate the effectiveness of tested methods in visualizing and communicating risk and risk-reduction value

E4.6 Assess the state of practice in each sector and across the region in adopting risk management methods for allocating resources for risk-reduction

Objective 4.5. Facilitate implementation of selected field pilot tests

E.5.1. through E5.n To be defined bases on specific project plans

Objective 4.6. Conduct evaluation of changes in NCR's CIP security and resiliency

E6.1 Establish an evaluation design and plan for long term assessment of progress toward greater NCR CIP resilience and security

E6.2 Execute evaluation plan

E. Project Description

(Evaluation points addressed: Statement of need, 20; Services to be provided, 20; Evaluation, 30; for a total of 70 points)

I. RELATIONSHIP TO NATIONAL INITIATIVES: *National Importance of Critical Infrastructure Protection in the NCR* (Available evaluation points: Statement of need, 20; see also Sections C and D)

As the location of critical government infrastructure, of significant economic activity, and of monuments and icons with high symbolic and political importance, the NCR is at the center of the nation's ongoing focus on homeland security relative to the terrorist attacks of September 11, 2001, and subsequent anthrax attack. The challenges for increasing the NCR's readiness have been outlined in a *GAO-Report (04-433)* which strongly advises the development of coordinated strategic planning and performance standards within UASI and other programs; observing that the NCR does not have a set of accepted benchmarks and best practices to identify desired goals.¹ Supporting the planning capabilities of the NCR Senior Policy Group (SPG) and other NCR groups regarding critical infrastructure protection is identified as a priority for Phases I and II. On a national level, critical infrastructure protection is mandated through various homeland security policies, legislation and plans.

The *National Strategy for Homeland Security* identifies eight initiatives under CIP mission area. The complexity of the homeland security issue is demonstrated by the fact that all of the initiatives are covered by at least four federal departments' planning or implementation activities. At the same time, there is a need for more coordination and leadership, in particular regarding initiatives that shall enable effective partnership with state and local governments and the private sector². The purpose of the NCR-CIP is to address this very need for the NCR. It will facilitate the integration of policies, programs, and plans that have been developed at the Federal, State, and local levels with the needs of the NCR. Findings from NCR-CIP Phase I and other ongoing research and regional exercises support the requirement for a cooperative, public/private/non-profit risk management approach.

The NCR-CIP project's overall goal is to create a more resilient National Capital Region by advancing critical infrastructure security at the asset, system and regional level. This directly supports *Homeland Security Presidential Directive 8 (HSPD) 8* policy of outlining actions to strengthen preparedness capabilities of Federal, State, local, and private sector entities.

NCR-CIP also responds to findings of the *9/11 Commission*, which observed that "[b]ecause 85 percent of our nation's critical infrastructure is controlled not by government but by the private sector, private-sector civilians are likely to be the first responders in any future catastrophes (p.317)." Among other measures, it then recommends the following regarding infrastructure protection on the Federal, State, and local level: sharing [of information] across the private sector, and by agencies to the private sector (p.394); allocation of funding should be based on assessment of threats and vulnerabilities, therefore we need metrics (criteria) to measure risk and vulnerability that assess all of the many variables (p.396); and removing obstacles to multi-jurisdictional response in areas such as the NCR (p.397)

¹ GAO 2004: p.24

Homeland Security Presidential Directive 7 (HSPD-7) required that DHS produce a comprehensive, integrated national infrastructure protection plan that includes the following elements: (a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructures with Federal agencies, State and local governments, and the private sector; and (b) a summary of activities to be undertaken in order to define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure. The **National Infrastructure Protection Plan** (NIPP) now published in “interim” form, constitutes this plan. The NIPP includes: First, a broadly defined, five-step *risk management* approach, very similar in concept to that contemplated for the NCR that serves as its principal process. Second, an organization to implement the plan, with sector-specific councils for owners/operators and government, respectively, coordinated by cross-sector councils of the respective parties, which in turn are coordinated by a national NIPP leadership council, representing all the CIP stakeholders, public and private.

In addition to these federal programs, the DHS and other agencies have sponsored the development of a number of analytic tools that, in their specifications and initial demonstrations, appear appropriate to meeting both national needs for tools to implement risk management in critical infrastructures and the NCR need for analytic tools. In Phase I, a review of these is being conducted: Initial findings are that the fit to the NCR needs is very promising.

These tools include: (1) specialized sector-specific Risk Analysis Method (RAM) at Sandia Laboratory for specific assets in water plants, dams, power plants, and nuclear facilities; (2) a generic Risk Analysis Method for Critical Asset Protection (RAMCAP) with specific adaptations being developed for assets in each specific infrastructure sector; and (3) a Critical Infrastructure Protection Decision Support System (CIP/DSS) for multi-sector regional risk management and more detailed models of individual infrastructures, under development by a consortium of National Laboratories.

Both the NIPP planners and the managers of the tool development have recognized the need for a regional component to both the NIPP process and organization and thorough testing in actual regional settings – presenting an unparalleled opportunity for the NCR to leverage its resources through cooperation with these Federal initiatives.

NCR-CIP Phase II activities will contribute to the implementation of the NIPP by using a risk management framework as the underlying logic for the asset, system and regional CIP strategy and to building analytic and decision capacity in the NCR. NCR-CIP has adopted a conceptually and functionally similar organizational approach (see Appendix II) to bringing together the business, government and non-profit communities for information sharing, coordination and joint priority-setting and decision-making. In the portion of the NCR-CIP Phase II program proposed for funding outside of the present UASI grant, NCR-CIP further complements the NIPP by using NCR’s experience (along with case studies of other regional public/private security programs) to define a *template* for a **Regional Infrastructure Protection Plan**.

Further, the approach and methodologies used by NCR-CIP are functionally aligned with federally sponsored CIP tool and process developers. Also in the portion on the NCR-CIP Phase II program proposed for funding complementary to the present UASI grant are plans to *test federally sponsored CIP tools* that appear to meet NCR specific needs. Depending on successful negotiations with several DHS offices and tool developers, these may include some or all the above tools. These evaluations will facilitate greater understanding of complex infrastructure

systems, allowing the NCR to develop new avenues for mitigation and consequence management.

II. REGIONAL PROTECTION PRIORITIES:

1. Needs and Guidance Driving NCR-CIP Phases I and II (Available evaluation points: Statement of need, 20, see also Section C)

With its efforts, NCR-CIP contributes to the stated ***NCR Goals and Objectives*** by ensuring preparedness planning efforts across the NCR, including the public, business and nonprofit sectors, which clearly define roles, relationships, processes and actions with deadlines.³ Its focus is on two of the ***NCR Commitments to Action*** – Decision-Making and Coordination, and Infrastructure Protection.⁴ It provides decision support to public and private CI owners by designing and facilitating sector and government coordinating councils, and helps to jointly identify and set protection priorities and guidelines for infrastructure assets and services in the NCR. In fact, the NCR-CIP is one of very few projects within the NCR’s UASI Phases I and II to develop strategies for critical infrastructures and their private and public sector owners⁵.

In Phase I, and continuing in Phase II, the NCR-CIP university consortium is *assessing vulnerabilities and protection in eight critical infrastructures* in the region (increasing to 14 in Phase II) to identify needs and options for tools, incentives and governance to assist infrastructure owners and operators to make the required decisions and investments to secure their assets and systems. It is also defining a strategy for enhancing the capability of the NCR as a region to identify, select, finance and coordinate risk reduction initiatives to be funded by business, non-profit organizations and governments at municipal, state and federal levels. The proposed work, then addresses the following of the list from the RFA:

- Assess vulnerability of and harden critical infrastructure
- Establish/enhance cyber security programs
- Establish/enhance public-private emergency preparedness programs
- Establish/enhance sustainable homeland security exercise programs
- Establish/enhance sustainable homeland security planning programs

2. Need for Decision-Making Organization and Tools Addressing Investments and Interdependencies

The critical infrastructure sectors in the National Capital Region vary widely in their approaches to vulnerability and risk reduction. The area of greatest underestimation and underinvestment is interdependencies – the reliance on other sectors’ performance to continue to provide critical services. Owners and operators of CI in many cases have not yet fully recognized, built, and acted on the business case for their own protection, and the NCR as a region lacks the planning and coordination framework to recognize, analyze and act on vulnerabilities that are not addressed by individual owners for lack of a business case. However, the protection of these infrastructures is vital to the NCR’s viability and functioning.

³ NCR Goal 1, Objective 1.1

⁴ NCR Commitments to Action 3 and 5

⁵ The current NCR-CIP project accounts for only about 2% -- 3% if the complementary Justice Department COPS grant is included -- of the nearly \$ 100 million dollars in UASI funds to date.

Based on state and national homeland security policies as well as other findings of Phase I of the NCR-CIP project, the following regional problems need to be addressed:

- (a) Virtually all the critical infrastructures must be included for the region to be as secure as needed because all are related through dependencies; no infrastructure is self-sufficient.
- (b) Sector level security needs to be significantly improved in virtually all sectors currently being studied.
- (c) Each sector must recognize and deal with interdependencies as they set CIP goals and risk reduction programs for their assets and systems
- (d) Sector-level CIP initiatives must be complemented by region-wide, multi-jurisdictional, public/private initiatives for the region to reach the desired level of security and resilience.

III. SPECIFIC OBJECTIVES AND IMPLEMENTATION STEPS OF PHASE II:

Derived Directly from Homeland Security Policies and the Needs and Findings Defined in Phase I (Available evaluation points: Goals and objectives, 20; Services provided, 20; total of 40; see also Sections C and D and Appendix I.)

The Phase II specific objectives and implementation steps are derived directly from these needs. The design of the project is purposefully parallel activities at the sector, region and national levels. (See also Section C and Appendix A for discussion of the goals, objectives, and implementation steps.) The specific objectives and broad implementation steps are:

- a) Assess state of security and gaps in the **sectors yet to be included** – agriculture and food, national monuments and icons, defense industrial base, information technology, government facilities, and commercial facilities – and integrate them with the eight assessed in Phase I.
- b) Enable **each sector** to enhance its **ability to make and act on the business case for CIP** by increased understanding, defining a coordinating decision body, the analytic tools to support the decisions, and facilitation in implementation and evaluation, i.e.:
 - i) Raising **awareness** of which assets and systems are critical, the value of CIP and the impact of interdependencies on security
 - ii) Developing public and private sector **councils** to share information, deliberate and decide on CIP options and to represent the interests of the sector in regional CIP deliberations and decisions
 - iii) Providing the **analytic tools and metrics** to determine vulnerabilities and risks and to evaluate risk-reduction programs as investments
 - iv) Facilitating **implementation** of the selected risk-reduction programs and
 - v) Performing **evaluation** of them for effectiveness and enhancement
- c) Enable the NCR to achieve a higher level of **resilience and security** as justified by the full **regional benefits and costs**, by (in parallel and coordination with the sector level needs):
 - i) Raising **awareness** of which assets, systems and sector operations are critical to the NCR as a whole, the value of CIP and the impact of interdependencies on regional security and resilience
 - ii) Developing public and private cross-sector **councils** and a public/private/non-profit leadership council to deliberate and decide on CIP options and to represent the interests

of the NCR in national CIP deliberations and decisions, especially the national Infrastructure Protection Plan organization and process.

- iii) Providing the regional *analytic tools and metrics* to determine vulnerabilities and risks and to evaluate NCR risk-reduction programs as investments
- iv) Facilitating *implementation* of the selected risk-reduction programs starting with “red teams” for the highest priority regional infrastructures
- v) Performing *evaluation* of them for effectiveness and enhancement
- d) Apply best efforts to augment the NCR’s funds and expertise through *collaboration with the Federal Government* to use the NCR as
 - i) A prototype to define a series of *templates* and variations for use in other regions (including integration with the NIPP process and organization)
 - ii) A *test bed* to evaluate and enhance advanced *risk management tools* for use in the NCR and other regions

In addition, the following cross-cutting tasks contribute directly to achieving goals a) to d):

- e) Facilitate *pilot implementation* – to be defined later in Phase I. Appendix Q is a list of preliminary concepts for future risk reduction projects. These and others will be validated, prioritized and some selected for testing and implementation.
- f) *Evaluate changes* in the NCR’s level of security and resilience – establish baselines for later comparison on key metrics (being defined later in Phase I).
- g) Provide a *clearinghouse* for vulnerability assessment and risk management information and guidance.
- h) Provide *direct technical assistance* to government and infrastructure service providers in the form of subject matter consultation, priorities, assessments, modeling, cost-benefits analysis, upgrades, and maintenance.

IV. EVALUATION: Gauging the Effectiveness of Meeting Each Major Objective and Setting a Baseline for Future Region-Wide Assessments of Change

(Available evaluation points: Evaluation,30; see also Section D and Appendix I)

Evaluation of performance, effectiveness and results is central to the strategy for Phase II. Three types of evaluation efforts will be undertaken. In ascending order of importance:

1. **Task Progress** – the extent to which the proposed activities are completed and delivered on schedule and in budget, basic project management supported by Microsoft Project and financial reporting.
2. **Task Effectiveness and Enhancement** – the extent to which the sets of related tasks achieve their objectives, e.g., sectors assessed, exercises conducted, councils organized, etc., the quality of those achievements as measured by satisfaction questionnaires, and the comparison of conditions before and after the task performance. (Appendix I details the evaluation tasks in relation to the programmatic steps.)
3. **Results** – the extent to which the NCR is made more secure and resilient will result from the coordinated efforts of many actors in the regional scene, as catalyzed by NCR-CIP Phase II and supported by the public, private and non-profit sectors over a sustained

period of time. A key objective of Phase II is to define metrics and study design for this evaluation and to measure the baseline against which future measures can be compared.

The first type will be performed in a continuous manner under Objective 7, Program management. The second and third types are defined in detail as the “E”-designated tasks in Section D and Appendix I. To summarize by objective:

1. Assess **remaining sectors**: The extent to which the assigned sectors are assessed for their state of security and integrated with those assessed in Phase I
2. **Awareness** of value of CIP and impact of interdependencies: Survey attitudes and knowledge base on CIP and interdependencies – *before* and *after* the exercise series – among leaders, managers, planners and security officers of NCR infrastructure owner/operators, non-profit leadership and government officials at city, county, and state levels.
3. Facilitate **councils** for information sharing, deliberations, and cooperative decision-making: the number of sectors and cross-sector councils formed relative to the number in the organization design; and, more importantly, surveys – before and after the organizational efforts – of frequency and decision-relevance of interactions among decision-makers within and across sectors and between them and public and non-profit decision-makers.
4. Provide **analytic decision support** – comparison of currently used methods for evaluating and selecting risk reduction initiatives and those used in tests of analytic tools through to actual or simulated decisions; and assessments of the extent to which the tested tools contribute to more effective decision-making.
5. Facilitate **implementation** – to be defined in Phase II on a project-by-project basis.
6. **Evaluate changes** in NCR’s infrastructure security and resilience -- establish an evaluation design, metrics and plan for long term assessment of progress and knowledge management toward greater NCR CIP resilience and measure a baseline for future comparisons at both sector and NCR-wide

These plans are a major commitment to high quality project management, efficiency and effectiveness of execution, accountability for results, and learning over time for what works and what does not.

V. PROGRAM INTEGRATION: *Phasing, Temporal Precedence Relationships and Resource Allocation*

(Available evaluation points: Goals and objectives, 20; Services to be provided, 20; Management overview, 5; Evaluation. 30; total, 75)

The work described in this proposal is a highly integrated program designed to build the framework of shared awareness, organization and decision support tools to realize a cooperative public/private/non-profit partnership for a more secure and resilient National Capital Region.

Phase II core task funding is sought from UASI at the same level as Phase I (when including the integrated COPS funds), so the basic program can proceed in the absence of incremental resources. Additional resources will be sought from DHS and other sources to enhance and augment the core tasks.

Table 2 displays the core UASI funding and the complementary funding by goal and objective. It is clear that the core work to build the capacity and framework for cross-jurisdictional, public/private/non-profit cooperation and coordination will be completed regardless of the results

of the incremental funding, but that the incremental resources contribute to both NCR and national purposes.

The program of tasks is also integrated by clearly defining the precedence relationships among the respective tasks. Figure 1 is a slightly summarized Gantt chart showing these relationships and the overall schedule of task performance.

NCR-CIP Phase II is planned for completion in eighteen months from the date of grant signature. For costing purposes, we have assumed that start date would be June 1, 2005, to exploit the availability of senior researchers in the summer period. Completion will be largely determined by the decisions of the participating stakeholders.

These exhibits underscore the full integration of goals and objectives, tasks, schedule, and resources. Additional integration will be developed with the state, county and city homeland security plans.

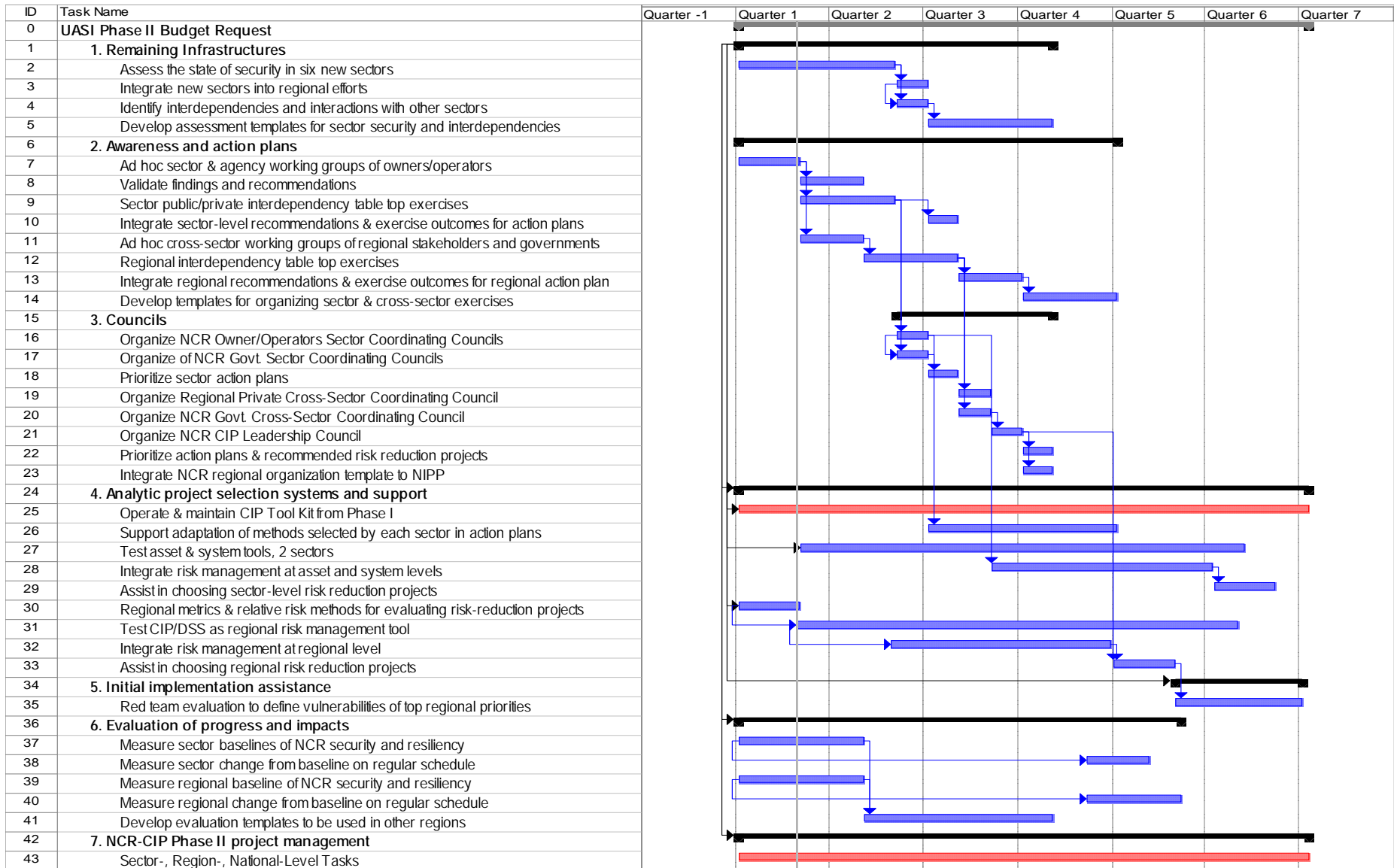
Table 2. Distribution of Requested Funding by Funding Source, Goal, and Objective

Proposed Funding Source	<u>Proposed for UASI Funding</u>				<u>Proposed for Other Funding</u>	Total Program by Objective
	<u>Sector-Level Tasks</u>	<u>Region-Level Tasks</u>	<u>Evaluation Tasks</u>	<u>Total UASI by Objective</u>	<u>National Integ. Tasks</u>	
Goals Objectives	<i>Owners' CIP business case</i>	<i>Regional CIP & integration</i>	<i>Efficiency effectiveness & outcomes</i>		<i>NCR-National CIP integration</i>	
1 Remaining sectors	\$ 500	*	*	\$ 500	\$ 80	\$ 580
2. Increase awareness	300	\$ 185	\$ 40	525	175	700
3. Form councils	145	35	40	220	80	300
4. Decision support	305	140	80	525	1,940	2,465
5. Facilitate implement.	**	335	**	335	600	935
6. Evaluate changes	135	135	25	295	125	420
Subtotal by GOAL	1,385	830	185	2,400	3,000	5,400
7. Program management				600		600
TOTAL by GOAL & Mngmt.	\$ 1,385	\$ 830	\$ 185	\$ 3,000	\$ 3,000	\$ 6,000

* Included in Project Management

**Projects to be funded outside of present program as selected in tasks above

Figure 1. NCR-CIP Phase II Summary Schedule



F. Organization, Experience and Qualifications of Applicant

*(Management overview: 5 pts, including section g; Fiscal management: 5 pts, with section h;
TOTAL: 10 points max.)*

In NCR-CIP Phase II, the University Consortium for Infrastructure Protection (UCIP) will build on the significant foundation established in Phase I to address critical infrastructure protection on the regional level. The proposed efforts for Phase II will leverage the proven methodology utilized in the research activities in Phase I as well as relationships established with infrastructure owners and operators and other regional stakeholders in order to maximize effectiveness.

The UCIP consists of over 25 senior researchers plus post-doctoral fellows and graduate research assistants (for position descriptions, see Appendix V) from the following leading research institutions in Maryland, the District of Columbia, and Virginia:

- George Mason University
- James Madison University
- Howard University
- University of Maryland
- Virginia Polytechnic Institute and State University (VA Tech)
- University of Virginia

Each member university brings to the consortium a unique expertise in the area of Critical Infrastructure Protection, consolidating significant regional competence. George Mason University will continue to manage the overall effort, coordinating, integrating and mobilizing the academic community, as well as other resources as directed by the SPG. The UCIP is housed within the GMU Critical Infrastructure Protection Program (GMU-CIPP), a separately funded project, and provides the UCIP with a strong intellectual and program base. The GMU-CIPP remains a national leader in the area of critical infrastructure protection since its inception prior to September 11th. Its mission is to engage the international research community to find practical solutions to challenges in critical infrastructure protection faced by both government and industry stakeholders. With particular emphasis on the complexities of the public-private relationship, the CIP Program has sponsored interdisciplinary and multi-institutional research within 11 academic units at GMU and at 14 universities nationwide, funding a total of 77 professors and over 200 research assistants and students.

Further, James Madison University is home to the Institute for Infrastructure and Information Assurance, which offers a curriculum around issues in critical infrastructure protection and information security. The Alexandria Research Institute of Virginia Tech includes the World Institute for Disaster Risk Management focused on enabling people to anticipate disasters and take protective actions, as well as the Critical Infrastructure Modeling and Assessment Program (CIMAP), a new initiative to assess critical infrastructures in Northern Virginia. The Critical Incident Analysis Group at the University of Virginia is a consortium composed of scholars, law enforcement officials (including the U.S. Justice Dept. and FBI), and professionals, such as therapists and psychiatrists, who specialize in analysis, prevention, and mitigation of critical incidents. Finally, among other areas of expertise, the University of Maryland has significant capacity in risk and decision analysis as well as engineering and is the home of: a DHS Center of Excellence in Homeland Security, the Center for International Security Studies, the Maryland

Fire and Rescue Institute, the Center for Supply Chain Management, and is manager of CAPWIN.

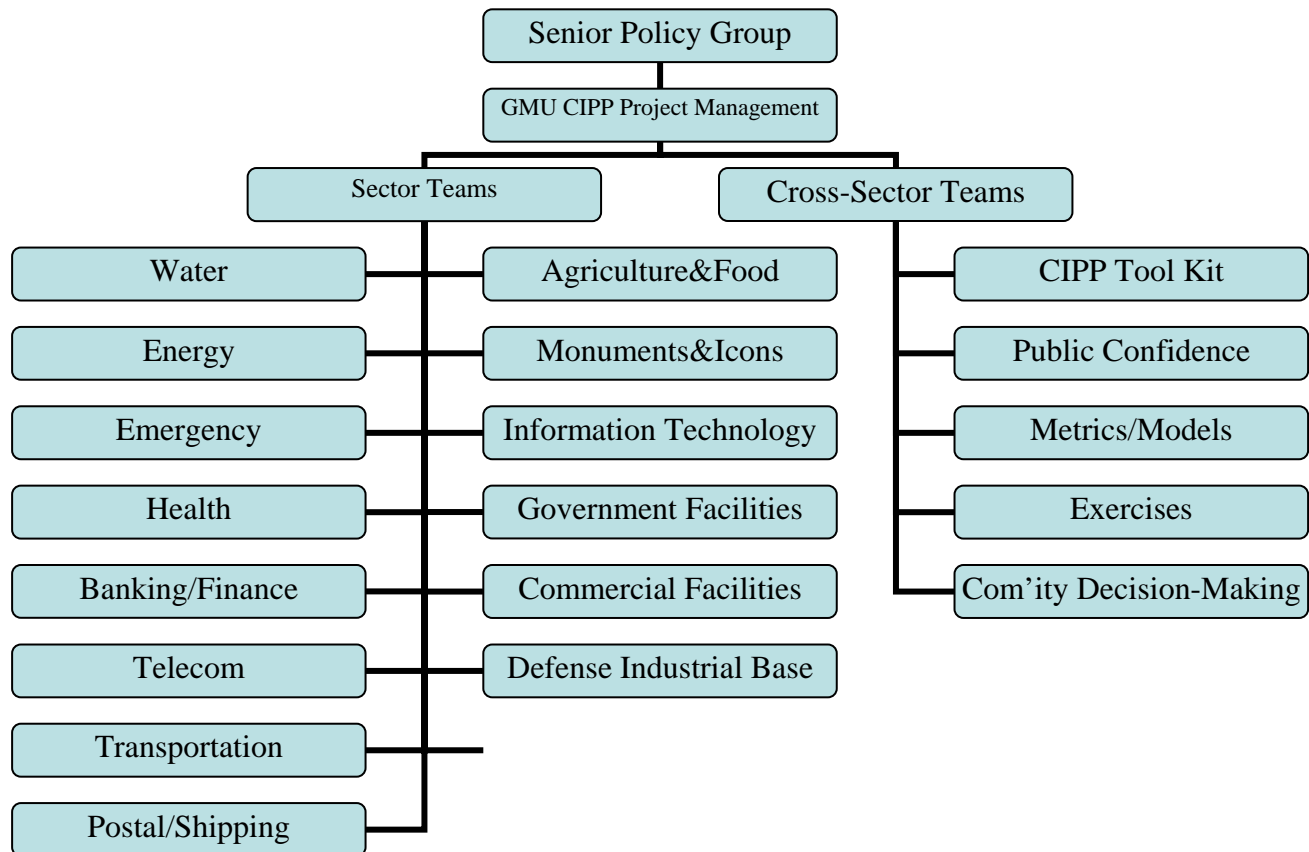
Phase II will be also complemented by key subcontractors who bring subject matter expertise in a particular area. (Please see Appendix III for allocation of resources to project participants.)

The Project’s Principal Investigator is John McCarthy, Director of the GMU-CIPP. The Project Director is Dr. Jerry Paul Brashear, Associate Director for the GMU-CIPP. Under Mr. McCarthy’s and Dr. Brashear’s leadership, the NCR-CIP management team, which consists of five staff members, coordinates the project deliverables and liaises with local, state, and Federal authorities, the private sector, and the research community at large.

The senior researchers have served as team leaders of the eight critical infrastructure sectors focused on to date, and additional expertise will be added to address the five new sectors to be undertaken in Phase II. An additional five of senior researchers lead cross-sector projects ranging from analytical modeling to citizens’ panels. The team leaders have the overall responsibility for the research and development activities, and as recognized subject matter experts in their specific area of expertise they will support the sector coordinating councils to be set up in Phase II (for senior researchers’ biographical information, see Appendix VI). Each team contains of at least one other senior researcher, plus several research fellows and assistants.

For management purposes, the project organization is set up as follows:

Figure 2. NCR-CIP Phase II Organization



G. Staffing Plan

(Management overview: 5 points, including section e, above)

This list contains all project staff; the following two sections B. specify the roles and responsibilities of the GMU project management and non-GMU senior researchers and consultants, respectively.

Table 3. Staffing

Name	Adv. Degree	Yrs. of Exp	Area of Expertise	Primary Sector or Task	Function
PJ Aduskevicz	B.A.	25+	Network Reliability, Disaster Recovery	Telecom	Subcontractor
Philip E. Auerswald	Ph.D.	15	Public-Private Partnerships; Economics	Metrics/Models	Senior Researcher GMU
George Baker	Ph.D.	25+	Infrastructure Assurance, Risk Assessment Methods	Metrics/Models	Sector Team Leader JMU
Greg Baecher	Ph.D.	25+	Water Resources Analysis and Protection	Water	Senior Researcher UMD
Brien Benson	Ph.D.	25+	Intelligent Transportation Systems; Regulatory Affairs	Transport	Senior Researcher GMU
John Bigger	M.A.	25+	Public Utility Systems; Electric Power Generation and Distribution	Energy	Sector Team Leader VT
Jerry P. Brashear	Ph.D., M.B.A.	25+	Risk Management, Energy; Policy Analysis; Planning	Project Management	Project Director GMU
Ami C. Carpenter	M.A.	5	Conflict Resolution; Coordination and Facilitation	Com'ity Decision-Making	Grad. Res. Asst/Ascc GMU
Sandra Cheldelin	Ph.D.	25+	Conflict Resolution; Coordination and Facilitation	Com'ity Decision-Making	Sector Team Leader GMU
Osita B. Chidoka	M.A.	10	Logistics, Transportation Systems Planning	Transport	Grad. Res. Asst/Ascc GMU

James T. Creel	B.A.	3	Administrative and Research Support	Project Management	Grad. Res. Asst/Asst GMU
Keith Critchlow	M.A.	20	Communication and Visualization; Public Confidence	Metrics/Models	Senior Researcher VT
E. Kathy Emmons	Ph.D.	25+	Information Security; Enterprise Integration	Information Technology	Senior Researcher GMU
Jonathan L. Gifford	Ph.D.	20	Transportation, Postal & Shipping; Regulatory Affairs	Postal& Shipping	Senior Researcher GMU
Sean P. Gorman	Ph.D.	5	Network Interdependency Mapping	Telecom	Senior Researcher GMU
Kathleen Hancock	Ph.D.	15	Geographic Information Systems (GIS); Spatial Analysis	Transportation	Senior Researcher VT
Gerald A. Hanweck	Ph.D.	25+	Finance, Risk Management, Econometrics	Banking& Finance	Sector Team Lead GMU
Mark H. Houck	Ph.D.	25+	Water Security, Reservoir Operations	Water	Senior Researcher GMU
Sushil Jajodia	Ph.D.	25+	IT Systems Security; Database Modeling	Information Technology	Sector Team Leader GMU
Kathleen Kaplan	D.Sc.	10	Communication Networks; Database Systems	CIPP Tool Kit	Senior Researcher HU
Fred Krimgold	Ph.D.	25+	Building Security, Disaster Management	Emergency Services	Sector Team Leader VT
Todd M. La Porte	Ph.D.	20	Citizen Involvement; High-Reliability Organizations	Public Confidence	Sector Team Leader GMU
Andrew Loerch	Ph.D.	25+	Operations Research; Analytic Modeling	Metrics/Models	Senior Researcher GMU
John A. McCarthy	M.S	25+	Homeland Security, Risk Management	Project Management	Principal Investigator GMU

Lamine Mili	Ph.D.	25+	Supervisory Control And Data Acquisition (SCADA) for Critical Infrastructures	Energy	Senior Researcher VT
Arnauld Nicogossian	M.D.	25+	Health Systems Security, Epidemiology; Biodefense	Health	Sector Team Leader GMU
Christine Pommerening	Ph.D.	10	Research Methods, Regional Coordination	Project Management	Senior Researcher GMU
Terry Ryan	M.A.	20	Risk and Threat Assessment Methodologies	CIPP Tool Kit	Senior Researcher JMU
Gregory Saathoff	M.D.	25+	Critical Incident Response, Shelter-in-Place	Public Confidence	Sector Team Leader UVA
Paula Scalingi	Ph.D.	25+	CIP Interdependencies, Regional Scenarios and Exercises	Exercises	Subcontractor
Laurie Schintler	Ph.D.	15	Telecom Security, Analytic Modeling	Telecom	Senior Researcher GMU
Jordana Siegel	M.A	10	Sector Coordination, Management	Project Management	Senior Researcher GMU
Anoop Singhal	Ph.D.	15	Network Security, Database Modeling	CIPP Tool Kit	Senior Researcher GMU
Roger R. Stough	Ph.D.	25+	Regional Analysis and Coordination	Com'ity Decision-Making	Senior Researcher GMU
Philip J. Tarnoff	Ph.D.	25+	Communications Interoperability; Emergency and Evacuation; Transportation	Emergency Services	Senior Researcher UMD
Natasha Udu-Gama	M.A.	5	Community-based Disaster Risk Information Systems	Emergency Services	Grad. Res. Asst/Assc VT
Mohan M. Venigalla	Ph.D.	15	Transport Systems Engineering and Security	Transport	Senior Researcher GMU
Michael Willingham	Ph.D.	20	Energy Supply and Management	Energy	Senior Researcher VT

Lee Zeichner	J.D.	20	Risk Management Methods; Finance and IT Security	Banking & Finance	Subcontractor
Tom Zimmerman	Ph.D.	25+	Health Systems Assessments	Health	Subcontractor

Project Management (see Appendix V for Position Descriptions and VI for Biographical Sketches)

John A. McCarthy (George Mason University)

As CIPP Director and Principal Investigator for George Mason University, John A. McCarthy will develop the overall vision that guides the NCR-CIP activities for the duration of the grant. He will oversee the interaction of the multiple university departments at the consortium universities. He will build partnerships between the NCR-CIP and public and key private sector organizations, and will seek matching funding from other homeland security grants. John McCarthy is a recognized leader in the field of homeland security and brings to bear an extensive network of government officials, private sector executives, military personnel, academics, and other members of the critical infrastructure protection community. He has a broad understanding of economics, information security, technology policy, and security policy. He has more than ten years of executive-level experience in the area of homeland security in both public and private sector positions, and has extensive experience integrating national/international CIP planning initiatives with key federal, state, and local emergency response structures. He holds a graduate degree in information resource management.

Jerry Paul Brashear (George Mason University)

As Associate Director, Jerry Brashear is responsible for managing the National Capital Region Project (NCR-CIP), including personnel, space, equipment, and budget management, public relations, and grant oversight matters. He will coordinate the efforts of the multiple university departments at the consortium universities. He manages the administration of the grant and coordinates with the administering government agency. He will be the lead contact for building the partnerships between the public and private sector actors in the NCR. Dr. Brashear has more than thirty years of experience, specializing in energy and natural resource policy, energy taxation, R&D program planning, risk management and technology policy. He has Ph.D. in the Interdisciplinary Program in Urban, Technological and Environmental Planning from The University of Michigan. He also received his MBA from Harvard Business School and graduated *magna cum laude* and *Phi Beta Kappa* from Princeton University.

Christine Pommerening (George Mason University)

As Post-Doctoral Research Fellow, Christine Pommerening will ensure and contribute to the academic integrity and scientific validity of the project, establish and maintain relationships with the research community, and apply advanced research skills to carry out specific project tasks. Christine Pommerening holds a Ph.D. in Public Policy, and a M.A. in Sociology. Her research focuses on the development of regional and international governance structures for new technologies, and organizational and institutional theory. She has worked in research projects

evaluating and implementing EU structural fund programs, public and private sector coordination, and regional economic development.

Jordana Siegel (George Mason University)

As Senior Project Assistant, Jordana Siegel will be tasked with circulation of information, coordination of participants, and organization of project-related activities. She will provide substantive project support for all project deliverables and key activities as outlined in the goals, objectives, and implementation steps. Jordana Siegel has worked in the field of critical infrastructure protection (CIP) since November of 2002. She contributed to the production of a weekly newsletter focused on issues in homeland security and provided strategic consulting services in the field to both private sector and public sector clients. Prior to her work in CIP, she was a consultant in the telecommunications industry, serving federal government, state government, and private sector clients.

Senior Researchers (see Appendix VI for Biographical Sketches)

Greg Baecher (University of Maryland)

As senior researcher, he contributes to the assessment of the agriculture and food, information technology, transportation, and water sectors. He will build research teams within his field of expertise, providing insight gained from working within the sectors. He will contribute significantly to project deliverables, in particular risk and decision analysis, risk communications and visualization, benefit cost analysis, civil engineering, public policy, logistics and supply chain modeling, as well as other tasks as assigned.

Fred Krimgold (Virginia Tech)

As senior researcher, he is responsible for the energy, emergency response, commercial and governmental facilities sectors, national monuments and icons sectors. He leads the research teams within these sectors. He will contribute significantly to project deliverables, in particular regional modeling, analysis and planning; risk assessment, risk communications and visualization, engineering and public policy, as well as other tasks as assigned.

George Baker (James Madison University)

As senior researcher, he is responsible for defense sector, risk and vulnerability assessment methods, economic analysis, and other tasks as assigned. He will contribute significantly to project deliverables, in particular risk and vulnerability assessment, engineering and public policy, as well as other tasks as assigned.

Gregory Saathoff (University of Virginia)

As senior researcher, he is responsible for public health and safety programs, including sheltering in place, risk communications, and public confidence. He will contribute significantly to these and other tasks as assigned.

Kathleen Kaplan (Howard University)

As senior researcher, she is responsible for information technology sector, data base enhancement, modeling and analytic methods, and other tasks as assigned.

Terry Ryan (UDT, Inc.)

As technical consultant, he is responsible for engineering and security assessments, vulnerability assessment and methods, risk assessment, methodology and management, planning and regional analysis and other tasks as assigned.

Lee Zeichner (ZRA Ltd.)

As regulatory affairs consultant, he is responsible for energy, banking and finance and telecommunications sectors, policy analysis, regulatory analysis and other tasks as assigned.

Paula Scalingi (The Scalingi Group)

As regional exercise consultant, she is responsible for table top interdependency exercises, planning, security policy analysis, economic and benefit/cost analysis and other tasks as assigned

PJ Aduskevicz

As technical consultant, she is responsible for telecommunications sector security, private sector perceptions of risk and other tasks as assigned.

Tom Zimmerman

As technical consultant, he is responsible for public health services, healthcare delivery, community sheltering, and other tasks as assigned.

H. Project Budget and Budget Narrative

I. Certifications and Assurances

J. Appendices

I - NCR Critical Infrastructure Needs, Tasks to Meet Them, and Evaluation of Effectiveness in Meeting Them

II –Functional Organization Schemes for Regional-National Integration

III – Resource Allocation by Provider

IV – References

V – Position Descriptions

VI – Biographical Sketches

Appendix I – NCR Critical Infrastructure Needs, Tasks to Meet Them, and Evaluation of Effectiveness in Meeting Them

A useful way to consider the strategy of NCR-CIP Phase II is to examine it in the matrix below (which is summarized as Table 1 in Section C). The proposed project has seven objectives contributing to the achievement of each of four goals, with specific tasks to meet each goal-objective combination. Because each respective sector will be addressed individually under Goal 1, the matrix designates these tasks as “S” for sector. Correspondingly, tasks addressing regional Goal 2 are designated “R,” evaluation tasks under Goal 3 as “E,” and national integration tasks under Goal 4 as “N.” Once sector numbers are assigned, R, E and N tasks will also be numbered for project management and reporting.

<u>NCR Need</u>	<u>Proposed for UASI Funding</u>			<u>Proposed for Other Federal Funding</u>
	<u>Sector-Level Tasks</u>	<u>Region-Level Tasks</u>	<u>Evaluation Tasks</u>	<u>National Integration Tasks</u>
<i>Goals for CIP Planning</i> <i>Objectives For Phase II</i>	<i>1. Enable owners/operators to make the CIP business case and implement & evaluate CIP decisions in up to 15 sectors, individually</i>	<i>2. Enable achievement of regional CIP security and resilience based on full regional benefits and costs and integrate with state, county and city strategies</i>	<i>3. Assess efficiency and effectiveness of task performance and outcomes</i>	<i>4. Leverage and integrate national CIP developments with NCR regional CIP and develop/test tools for use in other regions</i>
1. Assess remaining critical infra-structures and key asset sectors	S1.1 Evaluate the state of security in the sectors not yet analyzed ; advance recommendations for tools, incentives and governance	R1.1 Integrate the new sectors into the regional efforts. Identify important interdependencies and interactions with sectors already studied.	E1.1 All remaining sectors having priority to the NCR SPG and CAOs have been assessed for state of security	N1.1 Develop generic template for assessing the state of sector security and variations for adapting it to the respective sectors (IP, ODP)
2. Increase awareness of value of CIP and impact of inter-dependencies	S2.1 Form <i>ad hoc</i> working groups of owners/operators in each sector S2.2 Validate Phase I findings and recommendations with <i>ad hoc</i> sector groups	R2.1 Form <i>ad hoc</i> cross-sector working group of owner/operators and public officials to plan interdependency table top exercises R2.2 Determine community and non-profit stakeholders for table top exercise	E2.1 Assess <i>pre-exercise</i> level of awareness of within- and cross-sector interdependencies among key leaders, managers and planners of owner/operators and public agencies	N2.1 Develop generic template and variations for organizing <i>ad hoc</i> sector-specific and cross-sector planning groups for awareness planning (IP,ODP) N2.2 Develop generic template and variations for validating state of security evaluations (IP, ODP)

	<p>S2.3 Plan sector-level public/private interdependency table top exercise (meetings and workshop)</p> <p>S2.4 Conduct sector-level public/private table top interdependency exercise</p> <p>S2.5 Conduct sector-level after-action review and make recommendations</p> <p>S2.6 Integrate Phase I sector-level findings and recommendations with recommendations from the sector exercise to form sector action plans and organization</p>	<p>R2.3 Plan cross-sectoral public/private/- non-profit interdependency table top exercise (meetings and workshop)</p> <p>R2.4 Conduct all-region public/private/- non-profit interdependency table top exercise</p> <p>R2.5 Conduct region-level after-action review and make recommendations</p> <p>R2.6 Integrate Phase I region-level findings and recommendations with recommendations from the regional exercise to form the regional action plan and organization</p>		
<p>3. Initiate and facilitate councils for deliberations, coordination and decision-making</p>	<p>S3.1 Facilitate self-organization of NCR Owner/Operators Sector Coordinating Councils from the <i>ad hoc</i> sector working group</p>	<p>R3.1 Facilitate self-organization of NCR Owner/Operators Regional Private Cross-Sector Coordinating Council from <i>ad hoc</i> cross-sector working group (possibly expanding from BoT Emergency Preparedness Committee)</p>	<p>E2.2 Assess <i>post-exercise</i> level of awareness of cross-sector interdependencies among key leaders, managers and planners of owner/operators and agencies. Differences between pre and post evaluate effectiveness in raising awareness</p>	<p>N 2.3 Develop generic template for using table top exercises to raise awareness of interdependencies and action planning and organizing of public/private/non-profit partnerships (IP, ODP)</p>
	<p>S3.2 Facilitate self-organization of NCR Government Sector Coordinating Councils (sector specialists from NCR jurisdictions, possibly CoG committees or R-ESFs)</p>	<p>R3.2 Facilitate self-organization of NCR Government Cross-Sector Coordinating Councils from leaders, managers and sector specialists from NCR jurisdictions Council (possibly leaders from SPG, CAOs, EPC)</p> <p>R3.3 Facilitate self-organization of NCR CIP Leadership Council from the NCR Owner/Operator Council and the NCR</p>	<p>E3.1 Assess <i>pre-organization</i> frequency and CIP decision-relevance of interactions among owner/operators within and across sectors and between them and public and non-profit stakeholders</p>	

	<p>S3.3 Prioritize sector action plans from S2.6: standards, methods, incentives, governance, policy recommendations and risk-reduction projects; decide which are to be carried out within the sectors and which are to be referred to the NCR CIP Leadership Council – responsibilities and budget for near-term, mid-term and long-term actions</p>	<p>Government</p> <p>R3.4 Prioritize cross-sector and regional action plans from R2.6 – responsibilities and budgets for near-term, mid-term, and long term actions; prioritize the recommended risk-reduction projects S3.3</p>	<p>E3.2 Assess <i>post-organization</i> frequency and CIP decision-relevance of interactions among owner/operators within and across sectors and between them and public and non-profit stakeholders. Differences between pre and post evaluate contribution of NCR CIP organization to CIP decisions</p>	<p>level (IP)</p> <p>N3.2 Develop template and variations for organizing and chartering regional sector and cross-sector CIP organizations that can deliberate and make coordinated decisions, while retaining accountability(IP, ODP)</p>
<p>4. Provide analytic decision support – metrics, models and methods</p>	<p>S4.1 Assess, operate, maintain and enhance CIP tool kit from Phase I – online library, evaluation, and database of vulnerability and risk assessment tools and CIP literature</p> <p>S4.2 Support adoption/adaptation of methods selected by each sector in S3.3 action plans; introduce preliminary relative risk methods</p> <p>S4.3 Provide access to and support the database of S4.1 for the State of Maryland and Commonwealth of Virginia to use as the basis of field cases</p>	<p>R4.1 Establish and validate metrics for valuing and evaluating risk-reduction projects using risk portfolio concepts, benefit-cost ratios, and other pertinent management metrics.</p> <p>R4.2 Support use of preliminary relative risk methods in Leadership Council resource allocation deliberations in the near term, awaiting more advanced methods</p> <p>R4.3 Evaluate National Labs’ CIP/DSS, NISAC models, GIS-based methods and econometric approaches as tools for understanding and analyzing interdependencies and consequences of CI disruptions in the NCR</p>	<p>E4.1 Document current methods for allocating resources to CIP used by NCR owner/operators, jurisdictions and cooperative regional organizations</p> <p>E4.2 Evaluate effectiveness of relative risk methods in sector and regional resource allocation decision-making.</p>	<p>N4.1 Evaluate the NCR CIP tool kit as an aid in supporting CIP planning for assets, systems, sectors and regions for use in other regions (IP)</p> <p>N4.2 Case study of application of preliminary relative risk methods for asset and regionally coordinated resource allocation (IP, S&T, ODP)</p> <p>N4.3 Expand scope and collaboration in R4.3 to serve as test bed evaluating and enhancing the interdependency and consequence estimation models for use in NCR and other regions (S&T, IP, ODP)</p>

S4.4 Field test ASME’s RAMCAP, Sandia’s tools and others at asset and system levels in each of three volunteer sectors

R4.4 Field test National Labs’ CIP/DSS (and ,possibly others) as risk management tool for cross-sector regional application

S4.5 Leverage existing risk and decision support capabilities to developed risk visualization and communication tools for owner/operators of CIs

R4.5. Leverage existing risk and decision support capabilities to developed risk visualization and communication tools for regional decision makers.

S4.5 Integrate more advanced risk management at asset and system levels as they are demonstrated to be effective

R4.6 Integrate more advanced risk management at system-to system and regional levels as they are demonstrated to be effective

5. Facilitate implementation of selected field pilot tests

S5.1...S5.n To be defined in Phase I and above and selected in S3.3 and R3.4

R5.1 Conduct “Red Team” focused assessments and initiate risk reduction planning on top regional priorities
R5.2...R5.n To be defined in Phase I and above and selected in R3.4

6. Conduct evaluation of

S6.1 Establish an empirical baseline NCR security and

R6.1 Establish an empirical baseline NCR security and

E4.3 Assess the applicability of field-tested tools evaluating risk and valuing CIP assets and systems of the NCR

E4.3 Assess the applicability of CIP/DSS (and any others tested) to the multi-system and regional resource allocation decisions of the NCR

E4.4 Evaluate the effectiveness of tested methods in visualizing and communicating risk and risk-reduction value

E4.5 Assess the state of practice in each sector and across the region in adopting risk management methods for allocating resources for risk-reduction

E5.1...E5.nTo be defined bases on specific project plans

E6.1Establish an evaluation design and plan for long term

N4.4 Expand scope and collaboration in S4.4 to serve as test bed evaluating and enhancing asset and system risk management methods for use in NCR and other regions (S&T, IP, ODP)

N4.5 Expand scope and collaboration in R4.4 to serve as test bed for evaluating and enhancing regional risk management methods for use in NCR and other regions (S&T, IP, ODP)

N4.6 Expand scope of S4.5 and R4.5 to improve visualization and communication of CI risk and the value of CI risk reduction in resource allocation decision-making in NCR and other regions (IP, S&T)

N4.7 Develop a template and variations for integrating risk management into resource allocation decisions at the asset, system, multi-system and region for use in the NCR and other regions (IP, ODP)

N5.1...N5.n Field case studies in CIP for application to regions throughout the U.S. (IP and SSAs)

N6.1 Develop a template and variations for defining an

**changes in NCR's
CIP security and
resiliency**

resiliency for the CI sectors –
methods to be defined in Phase
I

S6.2 Measure change from
baseline on regular schedule
over time

resiliency for the region as a
whole – methods to be defined in
Phase I

R6.2 Measure change from
baseline on regular schedule over
time

assessment of progress toward
greater NCR CIP resilience
and security

E6.2 Execute evaluation plan

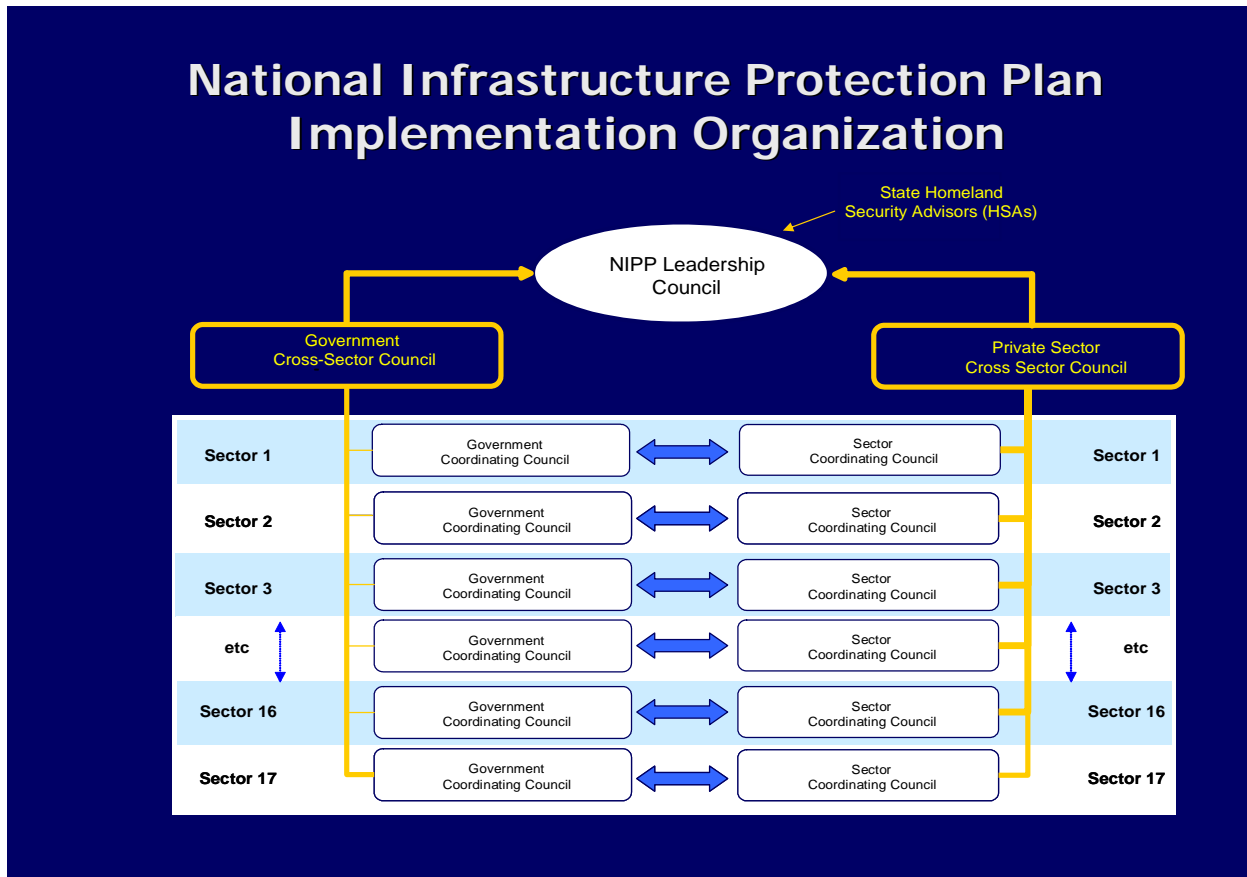
empirical baseline for CIP
evaluation – methods to be
defined in Phase I (IP, S&T,
ODP)

N6.2 Develop template and
variations for empirically
evaluating changes in asset
and regional security and
resilience over time (IP, S&T,
ODP)

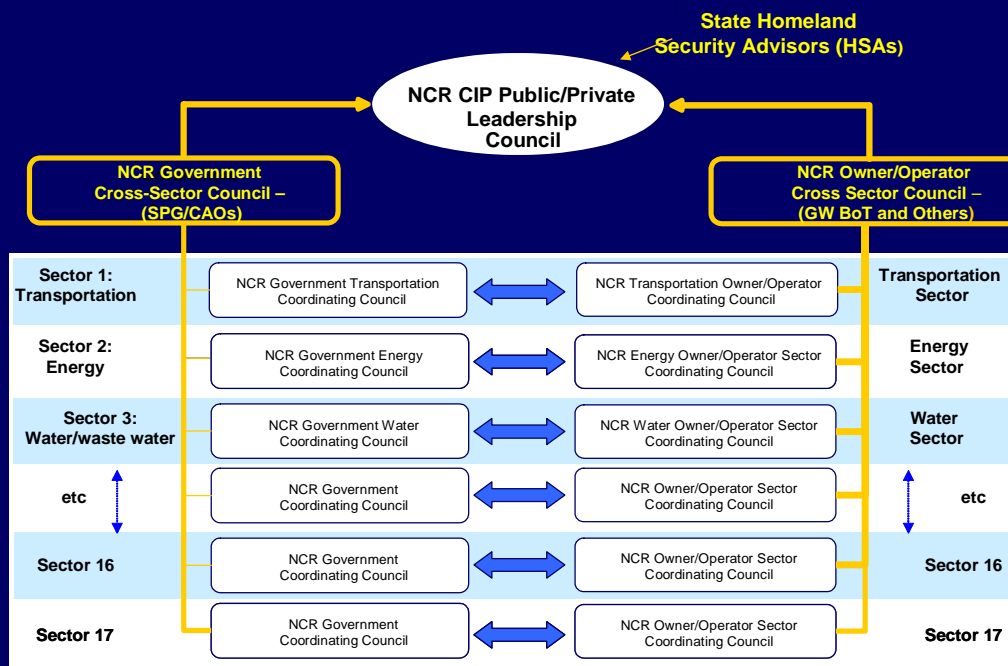
Appendix II – Functional Organization Schemes for Regional and National Integration

Below are sketches that illustrate possible ways in which the NCR regional critical infrastructure protection and/or homeland security programs could be integrated with the National Infrastructure Protection Plan. They are intended to be functional and conceptual only. Many sectors may wish to maintain informal organizations, others may wish to rely on their national organizations, and still others may decide to form standing organizations.

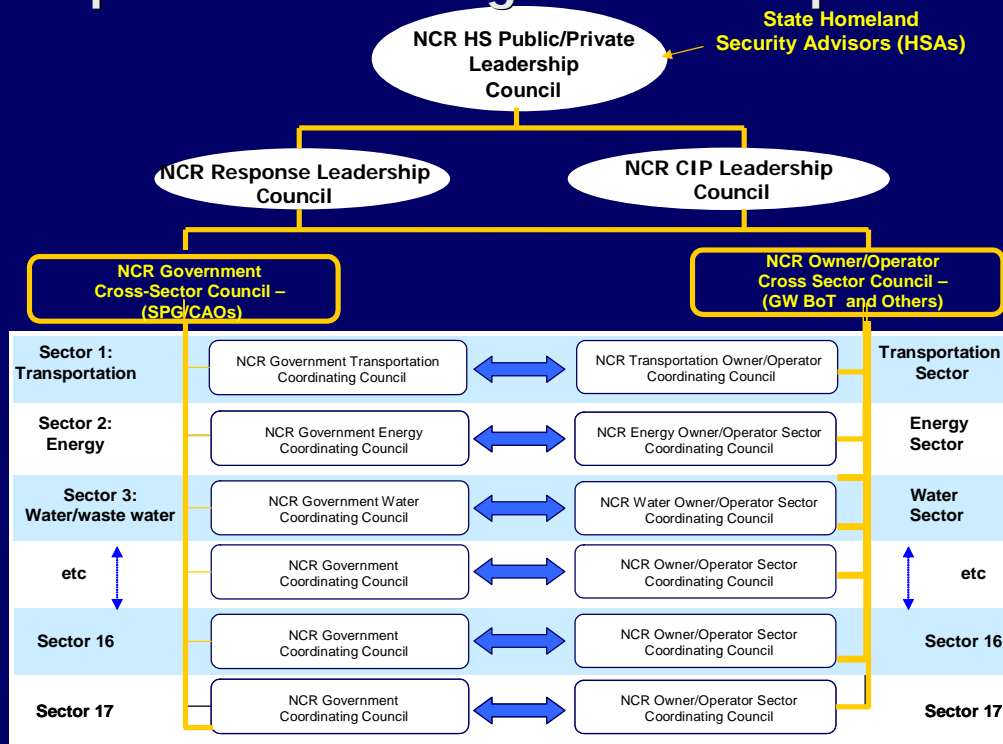
Existing organizations may be willing to assume roles in an NCR-wide public/private/non-profit partnership, such as Emergency Preparedness Task Force of the Greater Washington Board of Trade or other local business groups, the Non-Profit Roundtable, regional government groups such as the Chief Administrators Committee, the Metropolitan Washington Council of Governments, and the state and local governmental units addressed to homeland security such as the state agencies, the regional Emergency Preparedness Council, and the Senior Policy Group.



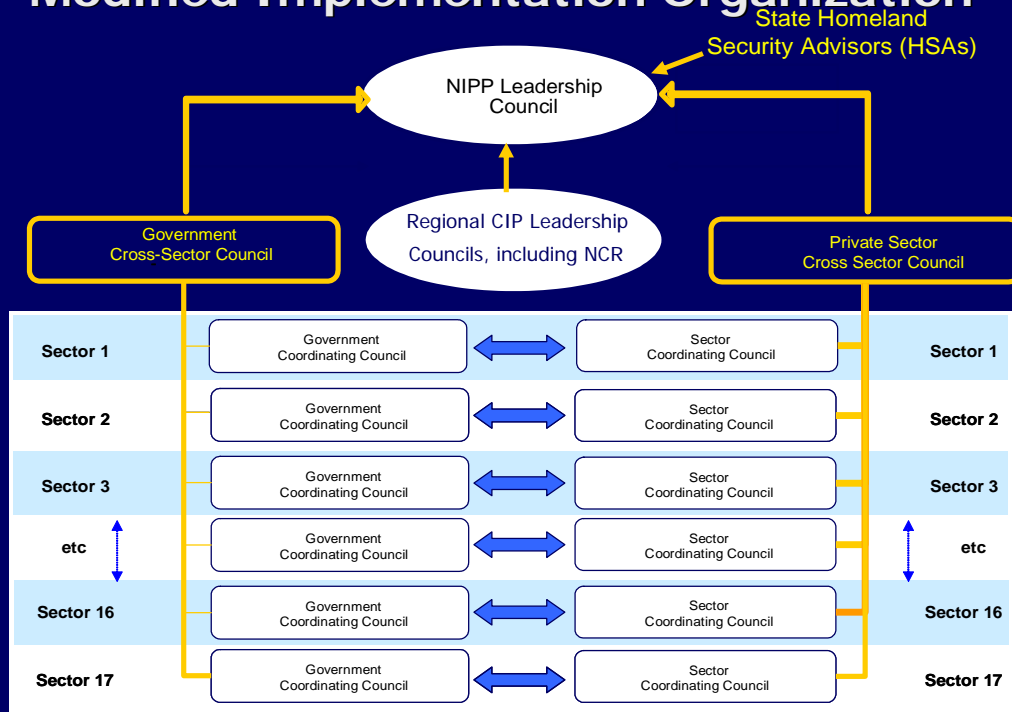
Regional Infrastructure Protection Plan Implementation Organization: Option A



Regional Infrastructure Protection Plan Implementation Organization: Option B



National Infrastructure Protection Plan Modified Implementation Organization



Appendix III – Resource Allocation by Provider (in \$k)

<u>Unit</u>	<u>UASI</u>	<u>Other</u>	<u>Total</u>
GMU, UCIP Manager	1,305	960	2,265
GMU Total:	1,305	960	2,265
Universities			
Virginia Tech	400	390	790
James Madison University	100	150	250
University of Virginia	50	20	70
University of Maryland	650	1,190	1,840
Howard University	25	25	50
Subtotal Universities:	1,225	1,775	3,000
Subcontractors			
PJ Aduskevicz	35	15	50
UTD, Inc.	130	120	250
Zeichner Risk Analytics	150	50	200
The Scalingi Group	125	50,	175
TFZ Associates, LLC	30	30	60
Subtotal GMU Subs:	470	265	735
Grand Totals:	3,000	3,000	6,000

Appendix IV – References

- Bush, G. W. (2002). *National Strategy for Homeland Security*. Washington, DC.: The White House.
- Bush, G. W. (2003). *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: The White House.
- Bush, G. W. (2003). *Critical Infrastructure Identification, Prioritization and Protection (HSPD-7)*. Washington, DC: The White House.
- Bush, G. W. (2003). *National Preparedness (HSPD-8)*. Washington, DC: The White House.
- Government of the District of Columbia. (2005). *REQUEST FOR APPLICATIONS (RFA) #05 HSGP – UASI*. Executive Office of the Mayor, Office of the Deputy Mayor for Public Safety and Justice.
- National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton.
- U.S. Congress. (2002). *Homeland Security Act of 2002, P.L. 107-296*. Washington, D.C.: GPO.
- U.S. Department of Homeland Security. (2005). *Interim National Infrastructure Protection Plan (NIPP)*. Washington, DC: U.S. Department of Homeland Security.
- U.S. General Accounting Office (GAO). (2004). *HOMELAND SECURITY: Management of First Responder Grants in the National Capital Region Reflects the Need for Coordinated Planning and Performance Goals. Report to the Chairman, Committee on Government Reform, House of Representatives* (No. GAO-04-433). Washington, DC: GAO.
- U.S. Government Accountability Office (GAO). (2005). *HOMELAND SECURITY: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security. Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives*. (No. GAO-05-33). Washington, DC: GAO.

Appendix V – Position Descriptions

Appendix VI – Biographical Sketches

George Mason University

John A. McCarthy

Principal Investigator, Critical Infrastructure Protection Program

John A. McCarthy has a unique blend of executive level government, business, and academic experience in the areas of national security relative to the maritime and transportation sectors as well as in-depth knowledge of the governmental interagency process. An experienced program and crisis manager, he has been particularly successful in delivering policy and technical solutions that are time sensitive and national/international in scope. Mr. McCarthy is a recognized thought leader within the information security policy and risk management arenas and is considered an authority on critical infrastructure protection and business continuity management issues by industry and government practitioners alike.

Mr. McCarthy is Director and Principal Investigator of the Critical Infrastructure Protection (CIP) Program at the George Mason University School of Law, where he also holds a faculty appointment as Research Professor of Security Studies. The CIP Project began as a \$6.5M directed appropriation from the Commerce Committee to develop and implement a broad inter- and intra-university research program that supports public and private sector research needs relative to critical infrastructure and homeland security. To date, more than 70 researchers at 15 different universities have been sponsored by the CIP Program including work in direct support of The White House, the Department of Homeland Security, and key industry sectors. Under Mr. McCarthy's leadership, the CIP Project funding has grown to over \$24M in follow-on grants and has been cited by both the Governor of Virginia and federal homeland security leaders as a model academic program supporting the national CIP agenda.

Prior to joining the CIP Program, Mr. McCarthy was a Director in KPMG LLP's Mid-Atlantic Risk and Advisory Services practice in Washington, D.C., where he provided computer security, critical infrastructure, and business continuity management solutions to government clients. Prior to joining KPMG, Mr. McCarthy served as a member of the professional staff of the Critical Infrastructure Assurance Office (CIAO), which supported the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism located within the National Security Council. He assisted in the development of an integrated National Infrastructure Assurance Strategy to address risks and threats to the nation's critical infrastructures. During the Y2K Conversion Period, Mr. McCarthy worked for the Assistant to the President for Y2K, coordinating cyber-security preparedness planning efforts within the public, private, and academic sectors. He played a key role in helping to build and operate the National Y2K Information Coordination Center (ICC) and served first as the ICC's Chief-of-Staff and then as the Deputy Director for Cyber Assurance.

With more than 20 years as a commissioned officer in the United States Coast Guard, Mr. McCarthy served in a wide variety of demanding field command and senior staff positions including command-at-sea and personal Aide to 19th Commandant. During the Gulf War, Mr. McCarthy helped design and supervise United Nation sanction-enforcement operations against Iraq. He has also held numerous positions at all levels of the federal response process including pre-designated Federal On-scene Coordinator (alternate) and Federal On-scene Coordinator's

Representative under the National Contingency Plan. Mr. McCarthy was a senior member of the multi-agency, on-sight command cadre responding to the downing of TWA Flight 800 off the south shore of Long Island, New York.

Mr. McCarthy holds a B.A. degree in Psychology from The Citadel--Military College of South Carolina, Charleston, S.C., and an M.S. in Information Resource Management (specialization in government) from Syracuse University, Syracuse, N.Y. He is also a graduate of the National Defense University--Information Resource Management College, Washington, D.C., and the U.S. Naval War College--Command and Staff College, Newport, R.I. Additionally, he is a distinguished graduate of the Department of Defense Chief Information Officer Certificate program. His military and civilian awards include the Legion of Merit, the Meritorious Service Medal (three awards), the Combat Action Ribbon, and the Vice President's National Partnership for Reinventing Government "Hammer" Award.

Mr. McCarthy is also a Senior Lecturer of the graduate faculty for Syracuse University's School of Information Studies, where he teaches a course on information security and critical infrastructure policy. He is regularly consulted on CIP/homeland security issues by television and print media including *The Washington Post*, CNN, MSNBC, *CIO Magazine*, and *CISO Magazine*.

Jerry Paul Brashear, Ph.D.
Associate Director/Project Manager

Dr. Brashear is currently the Associate Director of the Critical Infrastructure Protection Program for National Capital Projects at George Mason University and the Project Manager of the University Consortium for Critical Infrastructure, which is conducting the National Capital Region Critical Infrastructure Project. At GMU, he carries out the vision that guides the NCR's activities and oversees all efforts and findings of other universities and critical infrastructure experts on the project.

Dr. Brashear was the founder and Director of the Center for Petroleum Asset Risk Management at the University of Texas at Austin. There, he conceived, planned, organized and developed a research, demonstration and training program to advance the understanding of risk, real options, and portfolio management in the planning, evaluation and performance management processes. The program has become globally recognized as an emerging source of new techniques, processes and insights.

He founded The Brashear Group LLC, an independent consulting firm advising on capacity building, strategic and operations planning, policy, resource and economic analysis, and risk. He has been an invited speaker on planning and integrated risk management all over the world and has consulted with energy firms and ministries in the United States, Ecuador, Argentina, Colombia, and Brazil on policy, planning and controlling resource development.

Prior to forming his own firm, he served as Senior Vice President and Director of the Oil and Gas Practice at ICF Kaiser, an international consulting and engineering firm. At ICF, he specialized in energy and natural resource policy, energy taxation, R&D program planning, risk management and technology policy.

Dr. Brashear has numerous publications and has served on Professional and Civic Boards. He has Ph.D. in the Interdisciplinary Program in Urban, Technological and Environmental Planning from The University of Michigan. He also received his MBA from

Harvard Business School and graduated *magna cum laude* and *Phi Beta Kappa* from Princeton University.

Jordana Siegel

Jordana Siegel is currently the Senior Project Associate at the Critical Infrastructure Protection Program at George Mason University. Ms. Siegel serves as the Deputy Project Manager for the National Capital Region Critical Infrastructure Project. In this capacity, she supports all project activities, including strategic development, deliverable production, budget maintenance and other project management initiatives.

Ms. Siegel has worked in the field of critical infrastructure protection (CIP) since 2002. She has provided strategic consulting services to both private sector and public sector clients in the CIP arena and contributed to the production of a weekly newsletter focused on issues in homeland security. Prior to her work in CIP, she was a consultant in the telecommunications industry, focused on legislative compliance issues, serving federal government, state government, and private sector clients.

Ms. Siegel holds an MA in International Affairs, with concentrations in International Business and Latin American Studies, from the George Washington University. She also received her BA in Psychology from the University of California, San Diego.

Christine Pommerening, Ph.D.

Dr. Pommerening is a post-doctoral fellow at George Mason University's Critical Infrastructure Protection Program. She received her Ph.D. in Public Policy from George Mason University, and holds an M.A. in Sociology from Ruhr-Universität Bochum in Germany. Her research focuses on the development of regional and international governance structures for new technologies, and organizational and institutional theory. She has worked in research projects evaluating and implementing EU structural fund programs, public and private sector coordination, and regional economic development.

James T. Creel

James Creel is a research associate for the Critical Infrastructure Protection Program at George Mason University's School of Law and is part of the Project Coordination Team. A graduate of Virginia Tech, James has studied abroad in Europe and speaks both Turkish and Spanish. He is currently pursuing a Master's Degree in Political Science.

Farrokh Alemi, Ph.D.

Dr. Farrokh Alemi, Associate Professor, received his Ph.D. in Industrial Engineering with a focus in Decision Analysis from the University of Wisconsin-Madison. He has extensive experience designing and applying case-mix adjustment methodologies and is a recognized leader among faculty in the application of distance learning. In addition to academic teaching, he conducts research on behalf of federal and state agencies. Examples of current research include cost-benefit and cost-effectiveness analyses of substance abuse treatment within the criminal justice system for the National Institutes of Health, National Institute on Drug Abuse, and an analysis of financing policies for telemedicine substance abuse treatment for Substance Abuse Services Administration, Center for Substance Abuse Treatment. Dr. Alemi's early research included comparative analysis of severity indices in evaluating care of patients with myocardial infarction for the Health Care Finance Administration. More recently, he developed measures of severity of AIDS and automated methods of collecting patient's health status information.

Dr. Alemi has held the role of PI for the Robert Wood Johnson Foundation as well as the National Institute of Standards and Technology. He has had over 50 peer-reviewed publications. He is currently conducting extensive research for the Critical Infrastructure Protection Program's Health Sector.

Philip E. Auerswald, Ph.D.

Dr. Philip Auerswald is an Assistant Professor and Director of the Center for Science and Technology Policy at the School of Public Policy, George Mason University. His research pertains to the economics of technological change, science and technology policy, and industrial organization. He is co-author with Lewis Branscomb of *Taking Technical Risk: How Innovators, Executives and Investors Manage High-Tech Risks*, MIT Press, 2001. He is currently a member of the research team for a multi-year National Academies study of the Small Business Innovation Research (SBIR) program. He has been a consultant to the Department of Economic Development of the Commonwealth of Massachusetts and is principal author of "Competitive imperatives for the Commonwealth: A conceptual framework to guide the design of state economic strategy." He is also co-editor with David Auerswald of *The Kosovo Conflict: A Diplomatic History Through Documents*, 2001 (foreword by Sen. Joseph Biden Jr.), and was from 1995-2003 Editor of the *Foreign Policy Bulletin: The Documentary Record of United States Foreign Policy*. He holds a Ph.D. in economics from the University of Washington and a B.A. (political science) from Yale University.

Brien Benson, Ph.D.

Dr. Brien Benson is Research Associate Professor at the School of Public Policy, where his research focus is intelligent transportation systems. He is Manager of the National Center for ITS Implementation Research. He has published in such journals as *Transportation Research Record*, *ITS Quarterly*, and *IEEE Transactions on Engineering Management*. His research areas are public opinion in the transportation field, ITS institutional issues, and the policy process, and

he teaches program evaluation and the policy process. Dr. Benson is past President of ITS Virginia and was Chairman of the ITS America Communications and Outreach Committee for several years. Dr. Benson has served as Associate Administrator at the Federal Transit Administration. He received his Ph.D. in Public Policy from George Mason University.

Ami C. Carpenter

Ami C. Carpenter is a Research Fellow at the Institute for Conflict Analysis and resolution at George Mason University. She specializes in research and development of multi-stakeholder collaboration and conflict management in complex partnerships, and is an Associate Editor for Transnational Dispute Resolution Online Journal. Ms. Carpenter is a Ph.D. Candidate, writing a dissertation on the use of conflict preventive policies and practices in international development.

Sandra Cheldelin, Ph.D.

Sandra I. Cheldelin is the Vernon M. and Minnie I. Lynch Professor of Conflict Resolution and former Director of the Institute for Conflict Analysis and Resolution (ICAR). She earned her undergraduate degree in sociology at Oregon State University and masters and doctoral degrees in psychological foundations of education at the University of Florida. She has served on the faculty and as Provost at the McGregor School of Antioch University, Yellow Springs, Ohio; and on the faculty and as Academic Dean at the California School of Professional Psychology in Berkeley. Throughout her career in the academy Cheldelin has been an active practitioner. A licensed psychologist and expert in organizational conflict, she has applied her skills to support collaborative leadership, mediation, conflict resolution, and institution building to more than one hundred fifty organizations—colleges and universities, medical schools, associations, treatment facilities, religious and community organizations and corporations. She has served as keynote speaker and invited lecturer on workplace issues, including violence, change, and conflict resolution. She is coauthor of *Conflict Resolution*, (Jossey Bass, 2004) and co-editor of *Conflict: from Analysis to Intervention* (Continuum, 2003). She serves on a variety of conflict resolution related boards.

E. Kathlyn Emmons, Ph.D.

Dr. Emmons is presently the Senior Research Associate for the Critical Infrastructure Protection Program (CIPP) at George Mason University. At GMU, she initiates and supervises research projects and assesses findings of other universities and critical infrastructure experts on the various research projects conducted by the CIP Program office.

Prior to joining George Mason University, Dr. Emmons was a Professor of Information Management at the National Defense University. In that position, she developed and taught courses in national policies for Critical Infrastructure Protection and Cyber Security and federal compliance and response. She also taught Cyber Ethics, Enterprise Integration, and Information Security Program planning and policy development. Her major fields of research focused on strategic planning, leadership and organizational responses in public organizations. She also served as Chair of the Information Strategies Department where she was responsible for a faculty of 12 Ph.D.s and other senior federal information systems professionals.

Retiring from the federal government with over 24 years of service, other federal positions included project supervisor for deploying the Department of Defense's secure information systems (SIPRNet) for law enforcement organizations and program analyst for the Department of Energy's alternative energy, conservation and solar programs. Dr. Emmons has also worked in Germany with the U.S. Army, and she currently holds an active Top Secret/SSBI security clearance.

Dr. Emmons's educational portfolio includes a Ph.D. in Public Policy from George Mason University, an MA in Urban Studies from Trinity University, a Masters of Business Administration from Boston University, and a BA in History.

Jonathan L. Gifford, Ph.D.

Dr. Jonathan L. Gifford is a professor in the School of Public Policy at George Mason University. His primary field of expertise is transportation and public policy. He has written widely on this subject. His recent book, *Flexible Urban Transportation* (Pergamon, 2003) examines how U.S. urban transportation policy could be more flexible and capable of adapting to rapid changes in the economy and society. It argues that current planning approaches have developed such that project lead times sometimes extend to decades and funding programs tend to lock decision makers into courses of action that may not be advisable in the face of new developments and information.

Another element of his work examines the role of standards in the development and adoption of technology. He has looked particularly at methods of organizing technological cooperation across jurisdictional boundaries through loose coalitions and consortia. A case in point is the E-ZPass highway toll tag, adopted now by more than 3.5 million households in the northeastern U.S. Mandatory standards setting processes, which are more common in Europe and Asia, have met with less successful adoption and serious implementation problems.

He directs and teaches in the School of Public Policy's Master's in Transportation Policy, Operations and Logistics program, which he helped develop and launch in fall 2000. This unique program accepts students from a wide variety of educational disciplines and professional backgrounds, and provides them with a solid knowledge of the theory, policy, law, research and practices required for effectively and efficiently supplying and managing modern transportation facilities and services.

He also teaches a course on the Interstate highway system as a socio-technical system. This course is a section Technology in Contemporary Society (HNRS 253), which is the capstone course in the university's Honors in General Education. The course examines the history and development of the Interstate highway system, and the role it has played in the

development of modern America. The class explores the social and technical context of the Interstate program, its impacts on cities and suburbs, on industry, on the environment, and on society at large.

His other primary teaching focus is managing information resources, a course he teaches in the university's Master of Public Administration program.

He is active professionally in the Transportation Research Board (chairman of the committee on transportation and land development, and member of committees on transportation history, transportation asset management and strategic management) and the Intelligent Transportation Society of America.

He received his B.S. in Civil Engineering from Carnegie Mellon University. At the University of California, Berkeley, he earned his M.S. and Ph.D. (1983) in Civil Engineering (Transportation), with doctoral minors in economics, and urban and regional planning. His dissertation examined the history and development of the Interstate highway system from its origins in the 1930s through its design and deployment in the 1960s and beyond.

Sean P. Gorman, Ph.D.

Dr. Gorman received his Ph.D. from George Mason University's School of Public Policy working as the Provost's High Potential research candidate. He is also employed as adjunct faculty at American University's Kogod School of Business. Mr. Gorman has also served as VP of R&D for a telecommunications mapping firm and was Director of Strategy for a Washington DC based technology incubator. His research is focused on cybersecurity and he works with the GMU's Critical Infrastructure Protection Project. His cybersecurity research has been featured in the Washington Post, Wired, Der Spiegel, Associated Press, CNN, MSNBC, Fox, CNBC, and NPR. He has published in Telecommunications Policy, Environment and Planning A & B, Tijdschrift voor Economische Geografie, Journal of Crisis and Contingency Management and the forthcoming book Networks, Complexity, and Security. Mr. Gorman has also worked extensively with the New York University Taub Urban Research Center on e-business growth, wireless infrastructure, catastrophe preparedness and international telecommunications projects.

Gerald A. Hanweck, Ph.D.

Dr. Gerald A. Hanweck is Professor of Finance in the School of Management at George Mason University in Fairfax, Virginia and is presently Visiting Scholar in the Division of Insurance and Research of the Federal Deposit Insurance Corporation. He joined the faculty at George Mason in 1986, and teaches courses in corporate finance, applied global macroeconomics, financial institutions, and financial markets at the undergraduate and MBA levels. At the FDIC he is concentrating on the use of market information in bank risk management strategies, for use in establishing federal deposit insurance pricing, and the better identification of banks in financial distress. In this latter regard, scenario analyses are being developed relating macroeconomic factors to banking performance measures to better predict the effects of regional and macroeconomic cycles on banking company risk taking and vulnerability.

He has served as consultant to government agencies, banks and business and as an expert witness in litigation involving financial institutions and government agencies.

Dr. Hanweck received a B.A. in Economics from Stanford University and a Ph.D. in Economics from Washington University in St. Louis. Before joining George Mason University, he was an economist in the Division of Research and Statistics at the Board of Governors of the Federal Reserve System, Washington, D.C.

Dr. Hanweck's research interests include financial institutions and markets performance, public policy regarding these institutions and the structure of their markets, economic stabilization and monetary policy as they influence financial institutions and markets performance, and economies of scale and scope and mergers in the financial service industries. He has published research on these topics in academic and professional journals including *Journal of Banking and Finance*, *Journal of Monetary Economics*, *Journal of Money, Credit, and Banking*, *Journal of Economics and Business*, *The Antitrust Bulletin*, and *Bankers Magazine*. In addition to this research, Dr. Hanweck co-authored two books with Bernard Shull, *Interest Rate Volatility: Understanding, Analyzing, and Managing Interest Rate Risk and Risk-Based Capital*, published by Irwin Professional Publishing, January 1996 and *Bank Mergers in a Deregulated Environment: Promise and Peril*, Quorum Books, 2001.

Mark Houck, Ph.D.

Mark Houck received the Bachelor of Engineering Science degree in 1972, and the Ph.D. in Environmental Engineering in 1976 from the Johns Hopkins University. He has held faculty appointments in Civil Engineering at the University of Washington at Seattle (1976-78), and Purdue University (1978-91); and visiting faculty appointments at the Johns Hopkins University (1989-90), and Heriot-Watt University in Scotland (2003). At George Mason University (1992–present), Dr. Houck is Professor of Civil, Environmental and Infrastructure Engineering (CEIE). He is also an affiliate faculty in the Department of Systems Engineering and Operations Research, and Department of Environmental Science and Policy. He has served in various administrative positions at Mason, most recently as the CEIE Department Chair until August 2002. In the private sector, Dr. Houck has held the positions of Vice President of Water Resources Management, Inc., and President of Omtex Engineering, Inc. He was awarded the Huber Research Prize by the American Society of Civil Engineers, and he is a Registered Professional Engineer. He is co-editor of the international journal *Civil Engineering and Environmental Systems*.

Dr. Houck's research and teaching interests include water resource systems management, planning, and engineering; environmental systems analysis and engineering; and operations research. His most recent work has been in the area of water and wastewater infrastructure security. Two current projects include evaluation of vulnerability assessments in the water and wastewater infrastructure sector, and development of novel strategies for identifying optimal counter-measures to attacks on water infrastructure. He is teaching a new course in Spring 2005 on Water and Wastewater System Security.

Sushil Jajodia, Ph.D.

Dr. Jajodia is BDM International Professor of Information Technology and the director of Center for Secure Information Systems at George Mason University. He served as the chair of the Department of Information and Software Engineering from 1998-2002. He joined GMU after serving as the director of the Database and Expert Systems Program within the Division of Information, Robotics, and Intelligent Systems at the National Science Foundation. Prior to that he was the head of the Database and Distributed Systems Section in the Computer Science and Systems Branch at the Naval Research Laboratory, Washington and Associate Professor of Computer Science and Director of Graduate Studies at the University of Missouri, Columbia. He has also been a visiting professor at the University of Milan and University of Rome "La Sapienza", Italy and at the Isaac Newton Institute for Mathematical Sciences, Cambridge University, England.

Dr. Jajodia received his Ph.D. from the University of Oregon. His research interests include information security, temporal databases, and replicated databases. He has authored five books, edited twenty two books, and published more than 250 technical papers in the refereed journals and conference proceedings. He received the 1996 Kristian Beckman award from IFIP TC 11 for his contributions to the discipline of Information Security, and the 2000 Outstanding Research Faculty Award from GMU's School of Information Technology and Engineering. Dr. Jajodia has served in different capacities for various journals and conferences. He is the founding editor-in-chief of the Journal of Computer Security and on the editorial boards of ACM Transactions on Information and Systems Security, International Journal of Cooperative Information Systems, and International Journal of Information and Computer Security. He is the consulting editor of the Kluwer International Series on Advances in Information Security. He also serves as the chair of the ACM Special Interest Group on Security, Audit, and Control (SIGSAC) and the IFIP WG 11.5 on Systems Integrity and Control. He has been named a Golden Core member for his service to the IEEE Computer Society, and received International Federation for Information Processing (IFIP) Silver Core Award "in recognition of outstanding services to IFIP" in 2001. He is a past chairman of the IEEE Computer Society Technical Committee on Data Engineering. He is a senior member of the IEEE and a member of IEEE Computer Society and Association for Computing Machinery.

Todd M. La Porte, Ph.D.

Dr. Todd M. La Porte is an associate professor at the School of Public Policy at George Mason University. His long-term research interests are in governance and the use and impacts of information technologies in the public sector. He is also engaged in research network systems, critical infrastructure protection, and organizational response to extreme events such as natural and technological disasters and terrorism.

He is a founding member of the Cyberspace Policy Research Group, which was established under a National Science Foundation grant in 1997, and which has received additional support from the Pew Foundation. In addition, he has published work in public organizational challenges of the Web in disaster assistance, on European technology assessment

methodologies and practices, and on the social implications of telecommunications mobility. La Porte teaches courses on critical infrastructures and extreme events, global Internet public policy, introductory international political economy, technology and institutional change.

Previously, La Porte was a tenured member of the Faculty of Technology, Policy and Management at the Delft University of Technology in the Netherlands. Prior to this post, he served for six years as an analyst in the information technology and the international security programs at the Office of Technology Assessment, a research office of the U.S. Congress. His work at OTA focused on the role of wireless telecommunications and the National Information Infrastructure, international trade in telecommunications services and U.S. policy, and international defense industrial cooperation and the arms trade. He received his PhD in political science from Yale University in 1989, and his BA in sociology and political science from Swarthmore College in 1980.

Andrew Loerch, Ph.D.

Dr. Andrew Loerch is an Associate Professor in the Department of Systems Engineering and Operations Research at George Mason University. He holds a Master of Science in Operations Research from the Naval Postgraduate School, and a PhD in Operations Research from Cornell University. He is also a retired Army Colonel with 26 years of active federal service of which 15 years was spent as a military operations research analyst. He served as chief analysts and division chief of the Joint Warfighting Studies and Analysis Division of the Office of the Deputy Chief of Staff for Operations and Plans, and represented the Army in numerous joint studies including the Deep Attack Weapons Mix Study. His military career culminated as Chief, Force Strategy Division, Center for Army Analysis. He is currently the President of the Military Operations Research Society. He is an associate editor of the Operations Research journal and Military Operations Research. Dr. Loerch directs the track in Military Application of Operations research in the masters program in Operations Research at George Mason University. He presently receives funding through the Critical Infrastructure Protection Program for the Department of Homeland Security, and the Office of Naval Research.

Arnauld Nicogossian, M.D., FACPM, FACP

Arnauld Nicogossian serves as Distinguished Research Professor and Director, Office of International Medical Policy at the School of Public Policy, George Mason University. He has been asked by the National Aeronautics and Space Administration (NASA) to return on a part time basis as a Senior Advisor for Medical and Health Policy to the NASA Office of Chief Health and Medical Systems

Dr. Nicogossian retired from National Aeronautics and Space Administration in January 3, 2003, after a distinguished career spanning over three decades. He was the Associate Administrator for Life and Microgravity Sciences Office, Chief Medical Officer and Senior

Advisor for Health Affairs. Dr. Nicogossian managed and funded an extensive portfolio of research and development grants in the areas of space biology, medicine, physics and chemistry. He was also responsible for the oversight of the NASA workforce and astronauts health programs.

Dr. Nicogossian received his Baccalaureate in Biology from the College Franco – Iranian; the Medical Doctor degree, from the Tehran University (1964) in Iran. He completed an Internal Medicine Residency and Fellowship in Pulmonary Diseases, at Elmhurst Hospital, Mount Sinai Medical Services (1970), in New York City, where he was Chief Resident in Internal Medicine. Dr Nicogossian received a Master of Science degree in Preventive and Aerospace Medicine Ohio State University, Columbus Ohio (1972). Dr Nicogossian is a Diplomate of American Board of Preventive Medicine (Aerospace).

He has practiced internal medicine in New York and Fairfax, VA. He has published extensively, including two definitive textbooks in Space Physiology and Medicine. Dr. Nicogossian has been recognized nationally and internationally for his contributions to space medicine, international collaboration and contributions to improve life on Earth, telemedicine for disaster relief and in support of expeditions into extreme environments. He served as President of three professional societies, and holds a faculty appointment at the Uniformed Services University of Health Sciences, Bethesda, Maryland.

His expertise is in aerospace medicine; human factors in closed and hostile environments, health risks management, science and technology research and development, international public health and policy, and technology transfer to improve health care.

Dr. Nicogossian is currently conducting research and teaching graduate courses in the area of biodefense, biosafety and international public health policy.

Dr. Nicogossian is the recipient of several grants; four are related to CIP/NCR/CVA:

1. *Protecting the Nation's Blood Supply: A Critical Infrastructure*
2. *Epidemiology of Transportation and Bioterrorism*
3. *Critical Role of Citizen in Biodefense and Early Warning*
4. *Co Investigator of Thomas Zimmerman for the NCR Health Sector Vulnerability Assessment*

Laurie Schintler, Ph.D.

Dr. Laurie Schintler is Assistant Professor at the School of Public Policy at George Mason University, where she teaches graduate courses on transportation theory and models, regional development theory, and statistics and econometrics. Dr. Schintler has written numerous articles and papers in her field, including "A Prototype Dynamic Transportation Network Model" and "Evaluation of the Smart Flexible Integrated Real-time Enhancement System (SaFIRES)". Dr. Schintler is Book Review Editor for the *Annals of Regional Science*, and, among other service activities, is helping the Metropolitan Washington Council of Governments design and set up a web site for complaints regarding signalized intersections in the Washington region. Dr. Schintler received her Ph.D. in Regional Planning from the University of Illinois at Urbana-Champaign.

Anoop Singhal, Ph.D.

Dr. Anoop Singhal is a Research Associate Professor at the Center for Secure Information Systems at George Mason University in Fairfax, Virginia. His research interests are in the area of Network Security and Intrusion Detection using Data Warehousing and Data Mining. These techniques are useful in detecting new kinds of attacks.

He is researching a Flexible Data Model for the National Capital Region Critical Infrastructure Protection Project. This data model is used to store and analyze information about Vulnerability Assessment and Risk Management Tools and Procedures that include Telecom, Cyber Networks, Energy, Transportation and Banking/Finance sectors.

Dr. Singhal received his Ph.D in Computer Science from Ohio State University. He has several years of research and development experience at AT&T Labs and Bell Labs. As a Distinguished Member of Technical Staff he has led several projects in the area of VLSI/CAD, Databases and Network Management Applications at AT&T and Lucent. He is a senior member of IEEE and he has published more than 20 papers in leading conferences and journals.

Roger Stough, Ph.D.

Dr. Roger Stough is Associate Dean for Research and External Relations at the School of Public Policy, and is Director of the National Center for ITS Implementation Research. He is Professor of Public Policy at the School of Public Policy, where he holds the NOVA Endowed Chair and is an Eminent Scholar.

Dr. Stough has recently published two books on transportation, *Intelligent Transport Systems* and *Transport Policy*. He has authored more than one hundred scholarly articles, including many on intelligent transport systems, such as "Evaluating ITS Infrastructure in a Metropolitan Area" and "Impact of Network Configuration on the Efficacy of ITS".

Dr. Stough also writes extensively on regional development issues. He edits the *Annals of Regional Science* and has recently published two books in this field, *Regional Economic Development* and *Theories of Endogenous Regional Growth*. Dr. Stough's research interests in ITS include evaluation, telecommuting, and traveler information systems. He received his Ph.D. in Geography and Environmental Engineering from Johns Hopkins.

Mohan M. Venigalla, Ph.D.

Dr. Venigalla is a Transportation Systems Engineer with over 19 years of research, teaching and consulting experience. He worked at internationally recognized consulting, research and academic organizations. He is proficient in quantitative methods for transportation planning, traffic operations and traffic simulation. His work experience includes design and analysis of transportation systems encompassing travel demand modeling; transportation related air quality analysis; traffic simulation; network analysis, and intelligent transportation systems modeling.

Dr. Venigalla is also experienced in the application of several optimization techniques for transportation problems. He developed and applied a number of computer models for

transportation planning and traffic engineering problems. His background also includes urban and rural corridor studies, including preparing feasibility studies for major investments studies in the US and abroad.

He first started his career as an educator at an undergraduate engineering program where he taught civil engineering courses. After several years of research and consulting service, he returned to academia as an Assistant Professor at George Mason University in Fall 2000. Currently he is pursuing research in transportation air quality and information technology applications to transportation related problems. He has over 30 publications to his credit, which include technical reports, journal articles, and conference presentations.

James Madison University

George H. Baker, Ph.D.

Dr. Baker is Associate Professor of Integrated Science and Technology at James Madison University. He also serves as Associate Director of the University's Institute for Infrastructure and Information Assurance (IIIA). He is a consultant in the areas of critical infrastructure assurance, high power electromagnetics, nuclear and directed energy weapon effects, and risk assessment. He recently served as a member of the Congressional EMP Commission staff. Baker is former director (1996-1999) of the Defense Threat Reduction Agency's Springfield Research Facility, a national center for critical system vulnerability assessment. Much of his career was spent at the Defense Nuclear Agency (DNA) as the Integrated Electromagnetics Team Leader managing system protection, underground testing and standards development programs. From 1994 to 1996 he was chief of the Agency's Innovative Concepts Division overseeing the joint US-Russian space nuclear power technology, electro-thermal chemical (ETC) gun development, radiofrequency directed energy concept development and testing, and DNA's university grant programs. In 1998 Baker received the Agency Legacy Award for his leadership and innovation. He is a member of the NDIA Homeland Security Executive Board, the Institute of Electrical and Electronic Engineers, the Directed Energy Professional Society (Charter Member), the Association of Old Crows. He is a Summa Foundation Fellow and holds a Ph.D. from the U.S. Air Force Institute of Technology.

Howard University

Kathleen Kaplan, Ph.D.

Dr. Kathleen M. Kaplan has been an Assistant Professor at Howard University for four years with over twenty-five publications and one patent. Her interests in Critical Infrastructure Protection include the modeling and simulation of critical infrastructure interdependencies and SCADA systems.

Her research interests include intellectual property, biotechnology, data communications, and quantum computing. She has numerous publications and one patent pending for her Method for Sorting Permutations with Reversals.

Dr. Kaplan received her B.S. from University of Massachusetts Lowell, her M.S. from Florida Institute of Technology and her Doctorate of Science from The George Washington University.

University of Maryland

Gregory B. Baecher Ph.D.

Dr. Baecher is a professor at the Department of Civil and Environmental Engineering at the University of Maryland. He earned his Ph.D. in civil engineering from Massachusetts Institute of Technology. Dr. Baecher served in the U.S. Army Corps of Engineers. He has won numerous awards and has many publications. He currently serves on the Water Science and Technology Board at the National Research Council and was the Panel Chairman of *Analytical Methods for Water Resources Project Evaluation* from 2001-2004.

Philip J. Tarnoff

Mr. Tarnoff is an M.S. in electrical engineering. He is presently the Director at the Center for Advanced Transportation Technology at the University of Maryland. In this role, Mr. Tarnoff has been assigned the responsibility of creating a new organization that will be responsible for ensuring that the response of transportation agencies to major incidents is fully coordinated, and that all needed communication occurs. This requires close coordination with all members of the transportation agencies within the National Capital Region and has received the unanimous approval of the Transportation Planning Board of the Metropolitan Washington Council of Governments. He has been recognized for his contributions to transportation and has numerous publications.

University of Virginia

Gregory B. Saathoff, M.D.

Gregory B. Saathoff, M.D. is an Associate Professor of Research at the University of Virginia's School of Medicine and Executive Director of the University of Virginia's Critical Incident Analysis Group. In this capacity, he has organized annual conferences relating to

critical incidents and the Constitution, the terrorist threat abroad, protecting symbols of democracy, the threat of bioterrorism, suicide bombing and terrorist hostage taking. This has also included coordination of response to governmental and non-governmental critical incidents.

In 1996, Dr. Saathoff was appointed to a U.S. Department of Justice Special Commission charged with developing a process to assist the FBI's Critical Incident Response Group in identification and development of resources to assist the Bureau during critical incidents. Later that year, Dr. Saathoff was appointed to the role of Conflict Resolution Specialist; the position proposed and created as a result of the commission's work. He continues to serve as the Conflict Resolution Specialist to the FBI's Critical Incident Response Group, specializing in the identification, analysis and management of pathologic groups. In this classified role, he consults with the Crisis Negotiation Unit and the National Center for the Analysis of Violent Crime. He has assisted in the coordination of the Bureau's conferences on "The School Shooter", "Workplace Violence" and "Domestic Violence." Over the past twelve years, he has consulted to three prisons in the Virginia Department of Corrections, treating male and female violent criminal offenders who suffer from mental illness,

During the Gulf War, Dr. Saathoff was called to active duty and deployed overseas as an Army Reserve Psychiatrist, and was awarded the Army Commendation Medal. He retired after 8 years with the rank of Major. A member of the University of Virginia's Kuwait Project, he studied societal trauma in Kuwait subsequent to the Iraqi occupation. Subsequent to this work, Dr. Saathoff has served on the faculty of the Saudi-U.S. Universities Project located at the King Faisal Specialist Hospital in Riyadh, Saudi Arabia and also served as a reviewer for the Annals of Saudi Medicine. In addition to the Middle East, his work has taken him to projects in the former Soviet Union, Western Europe and Australia.

He serves as the Chair of the Committee on International Relations for the Group for the Advancement of Psychiatry. Dr. Saathoff has written The Negotiator's Guide to Psychotropic Drugs, and was a one of the co-authors of the FBI's threat assessment monograph: The School Shooter. He has also published in the area of personality disorders, police psychiatry, post-traumatic stress disorders, war trauma in Kuwait, biologic psychiatry and public response to weapons of mass destruction. On behalf of the Critical Incident Response Group, he was presented with a 2003 House Joint Resolution from the Virginia General Assembly, commending his group for its work in the area of terrorism. He serves as a Senior Fellow for the Homeland Security Policy Institute at George Washington University, where he is also a member of its adjunct faculty, as well as the Behavioral Science Research Advisory Board in the Federal Bureau of Investigation.

Dr. Saathoff received his B.A. in Psychology at the University of Notre Dame, his M.D. at the University of Missouri and his residency training in psychiatry at the University of Virginia. He is a Diplomate of the American Board of Psychiatry and Neurology.

Virginia Tech

Frederick Krimgold, Ph.D.

Dr. Frederick Krimgold is an architect specializing in disaster risk management including hazard and vulnerability assessment, mitigation design and implementation and mechanisms for financing of mitigation investment. He has worked in disaster management in developing countries over the past 30 years. He has been a researcher and research manager for the National Earthquake Hazard Reduction Program at the National Science Foundation and has served as a member of the Federal Emergency Management Agency Advisory Board. Dr. Krimgold has worked with the founding of the National Urban Search and Rescue System in the United States and the creation of the Disaster Management Facility at the World Bank.

Currently, Dr. Krimgold is the director of the Virginia Tech Center for Disaster Risk Management, a multi-disciplinary university research and implementation center for disaster risk management. The Center is affiliated with the World Institute for Disaster Risk Management that is a joint initiative of Virginia Tech and the Swiss Federal Institutes of Technology. The Center is currently completing a major research and publishing program on the topic of Integrated, Incremental Seismic Rehabilitation for the reduction of earthquake risk in existing buildings. Prior to this position, Dr. Krimgold served as the Project Director of the Federal Emergency Management Agency, Incremental Seismic Rehabilitation Series from 2000 to 2003. Dr. Krimgold has directed a major research and publishing program to introduce earthquake risk management to owners and managers of existing vulnerable buildings. Research has been carried out on the organizational, financial and functional characteristics of critical high risk occupancies including schools, hospitals, office and retail buildings and multi-family housing to develop strategies for the integration of physical risk reduction measures at minimum cost and functional disruption. This work opens new prospect for the management and reduction of risk in existing buildings

Dr. Krimgold's extensive career, which includes numerous publications, such as the *Independent Evaluation of USAID Gujarat Humanitarian Response and Rehabilitation Program, 2003*, includes a variety of additional experiences relevant and contributing to his expertise. Dr. Krimgold's educational portfolio includes a BA in Architecture from Yale University and a D.Tech, in Architecture and Planning from the Royal Institute of Technology, Stockholm. He speaks English, French, Swedish, and has worked in India, Turkey, Mexico, Russia, Armenia, the Philippines, and Ethiopia.

John Bigger

Mr. John Bigger is an M.S. in electrical engineering and has over 30 years project and program management experience in the electric utility and energy fields. Mr. Bigger has 10 years of engineering experience, at increasing levels of responsibility, at the Los Angeles Department of Water and Power, 21 years managing energy technology research, development, demonstration, and integration projects at the Electric Power Research Institute, Palo Alto, California. Mr. Bigger was part of a small group that created and then served as Technical Director of the Utility Photovoltaic Group, a not-for-profit organization to support the

commercial use of photovoltaic systems by electric utilities in the U.S. Since 1998, Mr. Bigger has served as president of the small consulting firm, Sol y Mer, Ltd; the firm develops projects and programs for utilities and other organizations in the renewable energy field. Beginning in 2000, Mr. Bigger has conducted research studies of energy infrastructures, their security, and their organization at the Alexandria Research Institute. These projects have been funded by the Commonwealth of Virginia and various agencies of the federal government.

Kathleen Hancock, Ph.D.

Dr. Kathleen Hancock is the Associate Director for the Center for Geospatial Information Technology and an Associate Professor in Civil and Environmental Engineering at Virginia Tech. Her research interests include the application of spatial analysis and geographic information systems and intelligent mapping for engineering problem solving; freight planning in transportation; highway safety including crash data analysis, cost/benefit analysis for highway safety, roadside safety feature design and development, static dynamic, full-scale and computer simulation testing of roadside safety features.

Her past work experience includes serving as associate professor and transportation program coordinator at the University of Massachusetts since 2001, and associate director of the University of Massachusetts Transportation Center and director of MassSAFE since 2002. She was an assistant professor at the University of Massachusetts from 1995 to 2001. Dr. Hancock has also worked in various engineering capacities for Momentum Engineering, The Scientex Corporation, and the Southwest Research Institute.

Dr. Hancock earned her Ph.D. and master's in civil engineering from Vanderbilt University in 1994 and 1991, respectively. She received her bachelor's degree in civil engineering from Colorado State University in 1982. Dr. Hancock received her A.A.S. in architectural technology from Del Mar College in 1977, graduating Cum Laude. She is a Registered Professional Engineer in Tennessee. She is a member of the Transportation Research Board and American Society of Civil Engineers.

Lamine Mili, Ph.D.

Dr. Mili is a Professor of Electrical and Computer Engineering at Virginia Tech. He received an Electrical Engineering Diploma from the Swiss Federal Institute of Technology, Lausanne, in 1976, and the Ph. D. degree from the University of Liege, Belgium, in 1987. Dr. Mili is a senior member of the Power Engineering Society of IEEE, the recipient of a 1990 NSF Research Initiation Award and of a 1992 NSF Young Investigator Award. He has 5 years of industrial experience with an electric utility. His research interests include risk assessment and management of catastrophic failures, risk-based decision theory, multi-criteria decision under uncertainty, robust statistics, power system stability analysis and control, robust signal processing, robust state estimation, nonlinear optimization, and multifunction radar systems. He published more than 60 technical papers; many of them appeared in journals such as the Annals of Statistics, Probability and Statistics Letters, IEEE Transactions in Power Systems, IEEE

Transactions on Circuits and Systems, International Journal of Electric Power & Energy Systems, Electric Machines and Power Systems, and the International Journal of Bifurcation and Chaos. Dr. Mili is the co-founder and co-editor of the International Journal of Critical Infrastructure. He has recently organized an NSF workshop dealing with the mitigation of the vulnerability of critical infrastructures to catastrophic events. The main papers presented at this workshop appeared in the first issue of the International Journal of Critical Infrastructures

Dr. Mili pioneered several methods in SCADA-based state estimation that have been adopted by the power industry. For example, various versions of the bad data identification method initiated by Dr. Mili have been commercialized by vendors such as Control Data Corporation, Siemens, and PCA Corporation, and implemented in the energy management systems of many electric utilities throughout the world. Furthermore, Dr. Mili's robust state estimation method was implemented at the control center of a Swiss electric utility and currently at a Brazilian Southern company. Because his topology estimator is not prone to divergence problems while being able to cope with all types of errors in the circuit breaker statuses, it has been recently incorporated in the energy management system of Siemens.

Besides state estimation, Dr. Mili made important contributions for solving a wide variety of problems relevant to the power industries. He proposed many practical solution methods in transient and dynamic stability, voltage stability, robust control, nonlinear optimization, security analysis, restoration, and risk assessment and management of cascading failures leading to blackouts. He and his student improved on the energy function approach for transient stability assessment by proposing a fast dynamic gradient method for potential energy boundary surface detection. Furthermore, he contributed to the development of a novel wide-area control using agent technologies together with fuzzy-neural networks to damp inter-area oscillations of a large-scale power system while coping with various nonlinearities and uncertainties of the system model. Recently, he and other colleagues pioneered the development of a nonlinear optimal power flow method based on the modified barrier-augmented Lagrangian technique to optimize the reactive resources of a blackstart system. As part of the EPRI-DOD Complex Interactive Networks Initiative, he developed a probabilistic method that find the weak links of a system where self-healing controllers are to be placed.

Michael Willingham, Ph.D.

Dr. Willingham is an energy and environmental analyst, with experience in policy, technology, educational program design, and professional training. His work experience includes the United Nations, USAID, the US Congress, the World Bank, the Peace Corps, the Navajo Tribe, and the private sector.

Since April 2000, Dr. Willingham has been attached to Virginia Tech Institute as an Adjunct Professor. Current projects include identifying the problems and opportunities confronting the Commonwealth in relation to the growth of high-tech industry and the move toward deregulation of energy services. During this period he undertook an assignment with USAID Ukraine in a six-week exercise to evaluate the success of USAID energy programs in Ukraine over the past eight years. He served as Chief of Mission for three-week in-country mission, and as head of the mission report preparation team. In another consultative capacity, he participated in a USAID-sponsored mission to India as part of a mission team to assist the

Government of India with policy aspects of sustainable energy development and greenhouse gas mitigation.

In 1970, Dr. Willingham was disaster relief volunteer in Peru, assigned to the Peruvian agency (Cooperacion Popular) following a major earthquake. He worked in the disaster area for six months, conducting environmental evaluations of towns, distributing supplies and preparing topographic maps for relocated population centers, and working with architect/planner to develop template for village reconstruction. Additional relevant activities include a mission to the Solomon Islands (1994) to explore the possibility of developing an environmental trust fund designed to protect the nation's timber resources, and also to determine disposal practices for imported waste oil, including the possibility of its use as an energy primary fuel. More recently, he has worked to analyze post-disaster impacts of Hurricane Isabel (September 2003) in the electric power sector.

Subcontractor Employees

PJ Aduskevicz

PJ Aduskevicz is a Senior Business Executive with extensive leadership in Optical Transport, Internet & Switching Operations: Engineering, Network Reliability, Security and Industry Forums and a proven track record of team building, increased responsibility and personal advancement with a thorough knowledge of the global marketplace. Additional areas of expertise include Network Reliability and Disaster Recovery, Cross Industry Roles/Industry Leadership, Capital Management, Engineering, Public Policy, Regulatory Policy, Operations Management, and Security.

In her professional career, she has worked as AT&T's Network Vice President of Disaster Recovery, Security and Reliability, where she led a team of specialized subject matter experts providing AT&T Disaster Recovery capability for service restoration in the event of major network interruptions such as 9.11.2001. She also managed formulation and implementation of corporate policy in response to Homeland security issues raised by the State and Federal Agencies and represented AT&T as external spokesperson in industry leadership positions and forums. Prior to this position, she also held the Network Vice President of Infrastructure and Media position from 2000 – 2002, and the Division Manager of Switching and Transport Engineering position from 1998-2000, both at AT&T.

She received her Bachelor of Arts from Western College for Women and participated in Executive Education Programs such as Penn State Human Resources Management, Eckerd College Leadership Development Seminar, Brookings, Understanding Federal Government Operations, and AT&T Advanced Management Program. She also holds a current Top Secret Clearance.

Terrence P. Ryan

Mr. Ryan, a Certified Protection Professional, has 22 years of security leadership and security management experience in the US, Europe, Asia and the Middle East. Recent work

includes consulting services in support of the National Capital Region assessment project., antiterrorism planning for US Navy ashore facilities, assessments at selected Reagan National Airport facilities, Veteran Affairs Hospitals, pre-construction antiterrorism planning in Arlington, VA, and antiterrorism exercise design for Seminole County, FL. Background includes directing infrastructure security and law enforcement for the U.S. Army Corps of Engineers, where he established the Corps critical infrastructure protection and risk assessment program for 300+ structures associated with the nation's inland waterway system. This \$80 million program is a benchmark for the nation's Federal, state and local dam owners. Experienced in planning and managing activities of intelligence, physical/information/personnel security, foreign travel, law enforcement, information assurance, foreign disclosure, and anti-terrorist programs. He retired as Lieutenant Colonel with 22 years of active Army service with Active Top Secret/SSBI security clearance.

Mr. Ryan received his MA in Management from Webster University in 1995, his BS in Criminal Justice from Rochester Institute of Technology in 1981, and his Certified Protection Professional (CPP) Number 10275 in December 2003. Additional coursework has included a Security Engineering Design ZCourse from Protective Design Center, an Electronic Security System Design, Electronic Security Center, a Combating Terrorism Course and the Counter Terrorism Instructor Training sponsored by the U.S. Army Military Police, a Special Security and Antiterrorism Driving Course, and a Risk Assessment Methodology for the Security of Dams.

Paula Scalingi, Ph.D.

Dr. Paula Scalingi is President of The Scalingi Group, LLC, which provides expertise to private and public sector organizations in the areas of infrastructure security, emergency preparedness, energy assurance, and information assurance. Her accomplishments include: development of a framework for a holistic preparedness approach and a concept for a private-public sector "Partnership for Regional Infrastructure Security" for the Pacific Northwest Economic Region, a consortium of five states and three Canadian provinces; organization and facilitation of a major infrastructure interdependencies exercise—*Blue Cascades* (June 12, 2002) and development of an infrastructure security Action Plan for the region. Other activities include: creation of similar infrastructure security partnership initiatives for the San Diego, California Region and the Gulf Coast Region (centered in New Orleans) for the U.S. Department of the Navy Critical Infrastructure Protection Program, including developing and conducting interdependencies exercises (*Golden Matrix* and *Purple Crescent*, respectively); also, facilitating the development of a Great Lakes Partnership for Infrastructure Security and Interdependence with the Chicago Manufacturing Center, FEMA Region V and regional stakeholders.

Dr. Scalingi also facilitated development of the first state-sponsored interdependencies study, including a public-private Partnership and interdependencies tabletop exercise—*Amber Waves*, for the State of Iowa. She assisted the Canadian federal government to develop its first regional interdependencies (*Silver Links*) initiative focused on the Northeast region/Canadian-U.S. border states and provinces. Other accomplishments include developing two regional exercises focused on cyber security interdependencies for the U.S. Department of Homeland Security—*Blue Cascades II* in Seattle in September, 2004 and *Purple Crescent II* in New

Orleans in October 2004. The former initiative led to the creation of the Puget Sound Partnership for Regional Infrastructure Security. In addition, Dr. Scalingi developed a regional security strategy framework for the San Diego Unified Port District; homeland security initiatives for a technology services company and an energy technology manufacturer; and assisted a major metropolitan water authority identify security shortfalls, conduct an interdependencies workshop and a follow-on tabletop exercise. Dr. Scalingi currently serves as an advisor to the National Capital Region (Maryland, Washington, D.C. and Virginia) Vulnerability Assessment Project and is helping develop their regional initiative effort.

Dr. Scalingi has extensive, in-depth experience in all aspects of infrastructure security and broader homeland security issues. Before establishing The Scalingi Group in October, 2001, she founded and served as Director of the Office of Critical Infrastructure Protection at the U.S. Department of Energy, where she developed and implemented a strategic plan, including a multi-year R&D program to develop CIP tools and technologies. She also conducted widespread outreach on cyber security and infrastructure assurance and assisted stakeholders to develop critical infrastructure protection action plans. Dr. Scalingi managed a program area focusing on infrastructure interdependencies analysis and analytic tool development and another that conducted vulnerability assessments at energy companies. She provided technical assistance to the Infrastructure Protection Subcommittee of the Utah 2002 Winter Olympics Public Safety Command, including developing a regional infrastructure assurance plan and the first interdependencies exercise — *Black Ice*. She also developed a team of multi-disciplinary experts from National Laboratories and other institutions to provide a “virtual analysis capability” to federal agencies. In addition, she developed with the California Utilities Emergency Association an interdependencies workshop, *Red Heat*, focused on energy reliability and security preparedness. She developed energy disruption preparedness guidelines for communities for the Chicago Metropolitan Area and Utah, which have been adopted by other states. Lastly, Dr. Scalingi assisted the electric power, and gas and oil sectors in developing their Critical Infrastructure Protection action plans and Information Sharing and Analysis Centers. She served as the government chairman of the National Petroleum Council’s CIP Subcommittee, as the DOE representative to the North American Electric Reliability Council CIP Working Group, and as an advisor to the Association of Metropolitan Water Agencies on CIP issues.

Before her DOE tenure, Dr. Scalingi was founder and director of the Infrastructure Assurance Center at Argonne National Laboratory and simultaneously director of the Decision and Information Sciences Division, where she managed and expanded the program base of the 370-person, multi-disciplinary division, which developed tools, models, and information systems to address needs of more than five dozen federal and private sector, and international organizations (more than 150 programs). During this time, she expanded the Division’s advanced information technology work in data management, analytic tools, and decision support; also, application of division and Laboratory capabilities to consequence management of chemical, biological, and nuclear incidents and to infrastructure assurance. She developed a new program area for the Laboratory that focused on critical infrastructure protection, comprised of more than a dozen projects for several federal organizations. In addition, she served as Technical Liaison to the President’s Commission on Critical Infrastructure Protection, 1996-97, overseeing Commission reports on electric power, oil and gas distribution and supply, chemical/biological water supply contamination, emergency services, legal and regulatory issues, and R&D strategy. Further, she developed a program focusing on chemical/biological dispersion modeling and

initiated discussions with DARPA that led to a multi-million dollar biological agent detection program.

Dr. Scalingi's experience also includes eight years at the Central Intelligence Agency, three years at the Arms Control and Disarmament Agency, and two years at the U.S. House of Representatives Permanent Select Committee on Intelligence. In addition to her activities as president of The Scalingi Group, Dr. Scalingi currently is co-director of the Stony Brook University Forum on Global Security, a non-profit organization reporting to the President of the University and located in New York City, which she co-founded to foster private/public sector cooperation on homeland security issues. The Forum's first major activity involved developing a pilot bio-security training program with a grant from the Carnegie Corporation.

Dr. Scalingi has served in leadership capacities in security and IT professional organizations. She regularly speaks throughout the nation at professional symposia and other events on infrastructure and homeland security topics and is a member of the faculty of the U.S. Office of Personnel Management's Critical Infrastructure Protection Course for federal managers. She is the author of a book and several articles on security, national security, and intelligence issues.

Lee Zeichner

Lee M. Zeichner is Publisher of the Zeichner Risk Assessment, a newsletter dedicated to critical infrastructure issues. The newsletter, which Mr. Zeichner began publishing in 2002, covers vulnerability and threat assessments, IT security, business continuity, liability, capital planning, and corporate governance.

ZRA also consults industry and government on the development of critical infrastructure programs as well as laws and regulations. Mr. Zeichner was senior counsel to the President's Commission on Critical Infrastructure Protection (1996-1997) and served as a legal consultant to the Critical Infrastructure Assurance Office (1998-2001). He now consults on critical infrastructure issues for the Department of Homeland Security, including the National Communications System and the National Cyber Security Division. He also serves as counsel for the Business Roundtable's Security Task Force and is a Visiting Scientist at Carnegie Mellon University's Software Engineering Institute.

Mr. Zeichner is a graduate of Georgetown University Law Center (1988 cum laude). He graduated from the University of Florida (B.A. 1983, Phi Beta Kappa) and received his Masters from Stanford University (M.A. 1984). Mr. Zeichner is a member of multiple bar associations, including the Florida and DC Bars, the Court of International Trade, and the Court of Appeals for the Federal Circuit.

Mr. Zeichner recently completed the third edition of Cyber Security & Corporate Liability, a guide for corporate counsel on security and risk management, published by Lexis Publishing (June 2003).

Thomas F. Zimmerman, PhD.

Dr. Zimmerman is Senior Research Associate in GMU School of Public Policy's Office of International Medical Policy. He is the principal investigator for the development of a vulnerability assessment guide to assist healthcare organizations in developing an organization wide *all hazards* situational awareness and to identify potential points of vulnerability as a foundation for risk management solutions. He served in the medical education and medical practice divisions of the American Medical Association. At the AMA, a primary responsibility was in the development of professional self-assessment and for continuing medical education.

He served as Associate Vice Chancellor for the University of Illinois' Medical Center, and the Director of the Illinois Area Health Education System, a successful program decentralizing education for the health professions in community settings. He held faculty appointments in the Center for Education Development and in psychiatry (medical psychology) at the University Of Illinois College Of Medicine. During his tenure as Associate Vice Chancellor of University of Illinois Medical Center (Chicago), he served on the leadership team to move health professions education out from and off the tradition geographic campus to community site extending out across the Northern half of Illinois. This involved the innovation of several technologies and their application to education, which have now become strategic in "distance education". Dr. Zimmerman directed a budget of \$19 million in this project.

Dr. Zimmerman was the founding Director of the Annenberg Center for the Health Sciences on the campus of Eisenhower Medical Center in Rancho Mirage, California. This Center is regarded as the state-of-the-art television production center for professional and consumer education. Dr. Zimmerman served as Executive Vice President for Education and Research for Eisenhower, and held the Bob and Delores Hope Chair in Medical Education.

Dr. Zimmerman headed the design and implementation for three successful professional education television networks currently operated by Primedia. These include: *Interactive Distance Training Network (IDTN)*, an advanced interactive network of training suites located in class-A office buildings across the U.S.; *PsychLink*: an education television network consisting of psychiatric hospitals and community mental health centers: and, *Family Medicine Television Network*: a television network consisting of healthcare practice sites where specialists in family medicine receive their training.

Dr. Zimmerman has extensive international experience in Europe, Russia, Mexico and South America. He served for several years as medical education consultant to the World Medical Association. Dr. Zimmerman serves as medical education consultant for *CenterNet*, the interactive television network of the Association of Academic Health Centers.