Improving Homeland Security &

Critical Infrastructure Protection and Continuity Efforts

Paula D. Gordon, Ph.D.

pgordon@erols.com

3/25/2003

Table of Contents

· The Initiative to Harness the Best Analytic and Modeling Tools to Develop Effective Protective Solutions

· The Initiative to Guard America's Critical Infrastructure and Key Assets Against 'Inside' Threats

· Overall Critical Infrastructure Protection Efforts

· Elements that the Current Approaches and the Alternative Approach Share

Part 3: Comparing Currently Mandated Initiatives with an Alternative Approach

· The Way in Which the Problem is Being Defined

· Recognition of Critical Infrastructure Sector Interdependencies and the Nature of Cascading Failures and Impacts

· Interdependencies and Cascading Impacts and Ripple Effects

· Cascading Impacts Resulting from 9/11

· The Nature and Extent of the Focus on Information, Data Gathering, the Cataloguing of Facts, and Modeling

· The Different Nature of Terrorism and Terrorist Threats Post 9/11 and the Implications of These Differences

· The Way in Which the Definition of the Problem Drives or Fails to Drive Action

· The Role of Pragmatic Strategies

· The Degree to Which Organizational, Professional, Jurisdictional, Cultural, and Political Challenges are Recognized and Addressed

· The Degree to Which "State of the Science" and "State of the Technology" Issues are Recognized and Acknowledged

· The Degree of Preciseness in the Use of Commonly Used Terms

· Way to Improve Current Efforts

Part 4: An Alternative Approach: Some Major Elements Involved in Defining and Addressing the Homeland Security Problem

· The Goals or Purposes of Addressing Homeland Security Problems, Challenges, and Threats in An Alternative Approach

· An Approach to Describing the Kinds of Weapons and Threats Challenging the Post 9/11 World

Return to Paula Gordon's Homeland Security Page or to Next Part

Improving Homeland Security &
Critical Infrastructure Protection and Continuity Efforts

Paula D. Gordon, Ph.D.

3/25/2003

Introductory Note

This paper refers to a number of key documents. These include the following: A **National Strategy for Homeland Security** (July 2002), the National Homeland Security Act of 2002 establishing the Department of Homeland Security (November 2002), **The National Strategy to Secure Cyberspace** (February 2003), and **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** (February 2003). No attempt has been made here to provide an in depth summary of the initiatives that have been described in these documents. The reader may wish to review the documents prior to reading this paper.

Part 1

An Overview of the Problem

This paper addresses the following questions:

~ What major homeland security and critical infrastructure protection initiatives have evolved and begun to be implemented since 9/11 and
~ What improvements are needed in homeland security and critical infrastructure protection efforts in order to advance the nation's homeland security goals?

Problemsolving

Before addressing these questions, it may be helpful to consider homeland security and critical infrastructure protection efforts in light of the problemsolving process. Note: "Problemsolving" will be used here as shorthand for "addressing a set of complex problems, challenges, and threats".

What are the major elements of problemsolving? The major elements involved in problemsolving can be seen as including problem definition, identification of alternative courses of action, resource availability, managerial capability, and leadership. In Table 1, these are more fully elaborated.

Table 1: Elements of Problemsolving

~ Problem Definition: Recognizing, defining, and understanding the nature and scope of the problem

~ Alternative Courses of Action: Identifying and judging the merits, feasibility, and potential promise of different possible approaches to addressing the problem

~ Resource Availability: Possessing adequate human, fiscal, and material resources and the ability to muster the resources needed to address the problem

~ Managerial Capability: Possessing adequate managerial and administrative capability needed to orchestrate efforts to address the problem

~ Leadership: Having the skills, vision, knowledge, experience, interest, understanding, initiative, commonsense, courage, sense of responsibility, ingenuity, creativity, commitment, and tenacity to determine and carry out a course of action, and having the flexibility and perceptivity to change course as changing circumstances may require.

Problemsolving in the Wake of 9/11

The events of September and October 2001 set in motion efforts to address challenges that had not been experienced before, challenges that very few had even imagined. The organization of government efforts on and after 9/11 was of necessity undertaken hastily. There was little time to give adequate attention to all the various elements involved in problemsolving that ideally should have been addressed. Action was needed on many fronts at once. Indeed multiple crises needed to be addressed. Initial efforts were born in an atmosphere of crisis. Even strategic planning efforts took shape in an atmosphere of crisis. These efforts reflected an amalgam of many different perspectives concerning the nature and scope of the problems, challenges, and threats before us.

Milestones

There have been many milestones to date: Plans, actions, and objectives have undergone many changes in the aftermath of 9/11. The U.S. Patriot Act was enacted into law. Executive Orders and Presidential Directives have been issued or have been the focus of renewed attention. A **National Strategy for Homeland Security** was crafted by the Office of Homeland Security and released in July of 2002. In addition, the National Homeland Security Act of 2002 establishing the Department of Homeland Security was enacted into law in November of 2002.

The following strategies were released by the Administration beginning in September of 2002. To a greater or lesser extent, these strategies all pertain to homeland security and critical infrastructure protection. These include: **The National Security Strategy of the United States of America** (September 2002), **National Strategy to Combat Weapons of Mass Destruction** (December 2002), **National Strategy for Combating Terrorism** (February 2003), **The National Strategy to Secure Cyberspace** (February 2003), and **The**

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (February 2003).

Some generalizations are offered here in Table 2 concerning ways in which the Administration has been addressing homeland security and critical infrastructure security efforts since 9/11.

Table 2: The Administration's Critical Infrastructure Protection Efforts Since 9/11

~ Development of pertinent strategy documents
~ Development and passage of pertinent legislation
~ Attention has been given to refining the way in which critical infrastructure is defined and to understanding critical infrastructure interdependencies and vulnerabilities and determining priority areas of consideration.
~ Increasing attention has been given to ways of protecting critical infrastructure.
~ Advisory groups and other organized efforts that came into being under PDD/NSC-63 prior to 9/11 have shifted and expanded their focus
~ Additional advisory groups and additional organized efforts have been established at several levels since 9/11. The newly established groups provide the Administration a means of eliciting input regarding the national strategy.
~ Efforts have been expended in the establishment of public/private sector partnerships, including notably the Partnership for Critical Infrastructure Security.
~ Strategies relating to the **National Strategy for Homeland Security** have led to the enabling legislation and to the development and refinement of related strategies and plans of actions.

Major Critical Infrastructure Noted in the National Strategy and in the Homeland Security Act of 2002

The Federal government's list of critical infrastructure and key assets includes the following:

~ agriculture, food (including meat and poultry and all other food products);
~ water;
~ public health;
~ emergency services (including emergency preparedness communications systems);
~ government (including continuity of government and continuity of operations;
~ defense industrial base;
~ information and information technology systems (including electronic financial and property record storage and transmission systems);
~ telecommunications systems (including satellites);
~ energy (including power production, generation, and distribution systems);
~ transportation;
~ banking and finance;
~ chemical industry and hazardous materials;
~ postal and shipping; and
~ national monuments and icons.

(from the **National Strategy on Homeland Security**, p. 32 and Title II, Section 201 (d) (5) of the Homeland Security Act of 2002).

In the **Homeland Security Act of 2002**, the term "'critical infrastructure' (also) has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 519c(e)". In that section, the term "critical infrastructure" means "systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or/and combination of such matters."

The Major Critical Infrastructure Protection Initiatives in the National Strategy and the Homeland Security Act of 2002

The major initiatives pertaining to critical infrastructure protection as these are described in the **National Strategy for Homeland Security** and as they have been mandated in the **Homeland Security Act of 2002** include the following:

~ Unify America's infrastructure protection effort in the Department of Homeland Security.

~ Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets.

~ Develop a national infrastructure plan.

~ Securing cyberspace.

~ Harness the best analytic and modeling tools to develop effective protective solutions.

~ Guard America's critical infrastructure and key assets against 'inside' threats.

~ Partner with the international community to protect our transnational infrastructure.

(**National Strategy on Homeland Security,** pp. 29 - 35)

The **Homeland Security Act of 2002**, as well other key Administration's actions and initiatives, reflect a certain approach to the defining the scope and nature of the problem of homeland security and critical infrastructure security. This is true of the **National Strategy on Homeland Security** (July 2002) and the subsequent release of related strategies. **The National Strategy to Secure**

Cyberspace (February 2003) has spelled out in greater detail strategies for addressing cyber-related infrastructure concerns. **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** (February 2003) has focused on strategies for addressing non-cyber-related infrastructure concerns. An alternative set of strategies based on a somewhat broader way of defining the problem will be described later in this paper. This set of strategies will highlight approaches that would help improve current efforts.

Similarity of Goals

It also bears noting that while the definition of the problem in that alternative approach is different in some ways from the definition of the problem implicit in the Administration's approach, the implicit and explicit goals that both Secretary Ridge and President Bush have stated are quite similar to the goals of the alternative approach. They share a common emphasis on national, economic, and personal and societal security.

In November of 2001, Governor Tom Ridge, then head of the Office of Homeland Security, spoke of the need for a strategy that would help ensure national security and economic security, as well as personal security. Indeed, in signing the terrorism insurance bill on November 26, 2002, President Bush also underscored his determination "to make American safer" and "make our economy stronger."

Part 2
A Preliminary Assessment of Efforts

What follows is a preliminary assessment of efforts made to date regarding homeland security and critical infrastructure protection initiatives. Several questions are raised here regarding the progress that has been made to date involving homeland security and critical infrastructure security and continuity.

These questions include the following: Has the Administration made progress in implementing its efforts thus far? Is the implementation of these efforts likely to help ensure realization of the Administration's stated goals? Would a change in strategy and the implementation of other initiatives be more likely to ensure the realization of the Administration's goals? If, so what would those alternative or modified initiatives look like?

Six of the initiatives just noted are viewed here in light of these questions.

The Initiative to Unify America's Infrastructure Protection Efforts in the Department of Homeland Security

In order to be successful in implementing this initiative, adequate attention needs to be given to organizational culture and change issues. This can be accomplished through providing education and training for those in government who have responsibilities relating to homeland security and critical infrastructure security and continuity, including those in positions of greatest responsibilities. In order for efforts to be maximized, there needs to be present both a common understanding of the challenges being faced, as well as a common sense of purpose. Reorganization is no guarantee that individuals from extremely different professional backgrounds and organizational cultures, and individuals from organizations that have had markedly different missions will be able to collaborate effectively. Managerial skills, leadership, and education and training may well be key to the success of reorganization efforts. (Education and training initiatives that would address these concerns are described in some detail in Paula D. Gordon, August 2002).

Regarding the physical location of the Department, there is an argument to be made for leaving the parts of new Department where they are at present and using cybertechnology and telecommunications to maintain a virtual organization. The productivity of the Department might be enhanced greatly if there were no

major disruptions owing to physical relocation of various part of the Department. If massive relocations take place, the Department would likely lose numerous skilled and knowledgeable employees.

The Initiative to Build and Maintain a Complete and Accurate Assessment of America's Critical Infrastructure and Key Assets

With some exceptions, most infrastructure sectors are only at the beginning stages of assessing infrastructure and key assets. **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** (February 2003) provides a helpful overview of the status of such efforts. It also provides a plan of action. There appear, however, to be many unresolved issues including the level of detail that is needed or sought when it comes to undertaking such assessments. Some might refer to this initiative as a "boil the ocean" initiative, owing to the daunting amount of data that would be sought and processed. The costs of such undertakings are also in question. Another question is the extent to which government will be directing, facilitating, and/or controlling the process. In addition, there is a question concerning the availability of individuals with the knowledge, skills, experience, and expertise to carry out the assessments.

For those sectors just starting out, the likelihood of achieving goals set by the Administration seems quite problematic as of March 2003. Some additional reasons for this beyond those just mentioned involve the technical, as well as practical feasibility of completing assessments involving such an overwhelming amount of information and requiring such extraordinary skills of research, synthesis, analysis, and understanding.

Another reason that the success of efforts is problematic is that faulty assumptions are being made concerning the "solvability' of the problem. One can also question the usefulness of assessments that provide an overabundance of information, and an amount that some would argue far exceeds the amount of

information needed to take effective action. The approaches to assessment that are described in the **National Strategy for Homeland Security** (July 2002), the National Homeland Security Act of 2002 establishing the Department of Homeland Security (November 2002), and **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** (February 2003) seem to be geared toward implementation of a micromanaged strategy. Yet, micromanagement and crisis management are not compatible since the former assumes a predictable environment. Crisis management takes place in an unpredictable environment and calls on skills and approaches that are quite different from those involved in micromanagement. A major question that needs to be addressed is this: Are we in an environment that is essentially predictable or are we in a turbulent environment that calls for crisis management and extraordinary flexibility and creative thinking and problemsolving? The documents just mentioned seem to be based on the assumption that we are in an essentially predictable and stable environment, not a turbulent environment in which immediate and near term actions to address problems are needed. The alternative approach that will be described in this paper assumes that we are in the latter kind of environment and that crisis management is needed to address immediate problems, challenges, and threats.

Assessments and Action

Consider an analogous hypothetical situation involving national health policy: How would national health policy be affected if a decision were made to conduct a detailed health assessment every child in the nation? Even if time and resources permitted the completion of a health assessment of every child, how could such detailed assessments be used in a timely way to determine what actions needed to be taken? Isn't there a point at which you can gather more information than you need in order to take action? It there a point at which you can gather more information than you can possibly use?

Looked at from a slightly different perspective, what would the difference in policies and actions likely be if we were to address health problems based on the needs that are already known and obvious as opposed to waiting to address health problems until after an extensive and comprehensive assessment were completed? Would policies and actions be likely to be that much more effective if it were possible to have perfect knowledge of the nature and extent of the problem? Might it be possible to arrive at a sufficient assessment of what needs to be done without undertaking a long term, time and resource intensive assessment? Might it be possible to make a quick assessment relying on an understanding of facts that are known or that are discernible in the near term, based on common sense, experience, knowledge, wisdom, and good judgment? Isn't that the approach that the best and most effective leaders and managers have always used in a crisis situation? Indeed, in a Federally-declared disaster, quick assessments of damage are required in order to qualify for Federal assistance. The assessments need to be quick so that action can be taken as soon as possible to minimize the impacts of a disaster and to proceed with the response and recovery process.

There is a need to recognize that a crisis situation full of unknowns calls for common sense, experience, and wise and courageous action that take into consideration that which is already obvious. The alternative approach outlined in this paper emphasizes the need for taking action in as timely a manner as possible while basing actions on immediate or near term assessments of the situation.

The Initiative to Develop a National Infrastructure Plan

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (February 2003) is a major milestone in the development of a critical infrastructure protection plan. This strategy document, along with **The National Strategy to Secure Cyberspace** (February 2003) constitute the most

fully elucidated plans released by the government on infrastructure protection since 9/11. A major emphasis of **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** is assessment. The concerns just raised regarding assessment-related initiatives are relevant here as well. There may need to be a reworking of the approach if there is to be buy-in on the part of those in the private sector who own and have responsibility for upwards of 85% of the critical infrastructure. If the plan is to provide a basis for collaborative efforts, that is one thing. If the focus is on government regulation or centralized planning, then major resistance can be expected. In addition to the question of "buy in", there are potential major issues involving proprietary or closely-held information. There are concerns regarding costs, accountability, and liability. The plan that is detailed in **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** may be viewed in some ways as a "one size fits all" approach. It also would seem to require micromanagement to implement. It seems highly unlikely that such an approach would find widespread acceptance even if the task were feasible and resources were readily available. Instead an approach that focused more on near term positive actions could be taken. Such an approach could focus on enhancing preparedness, protection, security, contingency planning, response and recovery capabilities, consequence management, and continuity planning. This alternative approach would seem more feasible, acceptable, and helpful than undertaking long term assessments and waiting to determine what actions to take to enhance these capabilities and preparedness efforts. If decisionmakers cannot let go of their emphasis on long term, time and resource intensive assessments, then it would seem extremely important to implement a second and simultaneous strategy, one that focuses on addressing preparedness, security, and continuity needs in the near term, while also focusing on constantly improving near term readiness for dealing with challenges and problems that might occur.

The Initiative Aimed at Securing Cyberspace

A new national strategy for securing cyberspace, **The National Strategy to Secure Cyberspace,** was released in February of 2003. Efforts to develop a national infrastructure plan and actions to secure cyberspace have been ongoing since the issuance of PDD/NSC-63. Implementation efforts have been amplified and taken on new dimensions since 9/11. However, even with the release of **The National Strategy to Secure Cyberspace** in February, efforts do not seem to include the same kind of pragmatic focus that was apparent during Y2K. A difference between that time and the present is that during the years preceding the Y2K rollover, there was sufficient recognition and understanding of the threats and challenges posed by Y2K-related failures, including cascading failures that could have been triggered. At present, there is no comparable level of recognition and understanding of the seriousness of the threats of cyberterrorism and cyberwarfare and threats to cybersecurity and continuity. Plans of actions are needed that are based on an understanding of the nature of the threats and on an understanding of what needs to be done. Leadership and facilitation of efforts appears fragmented and a common sense of direction appears to be missing. There is also a question concerning how priorities will be determined. In addition, there is another question: How well will cross sector vulnerabilities be addressed? While vulnerabilities involving digital control systems (DCS) and Supervisory Control & Data Acquisition (SCADA) Systems are discussed in **The National Strategy to Secure Cyberspace**, the difficulties of implementing approaches that address such vulnerabilities do not seem to be fully acknowledged or well thought through. Vulnerabilities relating to the satellites and the Global Positioning System (GPS) in particular seem to be overlooked.

As regards actions needed to enhance cybersecurity, the recommended guidance that existed prior to February 2003 did not seem to be reaching those who needed it, including those inside government. (Witness the results of the report card for 24 Federal agencies that Congressman Horn issued in 2002. This assessment will be more fully described below.) Whether the latest guidance

that can be found in **The National Strategy to Secure Cyberspace** will have the hoped for effect seems doubtful. It order for it to be effective, it would need to be accompanied by exceedingly successful awareness raising, education and training, and technical assistance initiatives that equaled, if not surpassed approaches used for Y2K. To be successful it would seem helpful that such approaches build on Y2K legacies and lessons learned. (This topic is discussed more fully in Paula D. Gordon, November 2001.)

A comprehensive multi-pronged approach is needed that includes a focus on a range of concerns:
~ underlying problems that give rise to vulnerabilities;
~ preventive and protective actions;
~ remediation and mitigation;
~ preparedness in the face of threats of attacks, sabotage, and mischievous actions that can have potentially devastating effects on operating systems;
~ crisis management, contingency planning; and
~ planning and preparedness for consequence management, recovery and continuity.

The Initiative to Harness the Best Analytic and Modeling Tools to Develop Effective Protective Solutions

Efforts to date appear to be fragmented and a variety of very different approaches appear to be under consideration. These approaches reflect a wide array of problem definitions and implicit values and purposes that are not necessarily in accord with the stated goals of homeland security and critical infrastructure security and continuity efforts.

The kinds of tools envisaged by those emphasizing the importance of this initiative may indeed be developed and they may be used, but how useful can such tools be in advancing overall homeland security and critical infrastructure

protection efforts? In order to have real utility, they would need to be based on a realistic understanding of the nature and scope of the problem that needed to be addressed. For instance, modeling a response or an alternative response to the anthrax attack of that kind that occurred in October of 2001 would need to take into consideration the organizational, jurisdictional, political, and cultural aspects involved in the situation. Questions concerning who's in charge? and where are the resources coming from? would be questions that need to be addressed in any modeling of a possible approach.

It might be equally if not more helpful to focus on lessons that could be gleaned from other situations that bear some similarity to the kinds of problems, threats, and challenges that we are facing now and that we are likely to face in the future. Scenarios could be considered. Simple as well as complicated scenarios can be effectively used for educational and training purposes. Much can be gleaned from the study of lessons learned in crisis situations that have occurred since 9/11, and all of these approaches may be of particular use to planners, crisis managers, and decisionmakers.

It would also be helpful to focus efforts on creating and sustaining healthy organizational cultures. It would be helpful to focus attention on building open lines of communication and trust among those who have perhaps not worked too well in emergency situations in the past, individuals who are likely to need to work together in the future. Memoranda of understanding could be worked out amongst the agencies, institutions, and jurisdictions that need to be working together to plan and prepare for contingencies and take other actions aimed at meeting homeland security and critical infrastructure protection goals.

The Initiative to Guard America's Critical Infrastructure and Key Assets Against 'Inside' Threats

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets has certainly been the farthest reaching elucidation of a plan of action to date. Still, there does not seem to be the kind of focus on the need for immediate and near term action that was apparent during Y2K. This may be owing in part to the fact that there is no universal recognition of the nature and scope of the threat. In addition there is no widespread understanding of steps that need to be taken. The costs associated with taking action may also slow the decisionmaking and implementation process. Leadership and facilitation of efforts to address challenges appear fragmented and a common sense of direction appears to be missing. Relevant guidance does not appear to be reaching those who need it. Well-coordinated efforts to get the message out, including the strategies released in February of 2003, are not evident.

Much needs to change in order to achieve a higher level of security and to ensure that efforts to meet security and continuity challenges are maximized. A more effective course of action is needed, one that helps ensure that guidance and technical assistance reaches those who could use it and one that also helps ensure that guidance and technical assistance are made available in a variety of inexpensive and easily deployable forms, including online. (See Paula D. Gordon, January 2002 for recommendations concerning uses of e-technology to advance homeland security efforts; January 2003 for current references and resources; and November 2001 regarding relevant Y2K lessons to be learned. Also see 1998 and 1999 for an overview of specific actions recommended for Y2K that would also maximize many of the kinds of efforts needed post-9/11.)

Overall Critical Infrastructure Protection Efforts

Prior to the release of **The National Strategy to Secure Cyberspace** and **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets**, the nature and extent of efforts seemed less focused, less well defined and less well coordinated than Y2K efforts. With the release of these two

strategic action documents, efforts do seem to be better focused and better defined than they had been previously. Implementation of the strategies described in **The National Strategy to Secure Cyberspace** (February 2003) would seem dependent on the emergence of individuals with leadership and managerial skills and resources who are able to help facilitate implementation of those strategies. The strategies described in the **National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** (February 2003) will face similar challenges, plus some additional ones. That strategy document **appears** to be prescribing a micromanaged approach to critical infrastructure protection and security, a kind of approach that could well prove unworkable on several levels. First of all there is a likely reluctance on the part of the private sector (and even parts of the public sector) to go along with the approach being prescribed. The approach would likely meet with considerable resistance if it is perceived as being ill-fitting and/or top down. The approach might also be difficult to implement owing to the need for considerable expertise to undertake a micro-level assessment effort and then develop and micromanage the implementation of the plans that would presumably follow from such an assessment effort.

Sector efforts in which notable headway has been made in the area of critical infrastructure protection and security include: air and marine transportation, banking and finance, electric power (the North American Electric Reliability Council), telecommunications; and oil and gas (the National Petroleum Council). The cross sector efforts of the Partnership for Critical Infrastructure Security (www.pcis.org) have also made promising strides.

In order for goals to be achieved in our current crisis environment, efforts need to be undertaken that reflect a broad and realistic understanding of the problem as well as a realistic assessment of current challenges and threats based on what is already readily known. At present, the initiatives as they have been developed do not seem to reflect such a focus, They do not seem to recognize that there is

a need to be ready, prepared, and protected with contingency plans in place "yesterday". Current efforts also seem to be based on faulty assumptions regarding the potential usefulness of micro-oriented analytic approaches and tools. Current efforts do not seem to be based on an adequate understanding of qualitative and non-quantifiable factors. They also seem to be based on faulty assumptions concerning the "solvability' of the problem, including especially the solvability of current problems and challenges using traditionally used methods. In addition, there seems to be a failure on the part of many to understand the implications of the crisis that we are in. There seems to be a failure to come to grips with the fact that we are in a situation that is full of unknowns, a situation that calls for common sense, experience, and wise and courageous action.

Many seem to have difficulty grasping the fact that predicting the behavior of homicidal/suicidal terrorists with any degree of certainty is not within the realm of possibility. Many also seem to have difficulty grasping the full implications that the presence and persistence of so many homicidal/suicidal terrorists have for the security of the nation and the world, as well as the future stability of civilization.

In addition, many seem to have difficulty recognizing how essential near term actions are and how essential it is that near term actions are taken now to maximize preparedness, mitigation, protective measures, security, contingency planning, crisis response and management capabilities, consequence management and recovery capabilities, and continuity of operations planning. These are key to maximizing efforts to address present threats and challenges.

There are similar difficulties in recognizing that actions that are taken to maximize preparedness, mitigation, protective measures, security, contingency planning, crisis response and management capabilities, consequence management and recovery capabilities, and continuity of operations planning need to designed to serve multiple purposes at once. Through using ingenuity

and common sense, it is possible to design actions that serve multiple purposes, actions that serve simultaneously to strengthen national, economic, and individual and societal security.

It should be noted that the government's Ready Campaign (www.ready.gov) that was launched in February 2003 represents a major step forward when it comes to preparedness, but these efforts do not begin as yet to equal Y2K preparedness efforts provided for during 1999 by the Federal Emergency Management Agency (FEMA) and the American Red Cross. Unlike Y2K preparedness efforts, there are no well publicized community-based efforts as yet. There are also no phone hot lines that the public can use to address questions to information specialists. There are also no hotlines that the public can use to check out rumors. There are not specialized hotlines that State and local officials can use to get responses to their questions.

The Ready Campaign that was launched in February 2003 provides guidance information in print and online. These encourage the public to stock three days of supplies. Such a stock of supplies would of course be helpful in a wide range of emergency situations, including man-made and natural disasters. Guidance that was issued in 1999 close to the Y2K rollover emphasized the need for 7 - 10 days of supplies. Older FEMA material had recommended two weeks of supplies. There is no reason that such initiatives could not be urged now.

There is also no comparable online policy forum, such as the one that the General Services Administration had hosted during 1998 and 1999 for Y2K. Such a forum might be helpful in surfacing and sharing valuable suggestions concerning ways to improve current efforts and build on the expertise and insight of those who may not presently be in roles of public responsibility.

The need for clearinghouse efforts is noted in the strategy documents released in February 2003. Such efforts include providing for the dissemination of

information concerning lessons learned and best practices. They need to do so both reactively and proactively. There is also a need to provide education, training, and technical assistance.

In sum, there are many ways that current efforts could be improved or augmented. Copious amounts of far-sightedness are needed in our current situation. Efforts need to be informed by self honesty, common sense, understanding, ingenuity, good will, humanity, belt-tightening, selfless service, and commitment to addressing the extraordinary challenges and threats facing us.

Last, but not least, the nation is still recovering from 9/11 and subsequent attacks. The fact that these impacts are still very much with us needs to be fully acknowledged and addressed.

Elements that the Current Approaches and the Alternative Approach Share

In his book, **Silence**, John Cage tells a story about Arnold Schoenberg, the composer. Schoenberg was teaching a class on music composition at UCLA. He posed a musical composition problem to the class and asked the class to come up with a solution. A solution was offered. Then he asked for additional solutions and the class came up with additional solutions. Finally, he asked the class what did all the solutions have in common?

Perhaps Schoenberg's questions can be applied to the problem of homeland security and critical infrastructure protection. What common elements can be found in approaches that are needed to address the homeland security and critical infrastructure problems, challenges, and threats?

Part 3
Comparing Currently Mandated Initiatives

with an Alternative Approach

The following parameters can be used to identify areas of weakness in current efforts and to compare current efforts with the alternative approach that will be described shortly. These parameters are listed in Table 3:

Table 3: Parameters for Comparing Currently Mandated Initiatives with an Alternative Approach

~ The way in which the problem is being defined, and, most importantly, the extent to which critical infrastructure sector interdependencies and the nature of cascading failures and impacts are understood;
~ The courses of action that have been identified and the basis for determining what courses of action to take;
~ The nature and extent of the focus on information, data gathering, the cataloguing of facts, and modeling;
~ The different nature of terrorism post 9/11 and the implications of these differences for the nation, the world, and humankind;
~ The way in which the definition of the problem drives or fails to drive actions;
~ The role of pragmatic strategies;
~ The degree to which organizational, professional, jurisdictional, cultural, and political challenges are recognized and addressed;
~ The degree to which "state of the science" and "state of the technology" issues are recognized and understood;
~ The degree of preciseness in the use of commonly used terms; and
~ The adequacy, appropriateness, and potential usefulness of approaches to understanding and assessing vulnerabilities.

Several of these parameters and aspects of them are discussed more fully here.

The Way in Which the Problem is Being Defined

A common frame of reference could help people understand each other when they speak of homeland security efforts and critical infrastructure security and continuity. The Homeland Security Impact Scale that will be described shortly may help provide such a framework. This impact scale may provide a context for understanding in a very general way the nature and scope of the challenges, threats, and problems facing the nation and the world. The impact scale can be seen as providing a way of looking at and comprehending the dynamically changing nature of the situation in which we find ourselves. The impact scale provides a frame of reference for understanding, considering, and interpreting the nature and scope of the problems, challenges, and threats that face us. It also provides a framework for considering the actual, possible, and potential impacts of those problems, challenges, and threats. The Homeland Security Impact Scale can help focus attention on ways of looking at actions needed to address those problems, threats, and challenges. It can conceivably help us focus homeland security and critical infrastructure protection efforts along the most positive and constructive lines possible.

Recognition of Critical Infrastructure Sector Interdependencies and the Nature of Cascading Failures and Impacts

Key to understanding the problems, threats, and challenges posed by terrorism today, is understanding critical infrastructure independencies and the potential for cascading failures and impacts. This understanding can be critical to the success of efforts to maximize homeland security and critical infrastructure protection. Yet, such a focus often gets left out of discussions of "critical infrastructure". Cascading failures and impacts refer to what can happen when failures or disruptions involving specific infrastructure assets or sectors have ripple effects that can extend to other infrastructure sectors.

Some excellent analyses and discussions of cascading impacts and the interdependencies of infrastructure elements can be found in the writings of

Richard G. Little (1999, 2002, May 2002) and Jeffrey R. Gaynor (2002) among others. A report issued in April of 1999 by the U.S. Department of Commerce also provided an excellent analysis of the cascading impacts that cyber-related failures and disruptions could have on national and global economies. Indeed these same kinds of failures could be triggered today by cyberterrorism and cyberwarfare or by sabotage or mischievous acts. The cascading effects could become widespread as a result of the slowly evolving degradation of cyber-related systems or the rapid and cascading failure of such systems and interconnected infrastructure.

Other relevant work on cascading impacts was done during the years leading up to Y2K. Many regional, national, and global scenarios were considered. Among these were scenarios by the Naval War College and the Department of Defense. Scenarios considered by the Naval War College are available online (Naval War College, 1999).

Senator Robert Bennett who had been at the forefront of Y2K efforts was one of the first to emphasize the significance of connectivity issues and interdependencies amongst the various infrastructure sectors. He was one of the first to draw attention to the very real potential for cascading failures. Consideration of Y2K-related scenarios can also be found online in a White Paper on Y2K (Paula D. Gordon, 1998 and 1999). A graphic depiction of Senator Bennett's approach can also be found there.

Scenarios have also been used widely since 9/11 in workshop exercises and simulations. Several that have been far reaching in their implications have involved cyberterrorism threats. Some examples include the Gartner Group's Sector 5 Conference held in Washington, DC, August 21 - 23, 2002 and the Digital Pearl Harbor Exercise also held in 2002. Information on both is online. As previously noted, consideration of such scenarios are extremely pertinent today because cyberterrorism and cyberwarfare and other threats to

cybersecurity and continuity could trigger the same kinds of mid-range and worst-case scenarios that were envisioned with Y2K. The attack of the slammer worm in early 2003 was the most recent example of how fast an attack could spread and how widely cybersecurity could be breached. Consider what the extent of the damage might have been had there been no software patches to stop the spread of this worm and no relatively simple ways to repair and prevent damage.

Other exercises and simulations have focused attention on a wide range of other kinds of scenarios, including ones involving public health threats. Scenario-driven exercises can be extremely helpful in that they can force individuals to consider interdependencies that they had not previously considered.

Some selected causes that could result in significant cascading impacts are listed below. If any of the following were to occur slowly and incrementally over time or if they were to occur as a result of quickly cascading failures and disruptions, the societal as well as economic impacts could be severe and long lasting.

Some of the possible causes of significant societal and economic consequences include the following:

~ Widespread or regional disablement of portions of the electric power grid;
~ Widespread or regional disablement of the Internet;
~ Widespread or selective disablement of computer systems or complex digital control and SCADA systems;
~ Destruction or disablement of refineries and/or pipelines;
~ Disruption or disablement of transportation systems;
~ Disruption or disablement of the financial sector;
~ Disruption or disablement of telecommunications systems;
~ Disablement of water purification and/or distribution systems;
~ Chernobyl- or Bhopal-type catastrophes.

A longer listing of potential problems will be provided shortly. Similar lists of problems that could be associated with cascading infrastructure failures can also be found in Part 2 of the White Paper on Y2K noted earlier (Paula D. Gordon, 1998 and 1999).

Recognizing the interdependency of infrastructure sectors or elements is crucial to the development of any plan of action whether it involve preparedness, protection, mitigation, contingency planning, crisis management, response, recovery, or continuity of operations. Recognizing the interdependencies of infrastructure sectors and assets is also crucial to any steps that are taken to strengthen the infrastructure. Viewing infrastructure sectors as if they could be understood sufficiently if considered solely in isolation from one another has extremely limited utility at best.

Interestingly enough, much attention is paid to interdependencies in **The National Strategy to Secure Cyberspace** and in **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets**. The discussion of cascading impacts, however, seems to be sharply circumscribed. Worst case, catastrophic, or cataclysmic scenarios in which resources would be significantly impacted or totally overwhelmed are not really considered. Neither are the possible worst case and near term impacts of catastrophic events. An assumption is also made that intensive analytic and modeling techniques can provide the most sound basis for developing and implementing a plan of action. The myriad of possible scenarios and the ultimate unpredictability of what can happened and how scenarios might actually unfold can render the use of such techniques of only limited utility to planners, policymakers and managers. The way in which a crisis unfolds and the factors affecting the responses to a crisis cannot ultimately be predicted; the factors that can come into play simply cannot be fully foreseen. Actions simply cannot be pre-scripted.

Interdependencies and Cascading Impacts and Ripple Effects

One way of viewing infrastructure interdependencies might be found in the following children's nursery rhyme:

For want of a nail the shoe was lost;
For want of a shoe the horse was lost;
For want of a horse the rider was lost;
For want of a rider the battle was lost;
For loss of the battle the kingdom was lost;
And all for the want of a horseshoe nail.

Another way of viewing interdependencies and the potential for cascading impacts might be in terms of the following analogy: If one were to throw rocks into a still pond, each rock would create ripple effects. If rocks were thrown into the pond simultaneously or in rapid succession and were in close enough proximity to one another, ripple effects would intersect and would create new ripple effects of their own. These effects cannot be predicted. Possibilities can, however, be considered. Owing to the many factors influencing the configuration of such ripple effects, it is not possible to map every conceivable scenario that could occur, nor would it be a wise way of using significant portions of one's resources. What can be helpful is to think through many different possible scenarios, including simple scenarios. Even simple scenarios can provide extremely significant learning experience. Indeed, if the learning that can be gleaned through studying simple scenarios has not been mastered, there is little to be gained in trying to absorb the lessons of more complicated and daunting scenarios.

Yet another way of viewing cascading impacts is to consider what happened as a result of the attacks on September 11.

Cascading Impacts Resulting from 9/11

It is critically important that we recognize the cascading impacts that have occurred as a result of 9/11. It is also important that we recognize that such impacts are continuing to occur. Many seem to have little awareness or understanding of these impacts even though the effects of 9/11 are still very much with us. The effects include psychosocial and societal impacts, as well as major economic repercussions. The 9/11 attacks as well as the subsequent anthrax attacks also have led to a refocusing of attention of government efforts and resources. Significant resources have not only been directed to response and recovery efforts, more resources continue to be directed at addressing homeland security and defense needs. There are even ripple effects from raising or lowering the nation's alert status.

The attacks of 9/11 immediately affected numerous sectors. Other sectors have been affected more gradually over time. Sectors that have been affected have included, but have not been limited to public works and emergency services, telecommunications, financial and financial services sectors, airlines, railways, tourism, the hospitality sector, and the insurance sector. While to date there seems to be awareness of some of these impacts, the most recent strategy documents do not seem to reflect a full recognition of the nature and extent of the impacts on security, economic stability, and the social fabric.

The Nature and Extent of the Focus on Information, Data Gathering, the Cataloguing of Facts, and Modeling

Another parameter that deserves attention involves the nature and extent of the focus on information, data gathering, the cataloguing of facts, and modeling. There is a point at which detailed information, data gathering, and cataloguing of facts can overwhelm the mind or otherwise make it difficult to consider, let alone settle upon a sound course of action. In the midst of a crisis, a focus on these

can get in the way of taking immediate action or near term actions that the situation may require. In fact, a continuing quest for facts can be a way of delaying action when action could be taken based on facts that are abundantly obvious.

In a crisis situation, in a situation in which the costs of inaction are high, one can be best served by taking the wisest actions possible at the time. Substituting study and acquisition of data for action for action may give one a sense of control, but it may cause the loss of valuable time and minimize one's chances for action or survival.

There are those who seem to be wedded to slow and methodical approaches to data gathering and analysis even in circumstances where common sense, experience, training, preparation, and good judgment could yield equally useful if not superior insights concerning what needs to be done. There are seemingly few who are versed in taking action based on what has been learned and what can be readily learned. For those unused to working in crisis situations, it can be helpful to consider what the differences might be between taking action in the near term and waiting to act until after extensive time and effort were spent in data gathering, study, and analysis. It can also be helpful to recognize that only a certain range of results are conceivable in data gathering and analytical efforts. It can be helpful to consider what the range of possible results might be and then ask these questions: Would any of these possible results affect the course of action that seems the most sound based on what is already known? Would any of the conceivable results of extensive research and analysis make a significant difference regarding what needs to be done? What common set of actions are needed whatever the results of the analyses might be? Surely there are actions that could be undertaken relying on common sense, experience, and good judgment alone. Note: Dean Harper and Haroutun Babigian (1971) described the concept of "advocacy evaluation" in the mental health field. The approach that I have described here has been borrowed and adapted from their work.

There is a widespread penchant today for dedicating extraordinary resources to data gathering, analysis, benchmarking, and assessment. Such proclivities can be emphasized to the point of slowing or even paralyzing the problemsolving process. There are also widespread tendencies to ignore common sense, or fail to use good judgment, or fail to draw on one's experience and wisdom. If those heading up efforts to rebuild Europe at the time of the Marshall Plan had allowed themselves to be hobbled by kinds of tendencies that are so prevalent today, we might still be rebuilding Europe. There are simply certain things that need to be done. Indeed, there are things that need to be done no matter what the short term or long term economic consequences. In-depth studies might well refine those most obvious actions in minor ways, but the actions that are taken may be little different from what they would have been had no extensive assessment been completed. In the end, the assessment of costs, risks and benefits involve consideration of values, principles, and purposes, any or all of which can override consideration of costs and risks.

If proclivities for in-depth studies and assessments had driven Mayor Giuliani's efforts, the response to the attacks of 9/11 would have been stultified. The nine miners in Pennsylvania would not have been rescued. The Three Mile Island near melt down in the '70s would have ended in large-scale disaster. Special Operations Forces that have been so key to military efforts since 9/11 would not be able to take action in dynamical changing and life threatening circumstances.

There are reasons why many have become so reliant on or enamored of doing extensive analysis. Such analysis can be a substitute for action. It can be a way of delaying action. It can also provide an illusion of control in a time of extreme uncertainty. Another reason is that the Newtonian paradigm, empirical methodology, and reliance on analysis that focuses on quantifiable data and measures have become deeply engrained in the minds of most everyone. This includes all who have studied in a university in recent decades and it also

therefore includes most who function in roles of public responsibility. Institutions of higher learning tend to focus on "narrow rationalist" approaches to understanding problems, threats, and challenges. They do not tend to do a good job in helping to develop the kind of leadership, managerial competencies, and organizational skills of a Rudy Giuliani. They do not tend to train individuals who are comfortable in exercising initiative; accepting and wielding responsibility; thinking "outside the box"; using sound judgment; and wedding knowledge, understanding, insight, intuition, well honed instincts, experience, and common sense to action. Indeed in organizations that are heavily micromanaged and regulated, those who have such capabilities can be seriously handicapped in their attempts to act using their common sense, knowledge, wisdom, judgment, understanding, creativity, skills, and discretion. Indeed, such individuals can find it difficult getting hired in the first place.

The Different Nature of Terrorism and Terrorist Threats Post 9/11 and the Implications of These Differences

The new kind of homicidal/suicidal terrorist values neither life nor the future viability of civilization. This new kind of terrorist manifests neither humanity nor conscience. They appear to have no moral compass or sense of the sanctity of life. Perspectives that were typical concerning the behavior of terrorists prior to 9/11 can no longer be viewed as being applicable. There is no way of predicting with any degree of certainty what any one of this new kind of terrorist, any group of such terrorists, or any network of terrorist groups might do. Will they go after hard targets, soft targets, mixes of these, or will they simply make threats and use fear to try to undermine the stability of society? A fairly thorough cataloguing of possible terrorist actions already exists. A vast amount is now known regarding the past and present intentions of the terrorists. Surely efforts to learn more need to continue in order to deter, kill, or apprehend and bring terrorists to justice. But how much more comprehensive or detailed does our knowledge need to be in order for us to take effective action when it comes to

emergency preparedness and contingency planning and taking steps to strengthen our security? There are only so many kinds of protective and preventive measures that can be taken. Why not begin by doing what we can do based on what we already know needs to be done? Why not plan to enhance our efforts when it is possible to do so? Once basic preparedness steps have been taken, additional questions might be asked. What can be done **now** based on what is currently known regarding weapons and tactics that could conceivably be used? What can be done now based on what is currently understood concerning the potential impacts of such weapons and tactics? In what ways could additional information conceivably alter basic actions that are needed now? **Why not attend as fully as possible to basics now?** The fact is that anything could happen at any time. The government's Ready Campaign launched in February of 2003 is a first step in the right direction. But there are numerous other preparedness approaches and initiatives, some of which have long track records. FEMA's community-based program model known as Project Impact is but one example. Other preparedness efforts undertaken during 1998 and 1999 for Y2K by FEMA and the Red Cross, as well as the President's Council on the Year 2000 Conversion could also be used as models or built on. The Citizen Corps, even if the program is not funded by Congress, could be implemented in some form. Our challenge is to continue to do what can be done now to address the problems, threats, and challenges we face, while keeping our focus on our goals of strengthening our national economic, personal, and societal security to the extent possible.

We are in a different ballgame post 9/11. There are no clear rules. Today's terrorists have stated and demonstrated their intent to destroy life without concern for even their own lives. They have been clear that there is no way that they can be appeased. There is nothing that can be done to change them from their destructive course of action. The implications that such aberrant behavior has for the future stability of the world are grave indeed. The full implications have yet to sink in fully. As others have said, "This is not your father's war."

The reason that any of this is important is that how the problem is understood can affect our motivation to take action.

In the Volume 1 of the **Discourses,** Meher Baba addressed the subject of non-violence and violence. He wrote that in a situation in which a mad dog is in a school yard, that a mad dog must be subdued using violence in order to protect the weak. This analogy seems to me to be wholly applicable to the homicidal/suicidal terrorists in the world today: Today's homicidal/suicidal terrorists can be seen as the mad dogs and the nation and the world as the school yard. The threat they pose is increased exponentially owing to their willingness to used weapons of mass destruction and disruption to achieve their destructive goals. It behooves us to do all in our power to rid ourselves of the threat they pose and to take defensive action in face of the attacks that we have suffered. At the same time we need to be doing all we can to strengthen and secure our situation. If we fail to act, our future and the future of generations to come will be in ever increasing jeopardy.

There can be multiple reasons for the fact that so many seem to be oblivious to the changes in the world that have occurred as a result of 9/11 and the implications of these changes. One of the reasons can be a certain naivete concerning human nature and the assumption that surely what we have seen to date have been isolated examples of aberrant behavior. For others, they may simply be disinclined or reluctant to recognize the full extent of the challenges and threats that face us. They may be in a state of denial. Yet another reason can be a deeply embedded assumption that taking action based on the results of traditionally accepted modes of analysis somehow holds the key to our security, that such approaches will allow us to control the situation that we find ourselves in and they can be relied on to do so in the future. Many seem to believe that action taken base on the use of these modes of analysis that have been so widely relied on in more stable times will somehow get us out of the situation that

we are presently in. They may be acting on the assumption, if not the hope, that a reliance on such approaches can in and of themselves somehow make things right.

The Way in Which the Definition of the Problem Drives or Fails to Drive Action

The November 2002 Hart/Rudman Task Force Report was a call to action. The President of the Council on Foreign Relations, Lawrence Gelb wrote the following in the introduction to the report: "…Still, given the stakes - potentially the loss of thousands of innocent American lives and the mass disruptions of American's economy and society-there are things we must be doing on an emergency basis to reduce our vulnerabilities here at home…." (Council on Foreign Relations, November 2002).

The interconnectivity of specific sectors of the infrastructure to the economy is stressed in the November 2002 Hart/Rudman report. The report also includes recommendations concerning specific steps that can be taken to reduce vulnerabilities. In making a case for implementing these recommendations, the authors of the report place their recommendations within a larger context of concerns. In their view, preparedness is crucial since preparedness can help "reduc(e) the appeal (of terrorism) as an effective means of warfare." The authors underscore the importance of taking steps to prepare for, protect against, and mitigate the impacts of possible attacks, and to be prepared to recover from them when they occur. They write: "By sharply reducing, if not eliminating, the disruptive effects of terrorism, America's adversaries may be deterred from taking their battles to the streets of the American homeland."

The approach taken by The Heritage Foundation in their Backgrounder issue of September 10, 2002 also emphasizes the need for action. The authors of that issue state the following: "Despite the progress that has been made on homeland

security thus far, much more needs to be done to eliminate blatant vulnerabilities, increase security, boost efficiencies, and facilitate preparedness and response capabilities in every community." (Heritage Foundation, September 2002). A number of specific recommendations are made there.

One of the recommendations in the report involves the need to address GPS vulnerabilities, since GPS plays such an important part in the nation's infrastructure. (Heritage Foundation, January 2002). Note: There is no comparable treatment of GPS vulnerabilities in **The National Strategy to Secure Cyberspace** and **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.** Little assurance can be found in these documents that DHS or the Homeland Security Council (formerly the Office of Homeland Security) might be constituting themselves in such a way that they will be certain to identify and address such cross-cutting and complex areas of concern. Perhaps this would be a more fitting role for the White House Office of Science and Technology Policy to play.

It is edifying to note that **The National Strategy to Secure Cyberspace** and **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets** reflect a greater consciousness of infrastructure vulnerabilities and their connection to national, economic, personal, and societal security than other government documents or legislation that have been issued or passed since 9/11. These documents are headed in the right direction, but would be better focused if many of the prescriptions and initiatives in them did not overshadow a concern for action in the near term and if they were not embarked on a path that could result in a deluge of information that might be either counterproductive or of limited usefulness.

The Role of Pragmatic Strategies

In 2002, Congressman Horn's Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations focused considerable attention on cyber-related critical infrastructure. Testimony before Congressman Horn's Subcommittee, including assessments by the General Accounting Office have tended to focus on cyber-threats, cybersecurity and cyber-related aspects of critical infrastructure. Congressman Horn also released a "Computer Security Report Card". This report card was based on agency reports from 24 different agencies. The reports were required under the Government Information Security Reform Act of 2000. The vast majority of the agencies received grades of D's and F's. Exceptions were the Social Security Administration (B-), the Department of Labor (C+), and the Nuclear Regulatory Commission (C). These results have especially significant implications for critical infrastructure security since the delivery of critical government services would be in jeopardy were there to be a failure of information technology within these agencies. A question that needs to be asked is this: Where is the sense of pragmatic concern that drove Y2K remediation efforts? Efforts to ensure cybersecurity and continuity require a similar commitment to pragmatic action. Among those addressing such concerns have been Michael Vadis (Dartmouth University), Paul Kurtz (National Security Council, and Edward Yourdon. See the latter's work released in 2002 entitled **Byte Wars: The Impact of September 11 on Information Technology**.

An extremely significant but relatively overlooked area of concern has gotten well-deserved attention in hearings held by Congressman Horn's Subcommittee. This area of concern involves the vulnerability of digital control systems and SCADA systems to sabotage and terrorist acts. As these systems play such a critically important role in so many critical infrastructure sectors, it is extremely important that adequate attention be given to addressing the vulnerabilities of the systems. (Joseph M. Weiss, 2002; Alan Paller, 2002; John S. Tritak, 2002) Many of the mid-range and worst case scenarios considered during Y2K included a concern for the failure of these complex systems and the impacts that

cascading impacts and disruptions could have. (See Paula D. Gordon, 1998 and 1999.)

The Degree to Which Organizational, Professional, Jurisdictional, Cultural, and Political Challenges are Recognized and Addressed

An example of the role that can be played by organizational, professional, jurisdictional, cultural, and political challenges can have in the managing of emergency situations can be found in the response to the anthrax attacks that began in October of 2001. There are those who feel that the handling of these attacks was extremely problematic. The individuals who had this point of view cite major problems that were not satisfactorily resolved at the time and that have not been completely resolved since. These problems included an absence of clarity regarding what the dimensions of the problem were, how to handle the uncertainties concerning the handling of the matter, who was in charge, and what resources could be and would be brought to bear in addressing the problem. These same individuals feel that unless such matters are resolved, it is unlikely that a future such attack would be handled any more effectively. There are also those who played key roles in the response to the attack who are apparently unaware of the nature and extent of these unresolved problems. None of the government strategy documents released since 9/11 and mentioned here seem to reflect any in-depth awareness of such issues.

The Degree to Which "State of the Science" and "State of the Technology" Issues are Recognized and Acknowledged

Complicating the response to the anthrax attack was the fact that key players and spokespersons possessed very different perspectives concerning the state of the science regarding all the different questions surrounding anthrax, including everything from diagnostic and treatment protocols to forensic and decontamination protocols. In an article on using e-technology to advance

homeland security efforts (Paula D. Gordon, January 2002), the need to hold "state of the science" or "consensus development" conferences on a range of different issues is discussed. These kinds of conferences could utilize an approach developed by the Office of Medical Applications of Research at the National Institutes of Health. Such conferences are needed in order to advance understanding concerning the status of scientific understanding and research. They are also need if the scientific community and key government spokespersons are to speak with as informed and consistent a voice as possible regarding cutting edge issues.

The Degree of Preciseness in the Use of Commonly Used Terms

The use of terms associated with "critical infrastructure" has become a source of confusion and a potential impediment to progress regarding critical infrastructure protection efforts. J. D. Moteff et al. (December 2001 and August 2002) and Richard G. Little (2002) have been among those who have written on this subject.

A major problem that soon emerges as a result of studying the subject of critical infrastructure and critical infrastructure protection is that the same terminology is often used in very different ways. This can be seen even within the same piece of legislation, report, strategy document, plan, or project. Awareness concerning this problem needs to be raised. One way of doing this might be to encourage greater attention to the use of the terminology "critical infrastructure security" or "critical infrastructure security and continuity" and to use those terms to apply to "strengthening, improving, protecting, and restoring critical infrastructure security and continuity." "Critical infrastructure security" and "critical infrastructure security and continuity" used in this way incorporate a kind of directional goal.

Using qualifiers may help clarify what meaning is intended when the term "critical infrastructure" is used. By getting in the habit of using qualifiers, meaning might

become clearer. For instance, many have come to use "critical infrastructure" when they are referring to "cyber-related critical infrastructure". Some use "critical infrastructure" to refer to "physical infrastructure". Some include both "cyber" and "physical" in their use of the term "critical infrastructure". Others might use "critical infrastructure" to include other non-cyber and non-physical kinds of critical infrastructure, such as essential government services and or national assets. It might be helpful to take the extra time and effort to clarify the meaning that one is intending when speaking of critical infrastructure and critical infrastructure security and continuity. Use of the following terms where appropriate might be helpful:

~ "cyber-focused" or "cyber-related critical infrastructure protection";

~ "cyber-related critical infrastructure, including digital control systems and SCADA systems" (when one intends to include such systems);

~ "cybersecurity/continuity" Note: Yet another way of clarifying the meaning given to critical infrastructure security or cybersecurity would be to add the concept of "continuity." For some the concept of continuity may already be encompassed in the concept of critical infrastructure or cybersecurity. For others, it is important to specify critical infrastructure security and continuity and cybersecurity and continuity. In this way there is no doubt that the person using terms is concerned for all aspects of protection and security including proactive measures intended to address a range of possible scenarios and remediation efforts to ensure that vulnerabilities are minimized to the extent possible and that continuity of operations is provided for to the extent possible;

~ "critical physical infrastructure";

~ "critical physical and other non-cyber infrastructure";

~ "critical infrastructure in general" (encompassing physical, cyber and other non-cyber-related critical infrastructure); and

~ "critical infrastructure security" might be used as shorthand for "critical infrastructure protection and infrastructure security and continuity in general" when the all-inclusive use of the concept is intended.

One reason for using these terms with greater care and precision is that a person's perspective concerning "critical infrastructure" may well be grounded in that person's professional training and expertise. Those who are specialists in one kind of critical infrastructure cannot be expected to have a ready interest in or understanding of all the various kinds of critical infrastructure. Those with specialized expertise may in fact find it hard to understand the various kinds interdependencies that exist among different kinds of critical infrastructure. They may fail to understand the kinds of cascading impacts that successive or simultaneous failures can have. An expert in computer technology may have little or not expertise concern digital control or SCADA systems and their vulnerabilities. Or alternatively, those with specialized expertise may intellectually understand that failures involving such systems could occur and could have cascading impacts, but they may have little or no experience or expertise that would prepare them to integrate or translate that understanding into responsible action.

Way to Improve Current Efforts

What might a national strategy or an assessment of national homeland security and critical infrastructure protection efforts look like if it were based on a more comprehensive problem definition found in the **National Strategy for Homeland Security** or the National Homeland Security Act of 2002 or **The National Strategy to Secure Cyberspace** and **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets**? What might a national

strategy or an assessment of a national homeland security efforts look as if it were based on an even more comprehensive problem definition than the one found in the most recent Hart/Rudman report? Basing actions on a broader and more comprehensive definition of the nature and scope of the problem could lead to improvements in the way in which homeland security and critical infrastructure protection efforts are being conceived and implemented.

When it comes to discussing efforts involving critical infrastructure, critical infrastructure protection, and critical infrastructure security and continuity, it may prove extremely helpful to consider what an "alternative" definition of "homeland security-related problems, challenges, and threats" might look like.
For the sake of brevity, only the most significant elements of a proposed "alternative" way of defining and approaching the problem will be highlighted here. Mentioned below are some major elements involved in defining and addressing the homeland security problem using the alternative approach being described here. Also included is a set of goals that are explicit in the alternative approach.

Part 4
An Alternative Approach: Some Major Elements Involved in Defining and Addressing the Homeland Security Problem

Some major elements involved in defining and addressing the homeland security problem include the following:

~ The goals or purposes of addressing homeland security problems, challenges, and threats;
~ The kinds of weapons and threats challenging the post 9/11 world;
~ The range of potential impacts that terrorist actions and threats can have;
~ Elements of critical infrastructure, critical infrastructure protection and critical infrastructure security/continuity;

~ Support functions and efforts needed for maximizing homeland security efforts; and
~ Some specific initiatives.
These will be considered in turn.

The Goals or Purposes of Addressing Homeland Security Problems, Challenges, and Threats in An Alternative Approach

The goals or purposes of addressing homeland security problems, threats, and challenges may be seen as including the following**:**

~ the nurturing and preservation of human life;
~ the fostering of civilized behavior and the preservation of civilization;
~ national security;
~ economic stability and security;
~ societal stability and security;
~ individual security;
~ critical infrastructure security/continuity; and
~ the preservation of natural resources and the environment.

An Approach to Describing the Kinds of Weapons and Threats Challenging the Post 9/11 World

In describing the nature and scope of the problem, it is important to recognize the kinds of weapons and threats challenging the post 9/11 world. These may be seen as including the following:

~ Chemical weapons;
~ Biological weapons;
~ Nuclear weapons;
~ Radiological weapons;

~ Explosives;
~ Hazardous materials releases as a result of sabotage or a terrorist act;
~ Suicidal bombers and terrorists;
~ Cyber-warfare and cyber-terrorism or other sabotage of cybersystems;
~ High frequency emitters, electromagnetic pulse, and other kinds of electronic weapons;
~ Other conventional and unconventional weapons and tactics, including missile launchers, truck bombs and the use of airplanes or vehicles as weapons, random sniper or bombing attacks, and destruction of data and records through non-cyber-related means;
~ Psychological warfare leading to debilitating psychosocial reactions that can accompany attacks or remain after attacks or that can evolve as a result of an ongoing climate of fear and uncertainty or new threats;
~ Incitement of civil unrest; and
~ Simultaneous or sequential use of mixes or different kinds of weapons and tactics.

A Way of Describing the Range of Potential Impacts That Terrorist Actions and Threats Can Have

In describing the nature and scope of the problem, it is important to recognize the range of different kinds of potential impacts that terrorist actions and threats can have in the post 9/11 world. These may be seen as including the following:

~ destruction of human life;
~ material destruction;
~ the weakening or destruction of the viability of civilization;
~ the weakening or undermining of national security;
~ the weakening or undermining of economic security and stability, including the viability of businesses and industries;
~ the weakening or undermining of societal and individual stability and security, including the possible unraveling of the social fabric;

~ the weakening or undermining of critical infrastructure security and continuity; and
~ the destruction of natural resources, the harming of the environment, and weakening or destruction of the viability of the environment.

Elements of Critical Infrastructure, Critical Infrastructure Protection and Critical Infrastructure Security and Continuity in the Alternative Approach

Any of the following sectors or sub-sectors can be categorized under the heading of critical infrastructure or critical infrastructure concerns. It is important to recognize the interdependent character of critical infrastructure and the potential for terrorist acts to trigger cascading impacts. Terrorist actions could conceivably include or impact any of the following:

~ Water supply, water quality, and water distribution systems
~ Water treatment facilities
~ Solid waste treatment facilities
~ Food
~ Agriculture
~ Livestock
~ Airports and air transportation
~ Ground transportation
~ Maritime transportation and ports
~ Rail transportation
~ Highways, bridges, and tunnels
~ Postal services, freight, and shipping
~ Cybertechnology, including information systems and networks
~ Digital control systems/Supervisory Control & Data Acquisition (SCADA) Systems
~ The Internet
~ Telecommunications

~ Fiber optic cable and phone lines
~ Satellites and Global Positioning System (GPS)
~ Financial investments, financial services and the financial sector
~ Insurance services and the insurance industry
~ Real estate investments, real estate services and the real estate industry
~ Energy
~ Electric power plants and facilities
~ Nuclear power plants
~ The coal industry
~ Oil and gas facilities and pipelines
~ Fuel availability, quality, and distribution
~ Chemical facilities, including chemical manufacturing plants, pipelines, and storage tanks
~ Nuclear weapons facilities
~ Hazardous materials facilities, including nuclear waste storage facilities
~ Dams
~ Hospitals and health care services
~ The availability, quality, and distribution of pharmaceuticals
~ The pharmaceutical industry
~ Public health and safety
~ Critical government services, including the continuity of government
~ Emergency management services and emergency medical management services including: emergency preparedness, mitigation, contingency planning, crisis management, consequence management, response, and recovery
~ Infrastructure preparedness, protection, contingency management, crisis management, consequence management, response, and recovery
~ Law enforcement and peacekeeping
~ Domestic intelligence
~ Foreign intelligence
~ National defense and defense capabilities
~ Defense facilities

~ Defense industrial base
~ Military support to homeland security
~ Border security and immigration policies and procedures
~ Large scale buildings and building complexes
~ Landmarks and national monuments and icons

Part 5
The Alternative Approach: A Description of Support Functions and Efforts Needed for Maximizing Homeland Security

The following kinds of support functions and efforts are needed in order to help ensure homeland security:

~ emergency management and emergency medical management, including preparedness, mitigation, response, contingency planning, crisis management, consequence management, and recovery
~ individual, family, and neighborhood and community preparedness
~ business and industry preparedness, mitigation, and protection
~ regional, state, and local emergency management
~ infrastructure preparedness, protection, contingency management, crisis management, consequence management, response, and recovery
~ public communication, information, and education of everyone from the general public to those who are in positions of public responsibility
~ public awareness and education and the media
~ media awareness and support for a constructive role for the media
~ development and implementation of public alert and warning systems
~ development and deployment of alert, warning, and information-sharing systems that are designed to keep individuals in positions of public responsibilities informed and to help support collaborative efforts
~ educating, training, and supporting first responders

~ educating, training, and supporting public works responders
~ educating and training in the areas of preparedness, mitigation, and protection
~ education and training of individuals in roles of public responsibility, including education and training initiatives focusing on capability and skills development for individuals who are a part of local, state, and Federal workforces with homeland security-related responsibilities
~ organizational development and change involving government efforts
~ research development and application
~ innovation diffusion, including technology innovation and application
~ knowledge, research, and technology transfer efforts
~ thinktank-type efforts that track developments and recommend initiatives to decisionmakers
~ the development and operation of clearinghouses, including the identification of model programs, approaches, policies, and legislation; the compilation and proactive dissemination of lessons learned; and the providing of technical assistance and organizational change assistance
~ intra- and inter-agency relations, networking, and coordination
~ intergovernmental relations, networking, and collaboration
~ relations and collaboration with Congress and other legislative bodies at the State and local levels
~ public/private sector networks, partnering, information sharing, and collaboration
~ international relations, networks, and collaboration.

Some Approaches and Initiatives Based on the Alternative Definition of the Problem

A set of alternative approaches and initiatives for homeland security are offered here. Many of these initiatives were noted previously in Paula D. Gordon (December 2001). Other initiatives have been outlined in Paula D. Gordon, January 2002, August 2002, and 1998 and 1999.

Some Specific Initiatives That Are a Part of the Alternative Approach

The best approaches from the past need to be considered and applied where appropriate. With respect to the restoration of economic security, this includes:

~ Instituting Policies and Programs that Foster Full Employment as a Means of Stabilizing the Economy and Strengthening National Security. A top priority is finding gainful and useful employment for all who are unemployed or underemployed. In addition to implementation of a stimulus package, this can be accomplished using a range of innovative means, including providing people with opportunities for part-time work and job-sharing that would allow them an opportunity to draw a salary while looking for work in their field or while retraining when retraining is necessary.

Other approaches include providing for microenterprise and small business loans, fostering the exchange of services ("time dollar" type approaches), and the exchange of commodities for other commodities or services. Innovative low-cost approaches to housing need to be explored and implemented to stave off and reverse the increases in the homeless population. Programs that address the growing problem of hunger in America are also direly needed. Job fairs, online services, and counseling need to be fostered. Other ways of connecting people up with jobs are needed. More people need to be trained in employment services.

~ Sponsoring and/or Finding Sponsorship for Public Works-Type Projects. The development by the public or private sector of the kinds of public works projects that brought the nation out of the Depression and the kinds of efforts that went into the implementation of the Marshall Plan. In those areas where government does not take the lead, then the private sector, the not-for-profit sector, and the general public need to take the initiative.

Individuals are needed to plan, develop, manage, and carry out public works projects, projects that will help rebuild and strengthen those elements of the nation's physical infrastructure that have been in need of attention for decades. For the sake of national security, economic security, and personal and societal security, America's physical infrastructure is in dire need of attention. (The American Society of Civil Engineers has done an excellent job of assessing the dismal status of the nation's physical infrastructure, ASCE, 2001. See Appendix 1.) It bears noting that in **The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets** (February 2003), the authors express a very different view concerning the condition of the nation's physical infrastructure. They state that "our infrastructure is generally robust and resilient."

~ Increasing Security-Related Efforts. Increased attention needs to be given to addressing security needs that currently exist. For instance, additional security personnel are needed in airports, mass transit systems, private and public buildings, nuclear power plants, chemical plants, refineries, and hazardous material facilities. Additional personnel are needed in law enforcement. Additional personnel are need in cybersecurity. Persons are needed to develop continuity of operations plans, data backup systems, and backup telecommunication systems.

~ Shoring Up and Expanding Emergency Preparedness Efforts. Individuals are needed who are skilled or who are interested in being train in any of the various aspects of emergency preparedness, including: disaster mitigation, contingency planning, response, recovery, consequence management, and continuity of operations planning and operations. Currently available training opportunities, including free training through FEMA that is available online, need to be more widely publicized.

~ Developing and Implementing Education and Training Initiatives for Homeland Security. Major education and training initiatives aimed at capacity building for addressing challenges relating to homeland and national security need to be undertaken. (See Paula D. Gordon, August 2002 for specific recommendations.)

~ Expanding Knowledge Transfer, Clearinghouse Efforts, including Information Dissemination, Training, and Technical Assistance Efforts A central information clearinghouse is needed immediately, one manned by information specialists. Disaster.gov (www.disaster.gov) that was launched by FEMA in November of 2002, could serve as the basis for such a service or www.ready.gov that was launched by the Department of Homeland Security in February of 2003, or an amalgamated effort involving the two.

~ Augmenting Health and Medical-Related Services. Social and mental health services, as well as health care services in general need to be expanded. More people need to be trained to serve in such roles.

~ Strengthening National, Economic, Societal, and Individual Security in Other Ways. Approaches need to be developed and implemented that will encourage the temporary (if not a long term) reconsideration of pay scales for those in both the public and private sectors. Attention needs to be given to the examples of those individuals in the private sector who since September 11 have announced their intention to forego their annual bonuses and/or reduce their salaries. Innovative approaches that companies can use to diversify products and services need to be explored. Other ways of "saving" companies and enterprises need to be explored and information concerning interesting approaches needs to be made available, including employee ownership and investment options. Innovative ways need to be found to keep people usefully employed without resorting to layoffs. Best practices need to be followed when layoffs cannot be avoided. Business for Social Responsibility

(http://www.bsr.org) is one source of such best practices. The growing number of layoffs needs to be stopped and reversed.

****

Undertaking such a multi-pronged strategy will have the effect of strengthening essential aspects of the nation's infrastructure. The value of the strategy, however, may become increasingly compelling with time as layoffs continue and strains to economic stability become more apparent. The abundance of good will, patriotism, and constructive and creative energy still available in the wake of 9/11 makes this an opportune time to build support for and implement such a strategy. It is hard to imagine a better moment to join forces to do what we can to strengthen national security, economic security, and personal security. The future of humankind may well depend on America's ability to remain a stable and steadying force in the world.

Different Approaches to Understanding and Assessing Vulnerabilities

How does one begin to consider or assess vulnerabilities in the post-9/11 world? Indeed beyond what common sense can readily reveal, how much more effort is needed to gauge vulnerabilities? What good does it do to analyze scenarios and their possible impacts if insufficient attention is given to taking common sense steps that would increase our chances of surviving, responding, recovering, and ensuring continuity in the wake of whatever may come our way? Taking such steps, of course, could help minimize current vulnerabilities.

Part 6

The Homeland Security Impact Scale: An Alternative Approach to Assessing Homeland Security and Critical Infrastructure Protection Efforts and a Frame of Reference for Understanding and Addressing Current Challenges

An extremely wide variety of perspectives is being brought to bear today on the subject of homeland security and critical infrastructure. Indeed, the subject of infrastructure and critical infrastructure protection is being defined in different ways, using very different perspectives, and sometimes with different purposes in mind as well. Is a common frame of reference possible? Could a common frame of reference be useful in strengthening homeland security and critical infrastructure protection efforts?

The Homeland Security Impact Scale may provide a tool that can help advance understanding of homeland security and critical infrastructure security challenges, options, and goals while providing a common frame of reference. The impact scale may also suggest ways of understanding impacts and the need to take action to reverse impacts. The impact scale may also help in assessing interdependencies of critical infrastructure sectors and the possible consequences of cascading failures and impacts.

The idea for the Homeland Security Impact Scale comes from a similar approach that had been used as a survey tool in 1998 by the Washington, D.C. Y2K Group (WDCY2K). WDCY2K was a group of professionals from the public and private sectors that met on a monthly basis in 1998 and 1999 to network, hear panels of speakers on topics relating to Y2K efforts, and discuss ways of addressing the challenges and threats posed by Y2K. The Y2K Impact Scale was used to survey the membership of the group to get a sense of the different ways in which the possible impacts of Y2K were being assessed (For the results of these surveys, see Bruce Webster, 1999).

The Homeland Security Impact Scale can be used to describe in a very general way the impacts and lingering effects resulting from 9/11 and the subsequent anthrax attacks. The Homeland Security Impact Scale" could be used as a means to describe or indicate in a very general way any or all of the following:

~ What the status of homeland security was prior to the attacks;
~ What the impacts have been since the attacks;
~ What the current status of homeland security has been at various points in time after the attacks; and
~ What the possible status of homeland security might be in the future given any of a range of possible scenarios involving a variety of conceivable factors, interventions, actions, or events.

There are certain givens in the use of this impact scale. To begin with all of the factors that are likely to affect the status of homeland security cannot be foreseen. In addition, because of the turbulent character of the current environment and the dynamically changing and unpredictable nature of the future, there is no tried and true way that the scale can be used to measure with any kind of precision the impact that certain interventions, actions, or events have had or are likely to have. Indeed, if one shares the assumptions implicit in the scale, one realizes that there is no tool or analytic approach that can be used in any kind of precise way to measure impacts. Just as suffering is not amenable to microanalysis and quantification, neither are the widely varied and multidimensional impacts, consequences, and implications of terrorist attacks.

The scale can be used, however, as an educational tool that may help individuals consider or recognize and acknowledge what the "general" state of homeland security is, how it has changed or how it might change. The impact scale can be used as a tool to suggest any or all of the following:

~ how well past impacts have been and are being addressed;

~ what possible kinds of impacts need to be protected against or prepared for given the immediate as well as the longer term effects of past attacks; and
~ what the importance might be of considering a wide range of problems, threats, and challenges that may need to be addressed in the future.

Here then is the Homeland Security Impact Scale:

Homeland Security Impact Scale

0 No real impact on national security, economic security, or personal security
1 Local impact in areas directly affected
2 Significant impact in some areas that were not directly affected
3 Significant market adjustment (20%) + drop); some business and industries destabilized; some bankruptcies, including increasing number of personal bankruptcies and bankruptcies of small businesses, and waning of consumer confidence;
4 Economic slowdown spreads; rise in unemployment and underemployment; accompanied by possible isolated *disruptive incidents and acts, increase in hunger and homelessness
5 Cascading impacts including mild recession; isolated *supply problems; isolated *infrastructure problems; accompanied by possible increase in *disruptive incidents and acts, continuing societal impacts
6 Moderate to strong recession or increased market volatility; regional supply problems; regional infrastructure problems; accompanied by possible increase in disruptive incidents and acts, worsening societal impacts
7 Spreading *supply problems and *infrastructure problems; accompanied by possible increase in disruptive incidents and acts, worsening societal impacts, and major challenges posed to elected and non-elected public officials
8 Depression; increased *supply problems; elements of *infrastructure crippled; accompanied by likely increase in disruptive incidents and acts; worsening societal impacts; and national and global markets severely impacted

9 Widespread *supply problems; infrastructure verging on collapse with both national and global consequences; worsening economic and societal impacts, accompanied by likely widespread disruptions

10 Possible unraveling of the social fabric, nationally and globally, jeopardizing the ability of governments to govern and keep the peace

---

* "Supply problems" and "infrastructure problems may include food shortages; availability of potable water; degradation of water purity, water distribution and/or waste management; fuel/heating oil shortages, disruptions in utilities (power, gas, telecommunications), disruption in the financial sector, disruptions in transportation (airlines, trains, trucking, ports, ships); pharmaceutical shortages; disruption of health care services or emergency medical services; disruption of fire and public safety services; disruptions or inadequacies, or overwhelming of public works operations and services.

- "Disruptions" and "incidents" can include anti-war and other demonstrations, work stoppages, strikes, organized vandalism, looting, and riots. Also included are sabotage and terrorist acts and attacks. (These notations have been adapted in part from notations used in the Y2K Impact Scale in 1998 by WDCY2K. See also Bruce F. Webster, 1999.)

Summation

Assessing the changing status of homeland security and critical infrastructure protection efforts since 9/11 and identifying ways of improving efforts are necessarily qualitative endeavors. Qualitative assessments will vary according to

the perceptions, perspectives, knowledge, understanding, and experience of those making the assessments.

An additional challenge in using the Homeland Security Impact Scale is that there is no precedent in human history for the kind of actions that have occurred and that may occur randomly and without warning in the future. We are in unknown territory. The full force of the implications of these realities does not seem to have been grasped. Evidence of this lies in the fact that there are those who continue to feel that traditional kinds of risk analysis, risk/benefit analysis, and vulnerability and threat assessment are as feasible and relevant post- 9/11 as they were pre-9/11. Those who grasped the implications of the changed reality recognize that "all bets are off" concerning what might happen. As a result, they may see the logic in developing and implementing plans of actions that are multi-dimensional and multi-purpose and address as many contingencies as well as possible. In the language of various fields, including emergency preparedness planning, strategies need to have a "dual use", "multi-use", or multi-hazard focus. Actions need to serve a range of possible purposes or address more than one problem, threat, or challenge simultaneously. The common denominator is that all actions need to have is that they all serve in some way to strengthen simultaneously national, economic, societal, and individual security.

If one accepts Secretary Ridge's and President Bush's stated goals of enhancing national, economic, and personal security as the goals of the Administration's homeland security efforts, then the question that follows is: What progress has been made in realizing these goals? If one assesses the impacts of the 9/11 attacks in the vicinity of the 3 - 5 range on the Homeland Security Impact Scale, then additional questions might be:

~ Have government efforts served as fully as they need to in order to minimize these impacts?

~ What more needs to be done?
~ What more can be done?

Some maxims that might apply here include the following:

~ Deciding where we need to go depends on where you think we are; and

~ What you think we need to do depends on one's perspective, experience, knowledge, understanding, and imagination and one's assessment of the seriousness of the situation that we are in.

While much progress has been made during very turbulent times, there are many actions that can be taken to improve and strengthen all aspects of our security and the position that we are in. The November 2002 Hart/Rudman report and the Heritage Foundation Report (January 2002) both state that vulnerabilities continue to exist and action is urgently needed. The latest strategy documents issued by the government while detailing well many of the vulnerabilities, do not seem to include the kind of strong focus on immediate steps that could be taken that could do much to strengthen our security and the stability of our position. Some of the prescribed approaches would focus extensive resources on long term time and resource intensive studies and assessments of problems, threats, and vulnerabilities. There are, however, problems that can be and need to be addressed now and in the near term, problems that do not require the prior completion of Herculean data gathering and analysis efforts.

What More Needs to Be Done?

What more is needed in the way of preparedness, mitigation, response, contingency planning, crisis management, consequence management, recovery, consequence management, and continuity of operations planning and

implementation? Have we begun to think adequately about such commonsense concerns?

The government launched a first major preparedness initiative in February of 2003. Other initiatives in a range of other areas are evolving. The goals have been generally identified, but to what extent do the current strategies help or hinder progress in achieving those goals. If the strategies serve to slow action and if they result in efforts to micromanage major elements of the problemsolving process, what is the likelihood that they will have a stultifying effect on the creativity and motivation of everyone involved? Creative energies and motivation are crucial to progress. They are crucial to the winning of wars. They are crucial to managing crises. They are crucial to addressing challenges that are unlike any we have known before.

By doing all that can be done to manage a potential or actual emergency, dual or multiple purposes can be addressed. By dedicating our efforts in this way to being as prepared as possible to deal with terrorist attacks, we will also be prepared to deal other man-made and natural disasters as well. We will also be better prepared to deal with hard times that come with economic downturns. Rebuilding, securing, and hardening our infrastructure, will serve to strengthen national security, economic security and stability, societal and individual security and stability.

Where we need to be focusing our efforts at any given point in time needs to reflect an awareness of the highly changeable character of the context that we are in. At the same time, our efforts need to reflect our highest sense of purpose and direction. A major reason for this is that a common sense of purpose, direction, and mission helps ensure that we all working together to do what needs to be done. Such a sense of purpose can become what Mary Parker Follett called "an invisible leader". A common sense of purpose cultivated through "invisible" as well as visible leaders can be key to motivation,

collaboration, and accomplishment. A common sense of purpose as well as a common understanding of the challenges we face, a common definition of the problem, can be key to our progress in addressing the extraordinary challenges before us.

****

Paula D. Gordon, Ph.D.
pgordon@erols.com

Appendices

Appendix 1: Infrastructure and the American Society of Civil Engineers (ASCE)

One way of using "infrastructure" can be found in a document produced by the American Society of Civil Engineers (ASCE, 2001). The ASCE focuses its concerns on what it deems to be the most important elements of the nation's physical infrastructure and the current status of these most important elements of the nation's infrastructure. The ASCE is particularly concerned by the fact that elements of the nation's physical infrastructure have not undergone major improvement in many years. The ASCE has highlighted the status of these major elements of infrastructure in a "report card" that they released in 2001. (ASCE, 2001) The assigned grades are based on "condition and performance, capacity vs. need, and funding vs. need".

ASCE 2001 Infrastructure Report Card

D+	Roads
C	Bridges
C-	Transit
D	Aviation
D-	Schools
D	Drinking Water
D	Wastewater
D	Dams
C+	Solid Waste
D+	Hazardous Waste
D+	Navigable Waterways
D+	Energy

The resulting grade point average is a "D+" for "poor". Based on their evaluation, the ASCE estimates that 1.3 trillion dollars needs to be invested in rebuilding the nation's infrastructure over the next five years. The failure to do so, they argue, will have a very deleterious impact on the nation's economy. (ASCE, 2001)

Appendix 2: The Bureau of Economic Analysis of the U.S. Department of Commerce ~ Another Perspective on Critical Infrastructure

There are many different ways of viewing the relative importance of specific kinds of infrastructure, some stated in terms of a well defined context, others not. One approach might emphasize the economic role that infrastructure sectors may be seen to play in contributing to the domestic gross national product. The Bureau of Economic Analysis of the U.S. Department of Commerce has provided an

example of this approach. In the year 2000, the Bureau rank ordered critical infrastructure sectors in the following manner:

Critical Sector GDP: 2000 Gross Domestic Product (in $Billions) of Critical Sectors

Sector	GDP
~ Finance, insurance, and real estate	1936.2
~ Electric, gas, and sanitary services	230.0
~ Telephone and telegraph	208.9
~ Manufacturing, non-durable chemicals and allied products	191.1
~ Manufacturing, non-durable food and kindred products	137.0
~ Oil and gas extraction	99.5
~ Transportation by air	93.0
~ Farms	79.0
~ Manufacturing, non-durable petroleum and coal products	36.5
~ Railroad transportation	22.9
~ Local and Inter-urban passenger transit	18.7
~ Water transportation	14.8
~ Coal mining	10.1
~ Pipelines, except natural gas	6.2
Total Critical Sector GDP	3083.9
Total US GDP	9872.9
$US GDP Represented by Critical Sectors	31%

Source: 2000 Bureau of Economic Analysis
As cited by Lawrence D. Dietz (2002)

The table can be seen as being somewhat misleading since critical infrastructure sectors are interdependent and cannot, in the final analysis, be viewed in isolation from one another. The table is also potentially misleading in that the figures that are used do not reflect future costs or past sunk costs. An example might involve nuclear power. The contribution of the nuclear power industry to the energy sector does not include the costs that will occur in the future of handling, processing, and storing hazardous waste.

Another example of future costs that are not reflected in current numbers have to do with the cost of taking action to reverse deteriorating conditions that have occurred or that will inevitably continue to occur over time, concerns that the ASCE has underscored. (See Appendix 12.)

The table is also misleading in that there are other sectors that are not included in the list that may be seen as contributing in an indirect, but essential ways to the placement of the sectors on the list. Problems or failures involving sectors that are not on the list could have devastating impacts on sectors that are on the list. For instance, what would be the effect on business and industry if the Internet became dysfunctional or computer security were to be widely breached? What would be the effect on the financial sector, on maritime and air transport, and on defense if GPS were to become dysfunctional?

Viewed in this manner, it becomes apparent there would be definite drawbacks in using the rank-ordered list to determine what areas of critical infrastructure most merit attention.

Appendix 3: The September 10, 2002 Washington Post Assessment

An interesting approach to defining significant elements of the nation's infrastructure can be found in an article by Eric Pianin, Marc Kaufman and others in the September 10, 2002 **Washington Post** entitled "How Experts Grade Homeland Security". In this article, the authors report on the status of the nation's homeland security efforts, including the nation's critical infrastructure protection efforts. The categories of infrastructure used were quite different from those used by the ASCE (Appendix 12). This is partly explained by the fact that the context of their use is quite different. The authors of the **Washington Post** article have their own way of defining and categorizing the various kinds of "critical infrastructure".

The following list includes all of the categories and subcategories used in the **Washington Post** article. Experts were selected by the **Washington Post** to provide brief assessments and assign letter grades in each subcategory**.** Note: "INC" stands for "Incomplete".

<u>The September 10, 2002 Washington Post Assessment</u>

<u>Transportation</u>

F Airports
B Airlines
A Trains, Trucks, and Buses
C Ports and Shipping
B/C- Bridges, Tunnels and Dams
B Public Transit Systems

<u>Energy</u>

A-/B+ Nuclear Power Plants

C Oil, Gas, Electrical Facilities

Infrastructure

B Food and Agriculture
D Chemicals, Hazardous Materials
B/B- Defense Facilities
B+ Mail
B Water Treatment

Counterterror

B Department of Justice
B- Intelligence Agencies
B Department of Defense
D- Health and Human Services
C-/D+ Homeland Security Department
INC First Responders

Public Places

D National Landmarks
C Office, Apartment Buildings
C+ Shopping Malls
D Stadiums and Arenas

Border

B- INS/Border Patrol
C+ Visas

Cyberspace

B- Internet, Computer Networks
INC Telecommunications
D Banking and Finance

In giving a letter grade to a subcategory, the designated expert provided a relatively brief paragraph explaining the reason for the grade. Each expert used his or her own set of criteria for grading. The criteria were often more implicit than explicit. Even so, it is evident that the criteria used for making the assessments varied greatly from expert to expert. Indeed ways of defining and understanding challenges and threats varied greatly. The apparent objectives that the expert thought needed to be achieved also varied greatly.

****

References

American Society for Civil Engineers, "Renewing America's Infrastructure - A Citizen's Guide", 2001 (http://www.asce.org/pdf/citizens_guide.pdf)

American Society for Civil Engineers, The Critical Infrastructure Partnership, http://www.tisp.org

Brookings Institution - Protecting the American Homeland: A Preliminary Analysis (May 2002) (http://www.brookings.edu/fp/projects/homeland/report.htm) (A revised and updated edition due on May 1, 2003.)

Council on Foreign Relations, Gary Hart and Warren B. Rudman, Co-Chairs, Terrorism Task Force Report "America Still Unprepared - America Still in Danger," (November 14, 2002) ID: 173844 (http://www.cfr.org/publication.php?id=5099)

Robert F. Dacey, Director, Information Security Issues, "Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk", Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, November 19, 2002

Robert F. Dacey, Director, Information Security Issues, "Critical Infrastructure Protection: Significant Challenges Need to Be Addressed", Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, July 24, 2002, Oversight Hearing on "Cyber-terrorism: Is the Nation's Critical Infrastructure Adequately Protected?" GAO-02-961T

Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Statement before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, Oversight Hearing on "Cyber-terrorism: Is the Nation's Critical Infrastructure Adequately Protected?" July 24, 2002. GAO-03-303T.

LTC Bill Flynt, "Capabilities Required to Perceive Cyber Attacks Against Distributed Complex Systems", Paper presented at InfowarCon 2002, Washington, DC, September 5, 2002

Gartner Group, The Results of the Digital Pearl Harbor War Game http://www3.gartner.com/2_events/audioconferences/dph/dph.html.

Gartner Group, Sector 5 Conference, August 21 - 23, 2002, (C-SPAN Archives)

Jeffrey R. Gaynor, "Critical Infrastructure Protection/Assurance," A 21st Century National and Homeland Security Imperative, Presentation to: Computer Security and Information Assurance V: Best Practices and Lessons Learned Conference, Potomac Forum, Ltd., Washington, D.C., January 23, 2002.

Joel N. Gordes, "Cyberthreats and Grid Vulnerability," Paper presented at InfowarCon 2002, Washington, DC, September 5, 2002

Paula D. Gordon, "Education and Training Initiatives Needed to Address Threats and Challenges to Homeland Security," August 14, 2002. See http://users.rcn.com/pgordon/homeland/. Also see http://www.mipt.org/pdf/education-traininginitiatives.pdf . .

Paula D. Gordon, "Infrastructure Threats and Challenges: Before and After September 11, 2001". **PA Times**, 24:12, December 2001 and **Journal of Homeland Security**, April 16, 2002. Also see http://users.rcn.com/pgordon/homeland/ .

Paula D. Gordon, "International Relations and National Agendas After September 11, 2001". **PA TIMES**, Vol. 25, Issue 2, February 2002. Also see http://users.rcn.com/pgordon/homeland/.

Paula D. Gordon, "Selected Homeland Security References and Resources," **Business Briefing: Exploration and Production**, Markets Research Centre, January 2003. Also see http://users.rcn.com/pgordon/homeland/ .

Paula D. Gordon, "Strategic Planning and Y2K Technology Challenges: Lessons and Legacies for Homeland Security". **PA TIMES**, Vol. 24, No. 11, November 2001. Also see http://users.rcn.com/pgordon/homeland/.

Paula D. Gordon, "Using E-Technology to Advance Homeland Security Efforts". **PA TIMES**, Vol. 25, No. 1, January 2002**.** Also see http://users.rcn.com/pgordon/homeland/.

Paula D. Gordon, "A Call to Action: National and Global Implications of the Year 2000 and Embedded Systems Crisis: A Working White Paper on Y2K," 1998 and 1999, http://users.rcn.com/pgordon/homeland/.

Dean Harper and Haroutun Babigian, "Evaluation Research: The Consequences of Program Evaluation". **Mental Hygiene**, 55(2) : 151-156, 1971.

Heritage Foundation, **Homeland Security Task Force Report**, January 2002, http://www.heritage.org/homelanddefense/welcome.html.

Robert Lemos, "Nation's Infrastructure Far from Secure". December 2, 2002, ZDNet http://zdnet.com.com/2100-1105-975677.html (article about the views of Ken Watson, head of the Partnership for Critical Infrastructure Security, on the nation's infrastructure.)

Richard G. Little, "Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures," **Journal of Urban Technology**, 9:1 (2002) 109 -123.

Richard G. Little, "Educating the Infrastructure Professional: A New Curriculum for a New Discipline," **Public Works Management & Policy**, 4:2 (October 1999) 93 - 99.

Richard G. Little, "Understanding and Controlling Cascading Failure: A Systems Approach to Multi-Hazard Mitigation," Presented at the 9th Annual Conference of the International Emergency Management Society Facing the Realities of the Third Millennium, May 14 - 17, Waterloo, Ontario, Canada.

J.D. Moteff, "Critical Infrastructures: Background, Policy, and Implementation" Updated July 30, 2002, Report to Congress, Congressional Research Service (December 2001), http://www.fas.org/irp/crs/RL30153.pdf.

J.D. Moteff, Claudia Copeland, and John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical? (PDF) August 30, 2002, http://www.fas.org/irp/crs/RL31556.pdf.

National Research Council, Board on Infrastructure and the Constructed Environment, **Protecting People and Buildings from Terrorism: Technology Transfer for Blast-effects Mitigation**, National Academy of Sciences Press, 2001.

Naval War College, "Naval War College Year 2000 International Security Dimension Project," 1999, http://www.nwc.navy.mil/y2k/y2ksite.htm

Alan Paller, Director of Research, The SANS Institute, Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, Oversight Hearing on "Cyber-terrorism: Is the Nation's Critical Infrastructure Adequately Protected?" July 24, 2002.

Eric Pianin, Marc Kaufman, Lucy Shackelford, et al., "How Experts Grade Homeland Security," **The Washington Post** (September 10, 2002) A20 - A21.

Riptech, Inc., "White Paper on Understanding SCADA System Vulnerability," http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf, January 200l.

Michael Scardaville and Jack Spencer, "9/11 One Year Later: Progress and Promise," **Heritage Foundation Backgrounder** No. 1584, September 10, 2002.

John S.Tritak, Director, Critical Infrastructure Assurance Office, Bureau of Industry and Security, U.S. Department of Commerce, Statement before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, Oversight Hearing on "Cyber-terrorism: Is the Nation's Critical Infrastructure Adequately Protected?" July 24, 2002.

U.S. Department of Commerce, International Trade Administration, Trade Development, Office of Computers and Business Equipment, "The Year 2000 Problem and the Global Trading System," April 9, 1999.

Bruce F. Webster, **The Y2K Survival Guide: Getting to, Getting Through, and Getting Past the Year 2000 Problem.** Prentice Hall, Upper Saddle River, NJ, 1999.

Joseph M. Weiss, P.E., Executive Consultant, KEMA Consulting, "Control System Cyber Security - Maintaining the Reliability of the Critical Infrastructure," Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, Oversight Hearing on "Cyber-terrorism: Is the Nation's Critical Infrastructure Adequately Protected?" July 24, 2002.

Edward Yourdon, **Byte Wars: The Impact of September 11 on Information Technology**, Prentice Hall, Upper Saddle River, NJ, 2002.

Legislation, Congressional Documents, Public Laws, Executive Orders, and Presidential Directives

Executive Office of the President, The Status of Federal Critical Infrastructure Protection Activities, Report of the President of the United States, January 2001.

Executive Order 13231, **Federal Register**, Volume 86, No. 202, October 18, 2001, pp. 53063 - 53071.

Executive Order 2001-13228. Executive Order Establishing Office of Homeland Security and the Homeland Security Council, October 8, 2001.

Executive Order 2002-034. Homeland Security Council Executive Order Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security, March 21, 2002.

H.R. 3448, Public Health Security and Bioterrorism Response Act of 2002, To improve the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies. Became law on June 12, 2002 http://www.absa.org/pdf/H.R.%203448%20-%20Biosecurity%20summary.pdf.

National Homeland Security and Combating Terrorism Act of 2002, Report of the Committee on Governmental Affairs United Stated Senate together with Additional Views to accompany S. 2452 to Establish the Department of National Homeland Security and the National Office for Combating Terrorism, June 24, 2002, Report 107-175.

National Security Presidential Directive: Homeland Security Presidential Directive-1, Organization and Operation of the Homeland Security Council, October 29, 2001.

National Security Presidential Directive: Homeland Security Presidential Directive - 3: Establishing a Homeland Security Advisory System.

The National Security Strategy of the United States of America, September 17, 2002 http://www.whitehouse.gov/nsc/nss.html.

National Strategy for Combating Terrorism, February 14, 2003, http://www.whitehouse.gov/news/releases/2003/02/counter_terrorism/goals.pdf.

National Strategy for Homeland Security, Office of Homeland Security, Executive Office of the President, July 2002, www.whitehouse.gov/homeland/book/.

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, February 14, 2003, http://www.whitehouse.gov/pcipb/physical_strategy.pdf.

National Strategy to Combat Weapons of Mass Destruction, December 2002, www.whitehouse.gov/news/releases/ 2002/12/WMDStrategy.pdf.

National Strategy to Secure Cyberspace (Draft), The President's Critical Infrastructure Protection Board, September 2002 whitehouse.gov/PCIpb/cyberstrategy-draft.html.

The National Strategy to Secure Cyberspace, The President's Critical Infrastructure Protection Board, February 14, 2003, http://www.whitehouse.gov/pcipb/.

Presidential Decision Directive/NSC-63, Critical Infrastructure Protection, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

Public Law 107-56, U.S. Patriot Act
http://www.google.com/search?q=%22US+Patriot+Act%22+%2B+critical+infrastructure&hl=en&lr=&ie=UTF-8&oe=UTF-8&start=20&sa=N.

Senate Bill 5005, Congressional Record, 148:150-151, November 20, 2002. National Homeland Security and Combating Terrorism Act of 2002 signed into law November 25, 2002.

U.S. House of Representatives, Committee on Government Reform, November 19, 2002 Computer Security Report Card "prepared by Chairman Stephen Horn, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, based on agency reports required by the Government Information Security Reform Act of 2000." http://www.house.gov/reform/gefmir/hearings/2002hearings/1119_computer_security/computersecurityreportcard.doc.

.