

*Critical Infrastructure Protection R&D  
Interagency Working Group*

**REPORT ON THE FEDERAL AGENDA IN  
CRITICAL INFRASTRUCTURE PROTECTION  
RESEARCH AND DEVELOPMENT**

**RESEARCH VISION, OBJECTIVES, AND PROGRAMS**

**January 2001**



## Table of Contents

Executive Summary	iii
I. Foreword	1
II. Introduction and Background	3
III. Vision and Goal	6
IV. The Challenge and the Threat	8
V. Objectives	9
VI. Sector Summaries of Current Programs and R&D Shortfalls	11
• Information and Communications	12
• Banking and Finance	16
• Energy	18
• Transportation	20
• Vital Human Services	22
• Interdependencies	26
VII. Developing a Federal R&D Agenda	31
VIII. International Dimensions of CIP R&D	33
IX. Management Challenges and Related Issues	36
• Institute for Information Infrastructure Protection	36
• Addressing the Shortage of CIP R&D Personnel	37
• Other Management Challenges	40
X. Updating the Critical Infrastructure Protection R&D Agenda	43
XI. Observations	44
XII. Recommendations	48
<b>APPENDICES</b>	
A. Glossary of Acronyms and Terms	49
B. IWG Organization Chart	51
C. Roster of Agency Points of Contact in the R&D IWG	52
D. Policy and Procedures Statement on International Research and Development Cooperation in Critical Infrastructure Protection	53
E. White Paper on the Institute for Information Infrastructure Protection	56



## Executive Summary

This report summarizes the work of the Critical Infrastructure Protection R&D Interagency Working Group (IWG) over the period of March 1998 - November 2000. This working group, chartered jointly under the National Science and Technology Council's Committees on National Security and Technology and PDD-63, drew upon existing reports, analyses, and expertise resident within twenty federal departments and agencies. Readers should recognize that while the analyses and recommendations of this report represent the collective thoughts and opinions of the interagency working group, they have not been formally vetted through the respective agencies.

In response to tasking from the National Science and Technology Council's Committees on National Security and Technology, as well as from the Critical Infrastructure Coordination Group established under PDD-63, the report proposes a federal research and development (R&D) strategy, as one element of a broader federal response, to the challenge of critical infrastructure protection (CIP). The report provides a vision, a set of objectives to achieve that vision, a proposed federal R&D agenda to achieve those objectives, budget options, and sets forth a management process to keep the strategy current in the months and years to come.

The report highlights eight priority R&D issues:

- Establishment of an Institute for Information Infrastructure Protection
- The education and training of research personnel in CIP R&D
- Interdependency analyses
- Threat, vulnerability and risk assessment studies
- System protection and information assurance
- Reconstitution of damaged or compromised systems
- The security of automated infrastructure control systems
- Intrusion detection and monitoring

The IWG makes the following recommendations:

- Existing and planned CIP R&D activities need to be coordinated with other initiatives such as information technology and weapons of mass destruction prevention to preclude overlap and promote synergy among these initiatives.
- A proper balance between fiscal restraints and responsiveness to the threats to the nation's critical infrastructures calls for greater levels of funding in the future over current FY 2001 levels of CIP R&D.
- The new Administration should explore options for R&D management models embodying the flexibility and nimbleness needed to ensure that the CIP R&D process can keep pace with the revolutionary technology environment for critical infrastructure

protection in the years ahead. The Institute for Information Infrastructure Protection, which has been recommended by the President's Committee of Advisers on Science and Technology (PCAST), should be reconsidered for support.

- Senior officials of the new Administration should receive a briefing in the very near future from the Intelligence Community on the nature of the critical infrastructure threat to the U.S. and its allies.
- A program to strengthen university training and research in disciplines that support CIP R&D should be proposed in the FY2002 or FY2003 budget cycle.

## I. FOREWORD

In January 2000, the federal government published the National Plan for Information Infrastructure Protection, part of which addressed research and development (R&D) issues. Since that time, an aggressive and fruitful investigation of the need for solutions to Critical Infrastructure Protection (CIP) R&D issues has taken place under the auspices of the CIP R&D Interagency Working Group (IWG). This report summarizes the work and recommendations of the IWG from March 1998 to November 2000 and updates both the previous November 1998 report on this same topic and the R&D work in the 2000 National Plan. It describes R&D to protect the increasingly interconnected infrastructures that are critical both to the functioning and growth of the U.S. economy and to our ability to defend this country's national security interests.

This working group, chartered jointly under the National Science and Technology Council's Committee on National Security and Committee on Technology, and the Critical Infrastructure Coordination Group, drew upon existing reports, analyses, and expertise resident within twenty federal departments and agencies, as well as a variety of outside expertise available to the IWG. Readers should recognize that while the analyses and recommendations presented below represent the collective thoughts and opinions of the interagency working group, they have not been formally vetted through the respective agencies.

### Origins

In March 1998, the National Science and Technology Council set up a Critical Infrastructure Protection Research and Development Interagency Working Group (CIP R&D IWG) under the joint oversight of the Committee on National Security and the Committee on Technology. This CIP R&D IWG was established to develop and sustain a coherent roadmap on what technologies to develop that, if implemented within critical national infrastructure sectors, would reduce vulnerabilities and counter threats that could cause major damage to the security, economic vitality, and social well-being of the United States. This roadmap would address both physical and cyber threats, as well as new threats arising from the growing complexity of, and interdependencies among, our critical infrastructures. While the agenda presented in this report primarily addresses hostile threats, it recognizes that natural and non-hostile problems also pose important challenges to our national wellbeing, as the Year 2000 problem demonstrates.

In PDD-63, the President directed that within 180 days, a schedule for a National Infrastructure Assurance Plan be submitted to him from the CICG Principals Committee with milestones for accomplishing, *inter alia*,

*“Research and Development: Federally sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.”*

To implement this part of the directive, the CICG decided to utilize the CIP R&D IWG already in existence. As a result of PDD-63, the IWG's charter was expanded to develop a process of ongoing R&D planning and appraisal, as well as to provide appropriate R&D support to the CICG and the National Coordinator.

The IWG in this report reviews the work of the last two years and sets out an R&D agenda that looks primarily at both ongoing work and new initiatives for the period FY2002-2007, although the IWG was sensitive to the further outyear implications of the agenda. For the purposes of this agenda, a new initiative is defined as either a new program start, or a previously unplanned expansion of an existing program.

Research and development is a critical component of the federal government's efforts to address the critical infrastructure protection challenge. The explosive growth in new technology, particularly in the information infrastructure, requires constant efforts to stay abreast of the new technologies, and new vulnerabilities and threats they bring in their wake. R&D's importance can also be seen by the fact that it represents 33% of the overall \$1.47 billion in critical infrastructure protection funding requested for FY2001.

The position of the CIP R&D IWG in the science and technology structure of the executive branch is shown in the attachment at Appendix B.

## II. INTRODUCTION AND BACKGROUND

The economy and national security of the United States are increasingly dependent on a spectrum of critical infrastructures, which can be broadly grouped in the following five sectors:

- Banking and Finance
- Information and Communications
- Energy
- Transportation
- Vital Human Services

These sectors were drawn from the 1997 Marsh Commission report on Critical Infrastructure Protection, *Critical Foundations*. As that report did, the IWG merged Emergency Services, Government Services, and Water Supply Systems into the Vital Human Services category, and Electrical Power and Oil and Natural Gas Production and Storage into the Energy category. The IWG established subgroups that correspond to each of these sectors, as well as a separate subgroup to address interdependencies among these sectors, and also set up special subgroups to address outreach and budget issues.

The above five critical infrastructures are highly interdependent, both physically and in their greater reliance on the national information infrastructure. This trend has been accelerating in recent years with the explosive growth of information technology (IT) and shows no sign of abating. Potential threats to the normal functioning of these infrastructures are both natural (“Murphy’s Law and Mother Nature”) and man-made. Individual outages can be serious enough, but this growing degree of interconnectedness can make possible a whole new scale of synergistic, nonlinear consequences.

Despite the fact that the private sector owns and operates the vast majority of the nation’s critical infrastructures, it does not invest heavily in long-term, high-risk security-related technologies, especially if they are too easily adopted by competitors, or otherwise unlikely to generate returns that investors can capture. Such technologies are “public goods” – their development and adoption would benefit the nation as a whole, but they would not benefit any single firm enough for that firm to shoulder their investment cost. Therefore, government becomes the only realistic underwriter to ensure that these technologies are developed – a need that extends beyond funding, since these technologies will serve no useful purpose if they are not adopted and deployed. Just as our government defends the nation’s airways and sea lines of communications, so too should it play a leadership role in defending the nation’s critical infrastructures. At the same time, the private sector has a key partnership role to play, given its major ownership share of the infrastructures, its business interests, and the expertise that it possesses.

The obligation to ensure that technologies to strengthen the critical infrastructures are placed into operational practice differentiates infrastructure protection R&D from other areas where government invests in development of industrially relevant R&D. Existing government technology programs do an excellent job of developing and implementing new technology in those areas where industry is eager to participate, and where the risk of failure affects only the original investment. In infrastructure protection, however, failure to adopt

new security technologies means that vulnerabilities in the nation's critical infrastructures will persist. To eliminate these vulnerabilities, the government cannot afford to deal only with those firms that are highly motivated to collaborate – it should also engage, for example, those private sector owners, operators, providers, and users of critical infrastructure products and services that may not know of, or may not be particularly motivated to adopt, technologies developed through government investment. To enlist the participation of these more reluctant partners, government should adopt innovative business incentives that provide the private sector with a greater degree of visibility, participation, and “buy-in” than is associated with many traditional government agency programs and procedures.

While the U.S. economy has long depended on several critical infrastructures, the coupling among them has historically been rather loose. Thus there has understandably been little need for concern about the possibility of cascading effects spreading to all the infrastructures based on an important failure in just one. The major 1965 failure of the electric power grid in the northeast United States had little lasting impact on the other infrastructures despite important, though non-cascading, short-term effects on other infrastructures. Yet important technological, economic, and regulatory changes have dramatically altered the relationships among infrastructures.

As the U.S. economy becomes ever more tightly connected through telecommunications, electronic signaling systems, power generation, information lines, financial connections, transportation modes, and other connections involving critical infrastructures, possible disruptions have far greater potential than ever before to ripple throughout the economy. This unprecedented degree of infrastructure interconnectedness will result in an increasingly enmeshed U.S. economy. In this situation, outage “ripples” in one infrastructure could become cascades of economic malfunction, as individual outages lead to outages in other infrastructures, which in turn intensify the first outages in a firestorm-type of phenomenon. This negative synergy could create havoc in an economy that did not have mechanisms in place to quell these effects.

One recent, and fortunately modest, example of this was the May 1998 failure of the Galaxy 4 telecommunications satellite, which led to an outage of 90% of pagers nationwide. However, the effects of the loss of this single satellite were not confined to the information and communications infrastructure – hundreds of thousands were unable to conduct routine financial transactions such as gasoline and other credit card purchases, using ATM's, etc., and there is evidence that hospitals and other vital services were affected as doctors and emergency workers could not receive pages. In this case, a point failure in the information and communications infrastructure created disturbances in the financial and vital human services infrastructures, among others. Were a 1965-type power failure to happen today, the effects of that outage would be far greater than they were 35 years ago.

At the same time that the information technology revolution has led to substantially more interconnected infrastructures with generally greater centralized control, the advent of “just-in-time” business practices has reduced margins for error in infrastructures. In addition, the trend toward deregulation and growth of competition in key infrastructures has understandably eroded the willingness of infrastructure participants to pay for spare

infrastructure capacity that could serve a useful “shock absorber” role in cushioning key infrastructures from failures elsewhere in the economy. Furthermore, the growth of mergers among infrastructure providers has led to further pressures to reduce spare infrastructure capacity as managers have sought to wring costly “excess” costs out of merged companies.

In addition, the rapid growth of IT and the Internet have also enabled skilled individuals and small groups of people to have impact all across the globe without leaving their homes. The “Iloveyou” and Melissa viruses wrought substantial financial and other damage as the result of individual actions, yet highly trained units in countries that are hostile to the U.S. could potentially inflict far more damage without ever leaving their homelands. This has particularly troubling implications for the security of our economy and our military forces. The Defense Department has made it a key priority to establish a Global Information Grid linking its forces and decision-makers far more tightly than ever before, thereby making sophisticated threats to information networks far more dangerous to us from a national security perspective than ever before.

While in many cases better management over networks and infrastructures, including implementation of existing security protocols, could have averted these problems, they nonetheless illustrate the new dimension of challenges that our ever-more-interconnected world presents to us. In addition, policymakers must deal with the reality that lapses in security and failure to fully implement proper configuration management practices will repeatedly occur, given the realities of human nature.

Any one of these trends would be a cause for uneasiness. The convergence of all five at the same time has no precedent in American economic history. Concern over these converging trends led the Defense Science Board in 1996 to decry this emerging situation as a “tunnel of vulnerability previously unrealized.” While important steps have been taken on individual infrastructures since 1998, the issue of interdependent and cascading effects among infrastructures has received much less attention. This situation calls for concerted private sector and federal efforts to build “shock absorbers and circuit breakers” of both a physical and policy nature into our economy to protect against major infrastructure breakdown, yet little is known about what these effects are or how they propagate.

### III. VISION AND GOAL

The vision to which the CIP R&D IWG has directed its efforts is that of a United States whose critical infrastructures are trustworthy and resilient. That is, they are able to provide the level of performance expected under a variety of conditions. To achieve this, they should have the ability to absorb intentional or unintentional outages with minimal impact on their ability to deliver needed levels of service, both directly to consumers and to the other infrastructures that depend upon it. This would be a daunting challenge even if the technology of these critical infrastructures were static. As we know, the technology embedded throughout the U.S. economy is undergoing a continuous and profound transformation. Accordingly, the IWG has sought to support the development of technologies that will counter threats and reduce vulnerabilities in those areas having potential for causing significant national security, economic, and/or social impacts.<sup>1</sup>

Such a robust set of critical infrastructures would have assured continuity and viability and be protected from hostile acts and natural outages that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety.
- state and local governments to maintain order and to deliver minimum essential public services.
- the private sector to ensure the orderly functioning of the economy and the delivery of essential information and communications, energy, financial, transportation, and other services.

As part of the vision, any interruptions or manipulations of these critical functions would be brief, predictable in impact, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

To help realize this vision, the CIP R&D IWG has as its goal to identify and support a vigorous and effective program of federal R&D in critical infrastructure protection. This program, along with private sector efforts, should enhance the security of our nation's critical infrastructures by rapidly identifying, developing, and facilitating the fielding of technological solutions and management tools and techniques to address existing and emerging infrastructure threats and vulnerabilities. The process to achieve this should be characterized by:

---

<sup>1</sup>Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*, Washington D.C., July 1998, p.xiii.

- an awareness of the state of new technological developments as they become embedded in infrastructures and the new avenues they present for hostile and non-hostile disruption of these architectures;
- an ability to produce an affordable agenda of R&D programs in critical infrastructure protection in time to be useful to those who make resource allocation and infrastructure protection planning decisions in government and the private sector;
- a functioning, effective interaction with the private sector, academia, and other countries so that R&D overlap is minimized and programs are pursued that best meet the needs of the private sector and government;
- an innovative management structure that is sufficiently flexible and responsive to a rapidly changing infrastructure environment in terms of technology and threats.

## IV. THE CHALLENGE AND THE THREAT

Technical specialists and policy makers are increasingly concerned that as our national infrastructures become more tightly coupled, disruptions will have much greater potential to reverberate throughout the economy. The spare capacity in our infrastructures, which was generally sufficient to shield us from major outages in the past, may no longer be enough to deal with major disruptions. The level of spare capacity in our economy has in many cases declined as well, thanks to the economic restructuring and forces mentioned earlier. We only have the vaguest idea of how hostile or non-hostile infrastructure disruptions could propagate in our tightly coupled economy.

As the attack on the USS Cole, the 1993 World Trade Center bombing, and recent hostile hacker attacks on information networks (Moonlight Maze, Solar Sunrise, etc.) have shown, asymmetric warfare against the U.S.—striking our vulnerabilities rather than our superior military forces—will likely grow in the future, as well as non-hostile disruptions. Threats of infrastructure attacks, especially involving information warfare techniques, have grown over the last few years and threaten to become a common feature of conflict between countries, and not just involving the United States. The China-Taiwan confrontation, which has seen threats and counter-threats of cyber attacks, and the escalating cyber-skirmishing that has occurred between Palestinian and Israeli hackers are just two examples of this.

Increasing numbers of countries and sub-national groups are developing the ability to attack lightly or unprotected sectors of the U.S. economy. Failure to understand how such attacks could propagate throughout our economy leaves economic and military planners unprepared to deal with infrastructure failures during military contingencies. In the highly interconnected economy of the future, hostile—and non-hostile—disruptions will have much greater potential to reverberate throughout the U.S. economy unless we take steps to build in the “shock absorbers and circuit breakers” to prevent it.

Additional classified information on the nature of the cyber and physical threat to our critical infrastructures is available from the Central Intelligence Agency. *The CIA briefed the CIP R&D IWG on this threat in 1998, 1999, and 2000. It is essential that decision-makers on this issue receive such a briefing in 2001 and the years to come.*

Generally, the private sector funds near-term R&D to develop tools to address infrastructure outages, but the federal government does more fundamental R&D. Federal funding for all critical infrastructure protection R&D has increased only modestly over the last few years and is now about \$600 million overall. As a proportion of the exploding level of IT investments in our economy, this R&D funding has seriously declined. Specific R&D areas that need to be addressed are presented below.

Beyond R&D funding, the country needs greater awareness of the critical infrastructure protection issue, especially of the interdependencies among these infrastructures and the catalytic effect this can have on our security. As Y2K taught us, it is best to take precautionary measures and plan ahead for a challenge like this.

## V. OBJECTIVES

The overall objectives of the federal program in critical infrastructure protection R&D are to promote and coordinate research to reduce vulnerabilities in our nation's critical infrastructure, and to promote the research and development of technologies that will detect, contain, and mitigate attacks against or other failures in these infrastructures. The CIP R&D IWG has three sets of more specific objectives, one each for the short-, medium-, and long-term.

The IWG's *long-term* objective is to achieve the goal of maintaining and supporting a vigorous and effective program of federal R&D in critical infrastructure protection that rapidly identifies, develops, and facilitates the fielding of technologies and management tools that provide protection against existing and emerging infrastructure threats and vulnerabilities.

In the *medium-term*, the IWG's objectives are to:

- *Sustain the process that has evolved since 1998 to develop and maintain an agenda for federal critical infrastructure protection R&D.* This agenda should be comprehensive and include information on ongoing federal programs, near- and long-term research plans, budget information, and proposed R&D policy.
- *Foster conditions for the development of a close partnership with the private sector, academia, and international community.* Given the volume of CIP R&D performed by and the expertise resident in industry, academia, and the international community, the federal program should be developed in close conjunction and partnership with these communities.
- *Facilitate the smooth and timely transfer of technology among government agencies and between them and the private sector.* This objective is closely aligned with the previous one. Technology developed in government laboratories should be rapidly transferred to the private sector, particularly if the federal government concentrates primarily on research and the private sector on development.

In the *short term*, the IWG annually develops and coordinates the federal government's critical infrastructure protection R&D agenda in accordance with guidance from PDD-63. The ideal agenda generally does not reflect budgetary constraints. While the IWG seeks to prioritize the R&D, the ultimate decisions on what level of CIP R&D to include in the federal budget rest will be made as the President's budget request is assembled each year. In developing the federal CIP R&D agenda, the IWG should:

- Share with other members of the IWG the program, technical, and budgetary information on the CIP R&D programs that each agency has under way or planned, which in its entirety constitutes the CIP R&D baseline.

- Monitor and coordinate ongoing and planned federal CIP R&D. The IWG provides a forum to identify and resolve issues in recommending a national R&D agenda, policy, and programs.
- Develop an ideal CIP R&D agenda that would allow the IWG to meet its long-term objective of a robust set of national critical infrastructures.
- Identify the gaps and shortfalls in CIP R&D by comparing the ideal R&D agenda with the R&D baseline, taking into account what is known about private sector R&D.
- Prioritize the unmet R&D programs needed to fill the gaps and shortfalls and provide this information as requested to the NSTC, CICG, etc.
- Maintain a dialogue with the private sector and academia on infrastructure challenges, R&D needs, and R&D resources.
- Maintain a dialogue with the intelligence community and private sector on infrastructure threats.

In addition, the IWG responds to the needs of the NSC, OSTP, National Coordinator, CICG, and infrastructure stakeholders as appropriate.

## VI. SECTOR SUMMARIES OF CURRENT PROGRAMS AND R&D SHORTFALLS

### Agency Summaries

Some of the critical infrastructure sectors fit neatly into individual departments, though even here there is overlap. For example, the energy infrastructure is directly associated with the Department of Energy, and Transportation with the Department of Transportation. Yet information and communications R&D is performed in several departments, most notably the Department of Defense, though Commerce, the National Science Foundation, and even Energy are also involved. And there is no “Department of Interdependencies,” so this critical area has no obvious agency home, though Energy and Defense are gaining in their recognition of how this issue affects their mission, as is Treasury. Funding by department for FY2000 and FY2001\* is shown in the table below.

### **Federal CIP and Related R&D FY2000-01**

DEPARTMENT/AGENCY	FY00	FY01(*)
Agriculture	0.0	9.0
Commerce	9.5	63.3
National Security	418.5	463.48
Energy	3.03	14.8
Environmental Protection Agency	0.0	2.0
Health and Human Services	0.0	2.0
Interior	4.0	0.0
Justice	3.4	0.0
NASA	2.6	0.0
National Science Foundation	26.02	32.98
Transportation	0.0	10.4
Treasury	3.9	8.0
Veterans	0.45	0.30
<b>TOTAL</b>	<b>471.4</b>	<b>606.26</b>

### Sector Summaries

Summaries of the sector activities and R&D recommendations are presented on the following pages.

---

\* FY2001 Budget, as submitted. Details of final FY2001 Congressional action unavailable.

# INFORMATION AND COMMUNICATIONS

## Introduction

The information and communications (I&C) infrastructure sector of the nation's critical infrastructures generates more revenue than most nations produce. Far more than any other nation, the U.S. has been able to utilize the potential of the new technologies to reshape its governmental and commercial processes. The United States has generally led the world into the information age, and in so doing has become critically dependent on its technologies to conduct national and international commerce, governmental functions, and military operations. These technologies enable the U.S. to keep its economy competitive, its government efficient, and its people secure. Thus, as the Director of OSTP, Neal Lane, testified in March 2000 before a subcommittee hearing of the House Armed Services Committee, ensuring the robust and reliable operation of our critical infrastructures "... is truly a national challenge - one that goes way beyond the traditional bounds of national security as our economic security, competitiveness, and our way of life rest upon the continuous and assured availability of the services provided by our infrastructures..."<sup>2</sup>

As is true for most critical infrastructures, developing the ability to protect the I&C infrastructure is neither an entirely public nor an entirely private responsibility. Infrastructure risks are common to government, business, and citizen alike and create a zone of shared responsibility and cooperation among industry, government, and academia. Reducing those risks requires coordinated effort within and between the private and public sectors. If we are to retain and build upon the competitive edge that information technology has given us, we need to work together on CIP R&D and in other pursuits to substantially improve the trustworthiness of our information systems and networks.

## Goals

The goal of the I&C Subgroup of the CIP R&D IWG is to coordinate federal I&C infrastructure R&D efforts. Specifically, the Subgroup supports the development of technologies that will counter threats and reduce vulnerabilities in those areas having potential for causing significant national security, economic, and/or social impacts.<sup>3</sup> Recognizing that it is impossible in the near-term to assure fully the continuity and viability of the I&C critical infrastructure, the I&C Subgroup's approach is to continuously improve the protection of the many components comprising the I&C infrastructure from identified security threats, vulnerabilities, and shortcomings. Accordingly, the Subgroup seeks to:

---

<sup>2</sup>From a statement of Dr Neal Lane, Director of the White House Office of Science and Technology Policy, during his testimony in which he addressed critical infrastructure protection matters in a joint meeting of the Readiness Subcommittee and the Research and Development Subcommittee of the U.S. House of Representatives Committee on Armed Services, March 8, 2000.

<sup>3</sup>Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*, Washington D.C., July 1998, p.xiii.

- Ensure that the recommended federal government I&C CIP R&D agenda is responsive to the needs of the NSC; National Coordinator for Security, Critical Infrastructure and Counter Terrorism; CICG; IWG; and infrastructure stakeholders as appropriate.
- Develop and coordinate the federal government I&C CIP R&D agenda in accordance with guidance from PDD-63 such that the agenda is comprehensive and includes information on ongoing federal I&C CIP R&D programs, near- and long-term research plans, budget information, recommended funding priorities, and proposed R&D policy, as applicable.
- Monitor and coordinate ongoing and planned federal I&C CIP R&D by providing a forum to identify and resolve issues in recommending a national I&C CIP R&D agenda, policy, and program.
- Foster conditions for the development of a close partnership with the private sector, academia, and the international community by developing the federal program in close conjunction and partnership with these communities. This is especially important given the volume of I&C CIP R&D performed by, and the expertise resident in, these communities. We need to maintain a functioning, effective, 2-way interaction among the Federal Government departments and agencies (to include the Critical Infrastructure Assurance Office, Sector Liaison Offices, etc.) as well as with the private sector (to include Sector Coordinators), academia, and other countries, which will allow us to gain synergy in critical infrastructure protection efforts. We will also minimize I&C CIP R&D overlap with other CIP R&D sectors as well as to counter-terrorism, Weapons of Mass Destruction Prevention, and other federal R&D. We will pursue federal I&C CIP R&D programs that best meet the needs of the private sector and government.
- Closely aligned with the previous goal, facilitate the smooth and timely transfer of technology among government agencies and between them and the private sector; technology developed in government laboratories should be rapidly transferred to the private sector, particularly if the Federal Government concentrates primarily on research and the private sector on development.
- Maintain an awareness among Subgroup members of the current threat environment as well as the new technological developments being incorporated into the I&C infrastructure and the new vulnerabilities they present relative to hostile/non-hostile disruption of this critical infrastructure.
- Support the CIP R&D IWG and its process in being an innovative coordination structure that is sufficiently flexible and responsive to a rapidly changing infrastructure environment in terms of technology and threats. Coordinate closely with the Interdependencies Subgroup concerning R&D programs applicable to: (1) protection of both the I&C infrastructure and other critical infrastructures, (2) interdependencies among the I&C and other critical infrastructures, and (3) overlapping I&C CIP,

counterterrorism, WMD, or other threats;

- Develop and coordinate an overall federal government I&C CIP R&D program agenda that takes into account R&D applicable to protection of the I&C infrastructure even when it is primarily conducted in response to a counter-terrorism, WMD, or other threat or concern, and that supports the following four primary thrusts, each of which draws on the resources of multiple agencies and covers a broad spectrum of cyber security issues:
  - (1) *Threat/Vulnerability/Risk Assessments* - focusing on threat, vulnerability, and risk assessments of the I&C critical infrastructure to include modeling and simulation programs, metrics, and testbeds;
  - (2) *System Protection* - focusing on cyber protection of individual systems, to include programs such as encryption, public key infrastructures, network security products, reliability and security of computing systems, robust I&C control systems, and secure supervisory control and data acquisition (SCADA) systems;
  - (3) *Intrusion Monitoring and Response* - focusing on technologies to detect and provide immediate responses to intrusions or infrastructure attacks to include such programs as network intrusion detection, information assurance technologies, mobile code and agents, network alarm systems, forensic tools for electronic media, and network defensive technologies; and
  - (4) *Recovery and Reconstitution* - focusing on those technologies required to reconstitute and restore the I&C critical infrastructure in the aftermath of disruptions to include such programs as risk management studies and tools, system survivability technologies, and consequence analysis tools and supporting technologies.

## Objectives

The I&C Subgroup's objectives are intended to achieve the foregoing vision and goals. They are based on the direction from PDD-63, the *National Plan for Information Systems Protection* (Version 1.0), and guidance from the Committees on National Security and Technology as well as the Critical Infrastructure Coordination Group (CICG), and the IWG in turn. Those objectives are to continue to develop, coordinate, and annually publish an I&C Subgroup:

- Statement of Vision/Goals/Objectives (so that all who are interested in making the vision a reality will share a common frame of reference).
- Assessment of Vulnerabilities/Shortcomings of the I&C Infrastructure (so that Federal Government I&C CIP R&D programs may be targeted, coordinated, prioritized, and proposed to address the identified vulnerabilities/shortfalls).
- Summary of Federal Government ongoing and completed I&C CIP R&D Programs (that are tied to identified vulnerabilities and/or shortcomings in critical I&C infrastructure).

- Summary of Gaps and Shortfalls I&C CIP R&D Programs (those proposed Federal Government I&C CIP R&D programs considered necessary to address the voids in federal R&D and thereby correct the identified vulnerabilities and shortcomings relative to the I&C critical infrastructure).
- Table of Federal Government I&C CIP R&D Programs Versus Vulnerabilities/Shortcomings that reflects: (1) specific identified vulnerabilities/shortcomings of the I&C critical infrastructure, (2) the specific, ongoing federal programs addressing each of the specific identified vulnerabilities and shortcomings, (3) the new initiative federal programs also needed to address the identified gaps and shortfalls in R&D that are not addressed fully by the ongoing programs, and (4) the expected products (outcomes) of each program.
- Summary of Federal Government I&C CIP R&D Program Priorities that reflects a general prioritization scheme for use by those who make resource allocation and critical infrastructure protection planning decisions in government, academia, and the private sector. This summary will reflect a general assessment of the most important I&C CIP R&D needs and will reflect program priorities within agencies; however, it will not be a rank-ordered, prioritization of all Federal Government I&C CIP R&D programs based on an overall interagency, program-by-program review.

### Major Efforts Underway

For FY 2001, nine federal departments requested funds in the President's budget submitted to Congress for 85 ongoing I&C CIP R&D programs. Some of these programs, however, are funded out of other programs and therefore do not appear as separate budget line items. The research areas or topics these programs address run the gamut from public key infrastructure and Internet security to mobile agents and advanced authentication systems. As part of the strategic oversight of these programs, the CIP R&D IWG has worked with other interagency, government/industry, and industry groups in sponsoring several government/private sector workshops which have greatly facilitated coordinating both ongoing programs and new initiatives planned for FY 2002 and beyond.

Many of these programs are cooperative endeavors or joint efforts among different departments, and a few are joint efforts between Government and academia. The Department of Defense's "Critical Infrastructure Protection and High Confidence, Adaptable Software University Research Initiative" is an example of expanded research opportunities across a range of selected topics that are deemed crucial to our CIP needs. A second DoD Broad Area Announcement was issued for the creation of a CIP and Information Assurance (IA) academic fellows program to expand the opportunities for scientists and researchers in related fields to enter into the arena of CIP/IA R&D. Indeed, DoD plays a major role in addressing CIP issues across the full spectrum of R&D efforts. Active CIP R&D programs are present throughout DoD, and they continue to receive strong congressional support.

## Major Challenges in the Information and Communications Infrastructure

The information and communications (I&C) Subgroup identified gaps and shortfalls after mapping the currently funded R&D against identified vulnerabilities and shortcomings in the U.S. I&C infrastructure. This year, Subgroup members compared the baseline of ongoing I&C CIP R&D programs against the identified vulnerabilities and shortcomings in the I&C infrastructure. They coordinated extensively to ensure that each of the planned programs was indeed directly addressing one or more of the identified vulnerabilities and shortcomings relative to the I&C infrastructure. They previously identified the R&D gaps and shortfalls relative to the identified vulnerabilities and shortcomings that the ongoing programs do not address. Those gaps and shortfalls fall into the four primary thrust areas previously listed under the I&C goals.

### Conclusion

In summary, it is vitally important to recognize that the overall effort to accomplish the R&D necessary to address all of the identified gaps and shortfalls in federal I&C infrastructure R&D is a cooperative effort. Many programs are complementary, while others are joint efforts. Accordingly, funding disapproval for a program in one department ripples across other departments and the programs involved in a very negative fashion. The end result is that the effectiveness in developing new technology applications to address the identified vulnerabilities to the nation's I&C critical infrastructure is compromised.

## **BANKING AND FINANCE**

While the Banking & Finance Sector Critical Infrastructure has some unique elements, it primarily consists of important subsets of the other infrastructures, especially the Information and Communications infrastructure. While there are some vulnerabilities and threats unique to the Banking & Finance Sector, the greatest part of the sector's risk is inherited from the underlying supporting infrastructure.

Another factor in coordinating R&D in this sector is that there has been little R&D of any kind done in this community. The only work that fits a traditional definition of R&D would be the development of new derivatives and financial forecasting tools. Consequently, there is no tradition of R&D being done in this area, in addition to the present lack of R&D managers to oversee the required work.

To address the new and expanding threats from foreign nation states, criminal enterprises and terrorists, the community has sponsored a number of initiatives with the support of the Treasury Department. In addition to the Information Sharing and Vulnerability Assessment Center, there is a Research and Development working group under Mr. Charles Blauner of J.P. Morgan & Co. This working group has identified what research is being done within the community and vetted the efforts underway within the government

and Information and Communications Sector. It also supports the protection of the Banking & Finance Sector Critical Infrastructure.

The major focus of the Fiscal Year 2001 program is a modeling effort to identify the vulnerabilities in the Banking & Finance Sector Critical Infrastructure. This builds on work of the National Coordinating Center for Telecommunications under the NCS, which has completed an extensive model of the United States backbone communications network. This object-oriented model is aimed at understanding the properties, vulnerabilities and required remediation for our national communications infrastructure.

As mentioned before, almost all banking and financial services ride over some portion of the communications infrastructure. This R&D effort is examining essential services such as funds transfer, clearing houses, stock markets, refunding, etc. in order to identify the inherited vulnerabilities from the communications infrastructure and best remediation strategies. For example, we may know that there is an existing or pending attack against a certain type of switch. Examination of the model would show where the switches are located and which essential financial services depend on them. Further examination would also show the extent of the impact if the switches were compromised and what alternatives are available to address the loss of the switch. As the tool develops a better understanding of the financial processes, the model will also be able to identify malicious intervention or criminal activity. While this level of sophistication will take time to develop, the simple mapping of financial transaction and funds flows in the communications model should reap substantial benefits:

- identification of potential vulnerabilities;
- the testing of remediation alternatives to find the best option;
- a tool for executive crisis management training and exercises; and
- during an actual crisis or information warfare attack, a means to identify the extent of impact and to evaluate responses in real time.

This effort will also serve as a model technology for identifying infrastructure interdependencies with other sectors.

The secondary focus of the Banking and Finance R&D program is on developing the forensic tools that the U.S. Secret Service and other law enforcement agencies need to combat electronic crimes and attacks on our Banking & Finance Infrastructure. This work is being done in coordination with efforts at the Justice Department but focus on the specific nature of electronic financial crimes.

The total budget request in Fiscal Year 2001 for this program was \$4 million, which will only provide “seed money” for these research efforts. The task of examining the vulnerabilities and interdependencies of the entire Banking and Finance Sector will require resources that far exceed this initial investment in developing modeling tools. Once we have the resources and are able to develop the modeling tools, then we can start R&D efforts to develop remediation steps for the vulnerabilities that the modeling efforts will identify.

# ENERGY

## Introduction

Our nation's energy infrastructure — composed of increasingly interdependent industries that produce and distribute electric power, oil, and natural gas — is undergoing rapid and dramatic changes. Advances in information technology, an increased reliance on electronic commerce, restructuring and deregulation initiatives, and other market forces are motivating much of these changes. The purpose of the Energy subgroup is to develop a research and development (R&D) program agenda that will address a wide range of needs for protecting this critical energy infrastructure. Applicable R&D encompasses both the physical and cyber components of the electric power, oil, and gas infrastructures, the interdependencies among those components, and the interdependencies with the other critical national infrastructures. The energy R&D program is aimed at developing cost-effective technologies and capabilities (e.g., databases, methodologies, and tools) that can be used to achieve several goals:

- Increase our understanding of physical and cyber disruptions (natural, accidental, deliberate) to the energy infrastructure, especially those that could result in cascading or widespread regional outages.
- Develop energy infrastructure assurance “best practices” through vulnerability and risk assessments.
- Protect against, mitigate the impacts of, and improve the ability to recover from disruptive incidents within the energy infrastructure.

## Major Research Efforts Under Way

The R&D agenda consists of two primary thrust areas:

- Analysis and Risk Management
- Protection and Mitigation Technologies

Specific topical areas include:

- *Infrastructure Interdependencies.* Development of methodologies and tools for characterizing and analyzing interdependencies among the energy infrastructures and with other critical infrastructures. This capability will help DOE and others within the Energy Sector identify critical system nodes and assess the technical, economic, and national security implications of energy technology and policy decisions designed to ensure the security of our nation's interdependent energy systems.
- *Vulnerability Assessment.* Focus on collaboration with the Energy Sector to conduct physical and cyber vulnerability assessments that identify infrastructure vulnerabilities,

raise awareness about these vulnerabilities, and enable the development of guidelines and “best practices” for industry to use in limiting vulnerabilities.

- *Scale and Complexity Analysis.* Research on the fundamental operational characteristics of large-scale, complex, nonlinear energy infrastructures. This program will develop technologies and capabilities that focus on stability, countermeasures, reduction of complexity, the effects of uncertainty, and behavior.
- *Consequence Analysis and Management.* Development of data, methodologies, and tools for evaluating the public health and safety, national security, and economic consequences of disruptions to energy infrastructures and the processes needed to assist in restoration and reconstitution following such disruptions.
- *Risk Management.* Development of risk management methodologies and tools to assist decision makers in quantifying system risks and in planning and implementing critical infrastructure protection strategies.
- *Policy Effects and Institutional Barriers.* Examination of the barriers between government and industry stakeholders in sharing Critical Infrastructure Protection-related information (e.g., threat and vulnerability information) and identification and implementation of solutions to barriers that may inhibit the ability to protect U.S. critical infrastructures.
- *Real-time Control Mechanism Technologies.* Identification of vulnerabilities inherent in real-time energy control systems and development of technologies to protect against disruption or unauthorized control of, or intrusion into, these systems.
- *Integrated Multi-sensor and Warning Technologies.* Improvement of existing integrated systems and/or development of new ones to warn of attacks and impending failures at critical nodes. Focus on anomaly detection and failure warning technologies.

### Major Challenges in the Energy Infrastructure

The R&D areas that DOE has selected are structured to complement and reinforce each other and related efforts. Capitalizing on the links and synergies across the initiatives to meet requirements is a major technical and programmatic challenge. Additional challenges in the energy sector which complicate the R&D picture include:

- Inadequate information to determine susceptibility to disruption of the energy infrastructure
- Lack of a coordinated process to collect and distribute threat information
- Inadequate response and recovery procedures and technology
- Interdependence of energy infrastructure and other infrastructures
- Increasing system interconnectedness and complexity of the energy system
- Increasing reliance on real-time system control

- Gaps in physical protection for energy infrastructure facilities
- Limited cyber security for SCADA systems
- Inadequate protection of energy-related information
- Reliance on unique, hard to procure equipment and materials
- Susceptibility to cascading failures
- Reliance on rapid access to accurate information

## Conclusion

Coordination and partnerships among agencies and the private sector are of paramount importance. Identifying and developing mechanisms to transfer the technologies, capabilities and “best practices” developed through this program to industry and public organizations at the federal, state, and local levels are key to the success of the program and to protection of our nation’s critical infrastructure.

## **TRANSPORTATION**

### Introduction

The Transportation Subgroup of the Critical Infrastructure Protection R&D Interagency Working Group (CIP R&D IWG) includes representatives from a number of DOT offices as well as several federal agencies. Incorporating relevant projects and proposals from these organizations, the subgroup formulated the Interagency Transportation Infrastructure Assurance (TIA) Research and Development (R&D) Plan. This plan provides a coordinated federal government response to multiple mandates: the 1997 Marsh Commission on Critical Infrastructure Protection, White House Commission on Aviation Safety and Security (1997), the 1999 DOT Surface Transportation Vulnerability Assessment, the 1999 National Research Council report, “Improving Surface Transportation Security: A Research and Development Strategy,” and related Presidential Decision Directives (e.g., PDD-62, PDD-63, PDD-67). These activities and initiatives are essential to protect the nation’s transportation infrastructure, operators, and users against future acts of terrorism and crime and will enable the transportation system to adapt rapidly to natural or intentional disruptions. Critical transportation infrastructure elements include: aviation, space transportation, highways, mass transit, pipelines, rail, waterborne shipping, intermodal connections, and interfaces with other transportation-dependent infrastructures, such as energy and telecommunications.

The Interagency TIA R&D Plan represents a comprehensive approach to assessing threats to the security of the nation’s transportation system and to preparing R&D projects that provide integrated security solutions (e.g., technologies, procedures) tailored to these threats. It addresses the:

- Physical security of transportation modes and intermodal connections (e.g., roads, railroad lines, bridges, tunnels, terminals, locks and dams, piers, etc.);

- Security of vital communications, navigation and information systems and networks (e.g., Global Positioning System);
- Susceptibility of transportation operators and users to weapons of mass destruction (WMD); and
- Development and dissemination of information about system threats, vulnerabilities and best practices to transportation system developers, operators and users.

#### Major Efforts Under Way:

Traditionally, aviation has conducted the bulk of transportation CIP R&D through the Federal Aviation Administration. This tradition continues today as aviation comprises 88 percent of ongoing transportation CIP R&D in the area of aviation security in FY 2000. Other current major transportation CIP R&D efforts include analysis of Global Positioning System (GPS) vulnerabilities; intelligence and security risk assessments, TIA training and awareness, information dissemination; chemical/biological agent detection; and research on operational methods for improving the performance of transportation systems.

Additional TIA R&D activities requested in the FY 2001 budget submission to Congress include aviation information systems security, intermodal terminal security at major transportation nodes, and human factors analysis on the transportation security system. However, Congress denied funding for the Information Systems Security program in its consideration of the FY2001 budget request.

#### Major Challenges to the Transportation Sector:

Responsibility for assuring the safety and security of the nation's transportation infrastructure and its continued operations is scattered among thousands of private companies and agencies at every level of government. This decentralized approach to transportation has resulted in transportation system security gaps, especially in areas where both responsibility and resources are divided or uncertain.

A second major challenge is managing the control of information on vulnerability assessments. The crux of the challenge is to restrict dissemination of sensitive information to malefactors while allowing private companies to obtain the vulnerability information they need. Additionally, many vulnerability assessments could involve the gathering of sensitive or proprietary information which, if provided to competitors, would be damaging to the participating private company. This information needs to be protected while still allowing it to be used to protect the infrastructure. Furthermore, many private companies fear that vulnerability assessments of their operations could open the door to tort liability suits. Although these questions have yet to be fully resolved, efforts are underway to address these concerns.

Specific analysis of gaps and shortfalls in this sector are in the final stages of review and are unavailable at this time.

## Conclusion

Aviation has a strong history of robust R&D efforts on transportation infrastructure assurance and security, a tradition that will continue. Given surface transportation's importance and vulnerability, as highlighted by several recent studies and high-profile incidents, it is essential to improve surface transportation security, given the emerging 21<sup>st</sup> Century threats of cyber terrorism and chemical/biological weapons. The interagency development of the Transportation Infrastructure Assurance (TIA) R&D Plan addresses and coordinates these challenging tasks of protecting our nation's transportation infrastructure from terrorist threats. The Plan's next stage will include heightened involvement of private industry in developing and honing transportation infrastructure assurance R&D.

## **Vital Human Services**

### Introduction

The Vital Human Services (VHS) sector includes three of the critical infrastructures named in Executive Order 13010:

- water supply
- emergency services
- government services, including defense.

These three VHS infrastructures differ from other critical infrastructures in that, with the exception of defense, they are focused largely at the state and local level and are largely governmental responsibilities. In spite of these differences, the VHS infrastructures face similar problems and vulnerabilities in communities across the country. The R&D efforts underway in the water supply and emergency services sectors are highlighted below. National Security is treated in a separate section immediately following.

### Background

The water supply sector CIP effort is primarily focused on the 330 large water supply systems, which serve communities of more than 100,000 people. The U.S. Environmental Protection Agency (EPA), as lead agency for the water supply sector, is working in cooperation with various associations on this issue, especially the American Water Works Association (AWWA) and the Association of Metropolitan Water Agencies (AMWA). Through these partnerships, EPA hopes to raise awareness of water sector vulnerabilities, encourage information sharing, and develop remediation protocols for the vulnerabilities that are discovered. The initial research effort is small and is focused on developing a vulnerability assessment methodology. Additional federal agencies including the Department of Health and Human Services (HHS) and the Federal Emergency Management Agency (FEMA) also assist with efforts in the water supply sector.

HHS requested funding in FY2001 to focus on emergency services infrastructures. Efforts include identifying key areas of interdependence among hospital and health care response and communications and transportation infrastructures, working with hospitals and related emergency services to identify operational vulnerabilities, and to determine ways to mitigate those vulnerabilities.

### Major Efforts Underway

In FY 2000, EPA entered into an interagency agreement with the Department of Energy to develop a vulnerability assessment methodology for the water supply sector. This methodology is an extension of the methodology developed for the federal dam community, which includes the Corps of Engineers, Bureau of Reclamation, Bonneville Power Authority, and Tennessee Valley Authority. The American Water Works Association (AWWA) – Research Foundation, a private not-for-profit organization that sponsors research for the drinking water industry, has also entered into a contract with Sandia National Laboratory to further support this vital work. Funds requested by HHS are also expected to assist in this effort. In the fall of 2000, a workshop with six to eight representatives of large water utilities outlined the approach of the methodology. This effort will extend into FY 2001, and the effort will be expanded to include field-testing and training for users.

In August 2000, EPA held a joint meeting on the water supply infrastructure with DOE at their Argonne National Laboratory. Most of the major federal water agencies and approximately 30 water utilities were represented. Meeting attendees reached an agreement on the approach and the priorities for water supply sector research.

Funds were requested in the FY2001 budget submission to Congress to initiate a more robust water sector CIP program. OMB has provided the following direction to the EPA:

“Through partnerships with AMWA and AWWA, EPA will work with water utilities undertaking measures to safeguard water supplies from terrorist and seditious acts. EPA will also implement an assessment of the vulnerability and methods to reduce vulnerability of the drinking water supply to terrorists acts.”

Other areas of interest include remediation measures, threat analysis and communications techniques, methods to identify and characterize chemical and biological agents, and a university or industry-based center of excellence in risk assessment and risk reduction. Specific efforts are underway, in cooperation with the FBI, to develop an Information Sharing and Analysis Center for the water supply sector to facilitate the exchange of threat and vulnerability information.

FEMA is also leading an effort to produce valid and verified databases of water distribution systems and to develop assessment tools for evaluating the threat to public health and safety posed by the introduction of a biological or chemical agent into a water system. Two prototype databases and assessment tools will be developed covering:

1) broad area populations at risk (statewide) and 2) local area populations at risk (citywide). The broad area prototype will allow the user to track an agent, under variable flow conditions, from the point of introduction to downstream water supply intakes and will determine the concentration and decay rate of an agent as it is dispersed within the water source. The local area prototype will allow the user to model the flow and concentration of an agent within a city or municipal water system, will assess the effects of water treatment on the agent, and will model the flow and concentration of an agent through the water distribution system.

The HHS program will focus on three of the VHS sector's high priority research and development issues identified by the NSC-lead interagency Critical Infrastructure Coordinating Group that need to be addressed to protect our critical infrastructures. First is the previously mentioned effort to develop a vulnerability assessment methodology for the water supply sector. Emergency services infrastructure issues include studying critical interdependencies between hospital and health care response systems and the communications, essential transportation, public safety, and emergency medical systems. This effort will look at how threats or damage to communications and transportation systems may affect the response capabilities of the hospital and health care community. A related effort will look at protection of hospital infrastructures. This effort will focus on critical hospital operations in response to a chemical or biological incident including decontamination, preventing cross-contamination, hospital capacity, etc.

#### Major Challenges in the VHS R&D Area

Ongoing water sector research is a small effort and leaves gaps and shortfalls in addressing identified vulnerabilities and shortcomings in U.S. water supplies. EPA is coordinating its efforts closely with other federal agencies and the private sector to identify the highest priorities and to work jointly to develop solutions to vulnerabilities and shortcomings.

The gaps and shortfalls in four major areas:

- *Threat/Vulnerability/Risk Assessments* – Focusing on threat, vulnerability, and risk assessment of the water supply sector critical infrastructure to include methodologies, benchmarks, field testing and analysis and communication of results.
- *Supervisory Control and Data Acquisition (SCADA) Systems*. Application of information assurance techniques to water supply SCADA systems and development of appropriate, cost-effective protocols. This work will rely heavily on efforts being conducted by DOE. The SCADA systems used in water utilities are similar to those used in the gas, oil, and electric power sectors.
- *Identify and Characterize Biological and Chemical Agents*. In conjunction with the Centers for Disease Control and other agencies, identify and characterize the behavior of chemical and biological agents in water. Determine the effects of water treatment on these agents and characterize the risks posed by these agents to the nation's water supply.

- *Center of Excellence for Risk Assessment of Water Supplies.* Establish a center of excellence to support communities in conducting vulnerability and risk assessments and in making decisions regarding water supply assurance.

### Conclusion

The cooperation of the water supply industry is essential in developing realistic research needs and in developing the tools that they need to evaluate and correct vulnerabilities. EPA has succeeded this year in establishing a good relationship with the major water association and has an agreement with them as to the priorities for the FY 01 budget.

### National Security

National Security Community CIP efforts are concentrated on understanding and protecting defense, national, and international infrastructures critical to national security during times of peace, crises, and war. Department of Defense (DoD) CIP addresses the relationship between critical assets and force readiness. It requires the identification, assessment, protection, monitoring, and operational assurance of cyber and physical infrastructures essential to the execution of the National Military Strategy. The challenge ahead is to maintain and build on the momentum and experience of recent years that demonstrated both the need for CIP and the ability of DoD to address CIP challenges on a global scale.

DoD has traditionally supplied the lion's share of R&D support for CIP R&D almost exclusively in the area of Information Assurance. Total federal CIP R&D funding has been between \$480-600M over the last few years, with defense providing typically about 80% of the total funding in this area.

Recognizing the increasing reliance on information systems by other critical infrastructures and their potential susceptibility to attacks, DoD is engaged in a wide range of activities that focus on protection of computer networks. The rapid advances in information and communications technology mean that as the years pass, entirely new infrastructure interdependencies embodying new technologies will emerge, and each will be accompanied by its own set of new vulnerabilities. The protection of information networks will require continuous improvement, and vigorous, focused research. The increasing reliance on information and communications systems by other critical infrastructures requires new efforts in the science, technology, and development of information and network security to achieve the most secure information network system possible, and to maintain our current position within the digital landscape.

The warfighting missions of the combatant Commanders-in-Chief (CINCs) span the globe and extend into space. With the draw down of overseas military force presence and the increasing dependence on outsourcing, DoD has increased its dependence on commercial and private infrastructures, many of which are neither U.S. owned nor controlled. The implications of the increasing interconnectivity and interdependence of commercial

infrastructures and defense sector assets demand that the DoD take steps to understand the vulnerabilities of and threats to the critical infrastructures on which it depends for mission assurance. Research efforts are required to understand and characterize the fundamental interdependencies of the DoD critical assets and infrastructures in order to circumvent potential vulnerabilities that may exist. The potential cascading effects of attacks on or failures of individual critical infrastructures need to be known. DoD must ensure that national and international infrastructure dependencies do not adversely affect the military's ability to fulfill its mission of national defense and global force projection as required by the National Security Strategy.

## **INTERDEPENDENCIES**

### Introduction

The economy and national security of the United States are becoming increasingly dependent on a spectrum of U.S. and international infrastructures, which themselves are becoming increasingly interdependent. This trend has accelerated over the last ten years with the proliferation of information technology and concomitant infrastructures, and shows no signs of abating. And while the U.S. economy has long depended on several critical infrastructures, the coupling among them had historically been rather loose.

In recent years, however, important technological, economic, and regulatory changes have dramatically altered the relationships among infrastructures. At the same time as the information technology revolution led to substantially more interconnected infrastructures with generally greater centralization of control, "just-in-time" business practices have reduced margins for error in infrastructure support. Deregulation and growth of competition in key infrastructures has eroded spare infrastructure capacity that served as a useful "shock absorber" in key infrastructures. Furthermore, the growth of mergers among infrastructure providers has led to further pressures to reduce spare infrastructure capacity as management has sought to wring "excess" costs out of merged companies to realize savings. Any one of these trends would be a cause for uneasiness. The collision of all four has no precedent in American economic history. While important steps have been taken in individual infrastructures, the issue of interdependent and cascading effects among infrastructures has received almost no attention. Accordingly, a greater understanding of the nature and implications of these infrastructure connections motivates this effort.

### What Are Interdependent Effects?

Interdependent effects are the effects that occur when an infrastructure disruption spreads beyond itself to cause appreciable impact on other infrastructures, which in turn cause more effects on still other infrastructures. When an infrastructure suffers an outage, it is often possible to estimate the impact that outage has on the infrastructure's ability to

deliver the service it provides. These are the “directly dependent effects” of the outage. However, that outage may also diminish the ability of other infrastructures, through no malfunction of their own, to deliver the level of services that they normally provide. These indirect effects make up a *first-order* interdependent effect.

Of course, the impact of the outage may not stop at these first-order effects. They may then go on to adversely affect still other critical infrastructure components, including even the infrastructure that was the original source of the problem, further aggravating the situation. These effects become *second-order effects*, which can propagate still further, causing still higher order effects. How far these effects propagate, and how serious they become, depend on how tightly coupled the infrastructure components are, how potent the effects are, and whether or not countermeasures such as spare capacity are in place. Either the outage effects will die out as they move further away from the base outage, limiting overall damage, or they will gather force in successively stronger waves of cascading effects until part or all of the infrastructure network breaks down. In the latter case, the loss of some key component creates a much broader failure out of all proportion with the original failure. Given the linkages among infrastructures, a cascading failure might cross infrastructure boundaries, as it did with the 1998 Galaxy IV satellite failure mentioned earlier.

### Major Efforts Underway

Several efforts are underway to try to tackle the difficult issues of interdependencies. These include efforts to learn about the secure operation of complex interactive networks/systems, and furthering the understanding of the dynamics of complex interactive networks/systems; technology development and vulnerability analysis capability R&D, aimed at analyzing national and defense infrastructures and their critical interdependencies; efforts to develop an easy-to-use, deployable state-of-the-art hazard and consequence prediction, digital databases, and a Geographic Information System (GIS), within a Graphical User Interface (GUI); collaborative work between the Disaster Research Center at the University of Delaware and the Research Center for Disaster Reduction Systems, a unit within the Disaster Prevention Research Institute at Kyoto University to better understand various aspects of damage caused by earthquakes; and interagency efforts to build upon a number of ongoing programs and laboratory testbed facilities

### Major Challenges in the Interdependencies Area

The major efforts underway, as well as those being investigated for the future, are designed to meet the following research challenges.

- Build a theoretical framework for understanding and predicting the nature of interdependencies and their effects on the country as a whole.
- Develop the capability to model and simulate in real time the behavior of the nation’s interconnected infrastructures by developing an architecture and related enabling technologies that can be used to integrate infrastructure-specific and interdependence

databases and analysis tools to study the linkages among the interdependent critical infrastructures, the interdependencies associated with those linkages, their impacts, and their likely causes.

- Develop a set of quantitative metrics for measuring the scale of impacts of interdependency-related disruptions.
- Develop new technologies and techniques to contain, mitigate, and defend against the effects of interdependency-related disruptions, such as escalating, cascading, latent, and cross-infrastructure failures.
- Develop capabilities to adequately and realistically test new methodologies, techniques, and technologies.
- Define a set of tasks for further work on specific national security policy issues that could be analyzed using these tools and methodologies. This could include, for example, characterizing the potential interdependence implications, from national security and economic perspectives, of current trends within the private sector (e.g., restructuring, deregulation, increased reliance on cyber monitoring and control systems) and their implications for national security; identifying interdependency vulnerabilities in the U.S. economy; and developing metrics for interdependencies.
- Develop the ability to characterize and incorporate new critical infrastructures into the models and methodologies as such infrastructures develop.

#### Guiding Principles of Interdependencies Research and Development

The Interdependencies Subgroup, in developing its draft agenda for interdependencies R&D, developed a set of six guiding principle characteristics that it believes the R&D programs in this area should follow:

- *Focus on True Cross-Infrastructure Behavior.* The research should address the effects from interactions among the different infrastructures and not be stove-piped on one infrastructure only. It may be necessary to focus on subsets of the entire set of infrastructures to make progress on interdependencies, but this should be only a way-station on the road to full interdependency analysis. At the same time, the focus should be on the interdependent behavior effects and impacts, and on measures to address these effects and impacts, and not the total behavior of the overall system of infrastructures.
- *Holistic Approach.* The research program as a whole needs to examine the entirety of the interdependency issue, to include positive interdependencies during the recovery and reconstitution phases as well as the negative interdependencies during the deterioration phase.
- *Near- and Long-Term Focus.* Individual research projects should have both near-term (3-5 years) and long-term (5+ years) relevance. At some point, it may be desirable to

pursue research that is strictly long-term in nature, but given the need for near-term research and the modest levels of funding that are likely to be available, long-term-only research is a luxury that is unaffordable at the present time.

- *Enhanced Resiliency and Robustness.* The research should have as a general goal the enhancement of the resiliency and robustness of the overall set of U.S. infrastructures. While the research objective of any specific project may be narrower than this, it should in some way contribute to this larger goal.
- *Vulnerability Orientation.* The research should be oriented toward interdependency vulnerabilities, as opposed to studying interdependent effects that do not threaten the viability of the U.S. economy or national security. As earlier, at some point it may be desirable to pursue research that studies relatively benign interdependent effects, but given the need for near-term research and the modest levels of funding that are likely to be available, such research is a luxury that is unaffordable at the present time.
- *Consequence Orientation.* The research should also be oriented toward interdependency consequences, as opposed to studying just the interdependent effects themselves.

### Research Issues

In planning for and conducting this research, there are several issues that will need to be addressed:

- *The level of dynamicity that is to be characterized in the architecture.* Technology levels are dynamic over the long-term but relatively fixed in the short term. How technological change is characterized and the scale of “permitted” change will need to be addressed. Likewise, commodity costs and availability could be treated as either fixed or variable. Physical plant available could likewise be treated as either fixed or variable, depending both on the level of architecture sophistication and time scale desired. A similar situation exists for operating practices.
- *Standards for inter-model data exchange.* Interdependency research will likely involve the combining of different sets of models, data bases, and related tools. While legacy components cannot be changed, new software and data, including that needed to integrate legacy inputs into an architecture, should be developed according to common standards.
- *Characterization of non-U.S. influences on U.S. infrastructures.* The U.S. economy and its associated infrastructures are becoming increasingly global in nature. While the focus of the modeling and related efforts is on the United States, the rest of the world plays an important role in the functioning of U.S. infrastructures. How and to what extent these influences should be represented will need to be addressed.

## Conclusion

Interdependencies among critical infrastructures is what makes this set of problems significantly different than those we have faced in the past, and it is what makes them difficult. Great work is being done in government, the national labs, academia and private industry to build an understanding of these issues, and tools to solve these problems. Clear challenges lie ahead for government, industry and academia to work on together.

In considering the interdependencies issue, the IWG noted the following factors:

- The CIP R&D IWG in 1998, 1999, and 2000 has been unanimous in its support for greater government research in the interdependencies area. Based on three years of interaction with the private sector and academia, the IWG has continued to find virtually unanimous support in these sectors for more government research into the question of interdependencies among the major infrastructures of the U.S. economy. Of all the CIP research areas, the IWG review continues to find that the issue of interdependencies had received little attention relative to that which the individual infrastructures have received, though there is a broad awareness of the need for and importance of the interdependencies issue. The IWG also has found that there was a critical lack of research underway on this issue in government, the private sector, and academia.
- The issue of interdependencies among critical infrastructures is a fundamental dimension of the critical infrastructure protection issue. Relative to the other infrastructure-specific concerns, interdependencies has been the least-studied and is probably the most in need of more comprehensive research. At the heart of this lack of attention to such a critical issue is the fact that unlike the individual infrastructures, there is no federal “Department of Interdependencies,” as there is a Department of Energy, Department of Transportation, etc. The agencies with the most relevant work in this area are the Departments of Energy, Defense, Transportation as well as the National Science Foundation.

## VII. DEVELOPING A FEDERAL R&D AGENDA

### Background and Methodology

While research and development is a broad term that covers activities from the most basic research through field R&D on deployed systems, the IWG has restricted its review to the following:

- *Basic Research.* This is research that increases the fundamental knowledge necessary for developing infrastructure assurance technologies.
- *Applied Research.* This is research that investigates the feasibility and practicality of proposed technological solutions.
- *Advanced Technology Development.* This is research that includes efforts to develop technologies and test their feasibility, effectiveness, and interoperability.
- *Proof of Principle and Validation.* This is research that evaluates the effectiveness of technologies in an infrastructure environment and assesses the performance, cost-effectiveness, and practicality of the technology from the perspective of the infrastructure.

Those familiar with R&D categories in the Department of Defense will recognize these categories as corresponding to 6.1, 6.2, 6.3, and 6.4, respectively. These are the categories that come before engineering and manufacturing development.

The CIP R&D IWG adopted a straightforward approach to developing a federal government R&D agenda. After preliminary briefings on the nature of the problem, the IWG identified the major vulnerabilities of each sector, as well as the existing CIP R&D work and programs already funded by the federal government in each sector. The IWG then sketched out an ideal, fiscally unconstrained set of programs to address these vulnerabilities in each sector. The gaps between the ideal and what was currently being undertaken then formed the raw material from which to develop an R&D agenda for FY2000 and beyond. Program initiatives were defined by the sector subgroups, taken from the Critical Infrastructure Assurance Office (CIAO) R&D Roadmapping study (dated June 10, 1998), or added by the IWG as a whole. The initiatives represent either an expansion of existing efforts beyond what is currently planned, or an entirely new set of initiatives. While in general the initiatives described are at the program level, in a few cases the IWG has identified specific projects.

### “A Work-in-Progress” Comprehensive Federal CIP R&D Agenda

Given the dynamic nature of the technologies involved, any comprehensive set of programs that is presented as a complete agenda for addressing critical infrastructure protection is at best a snapshot in time. Any program set will need to be updated on an

almost continuous basis. Accordingly, the IWG has assembled what it believes is a comprehensive but necessarily incomplete agenda of CIP R&D initiatives.

### Understanding the Agenda

A review of the extensive list of initiatives that the IWG identified illustrates the extent to which information technology has embedded itself in U.S. critical infrastructures. Of the initiatives that the IWG has identified as candidates for increased funding, less than one-third of these initiatives are not cyber-related. These represent less than 20% of the funding of the comprehensive agenda.

In reviewing these sector initiatives, the IWG found that while there are many important R&D issues to be addressed, eight stand out as the highest priority R&D issues:

- Establishment of an Institute for Information Infrastructure Protection
- The education and training of research personnel in CIP R&D
- Interdependency analyses
- Threat, vulnerability and risk assessment studies
- System protection and information assurance
- Reconstitution of damaged or compromised systems
- The security of automated infrastructure control systems
- Intrusion detection and monitoring

While some work has been done on the intrusion detection problem, this work has clearly not been sufficient to provide the level of detection needed. Thus it is included here, but ranked eighth because of the work already under way. The IWG also found that automated infrastructure control systems, especially SCADA systems, are important throughout the U.S. economy, and they appear especially vulnerable based on vulnerability work done to date. Accordingly, initiatives that address these two issues also merit priority attention.

The IWG emphasizes that these are program proposals only for the federal government. Although the IWG has briefed these programs to several private sector organizations, and to some extent the programs reflect gaps that may exist in the private sector, these proposals do not directly address the R&D the private sector is conducting. The IWG made some attempts to identify private sector R&D programs but found great reluctance to reveal any but the most general descriptions of their work. The IWG will prepare a more comprehensive listing of current federal CIP R&D programs after the results of congressional action on the FY2001 budget and OMB's final FY2002 budget data request are available.

The IWG wishes to emphasize that the program proposals described herein represent only the opinion of the IWG and do not necessarily represent the views of any agency. These recommendations, and the funding options discussed later, are made only to facilitate discussion among agencies for determining further steps in CIP R&D activity.

## VIII. INTERNATIONAL DIMENSIONS OF CIP R&D

Just as our critical infrastructures are inherently international, so too is the global science and technology base that will generate solutions to current and future infrastructure protection vulnerabilities. In general, the U.S. has no monopoly over the relevant technologies. Research and development in the field of information technology is a fully international enterprise today. In fact, it is even difficult to define a “domestic” science and technology base, given the substantial technical contributions made by foreign scientists and engineers within the U.S., by the overseas laboratories of U.S. companies, and by foreign or multinational firms with U.S. research facilities.

Moreover, the technologies relevant to infrastructure protection are largely unclassified, having been developed in the commercial sector or academia rather than in government or its contractors. Therefore, unless a particular R&D project involves classified material or is identified by its sponsoring U.S. government agency as raising particular sensitivities, it serves the U.S. national interest to draw on the global science and technology base, and to have the project done by the most qualified technical experts, wherever they may be. Indeed, the U.S. has a history of pursuing international science and technology collaboration as a means of stretching development dollars, broadening and deepening the talent pool that can be brought to bear, and building an international constituency for U.S. views. Many of the international science and technology activities, now considered to be CIP-related, reflect longstanding and continuing, collaborative efforts of private industry, academia, and government to resolve emerging information technology issues.

Appendix D of this document provides a Policy and Procedures Statement on International Research and Development Cooperation in Critical Infrastructure Protection. This Statement governs international cooperation on unclassified CIP R&D projects.

The Department of State has undertaken a variety of activities in response to PDD-63 including multilateral negotiations in the European Union (EU), Asia-Pacific Economic Cooperation forum (APEC), Organization for Economic Cooperation and Development (OECD), and other fora that addressed existing and emerging threats and vulnerabilities to our economic security. State has also led and coordinated bilateral negotiations and meetings with Canada, the United Kingdom, and Australia aimed at identifying, developing and facilitating science and technology solutions for CIP.

### Multilateral Agenda

- *EU.* A United States and European Union (EU) Task Force on Critical Infrastructure Protection (CIP) Science and Technology was established in October 1998 to enhance the security of critical infrastructures by identifying, developing, and facilitating technology and policy solutions to existing and emerging threats and vulnerabilities. The US Department of State co-chairs this Task Force with a senior European Commission representative from the Directorate General for Information Society. Over the past year the Task Force has sponsored a series of workshops and conferences resulting in cooperative exchanges between U.S. technical agencies and EC research organizations;

reciprocal exchange of information on cyber security research programs on an annual basis; coordinated research projects; visits and exchanges of scientists; and mutual exchanges of scientific and technological information.

- *APEC*. Within the APEC forum the U.S. (Department of State) succeeded in establishing a dialog on critical infrastructure protection telecommunication issues. At the APEC Telecommunications 21 Working Group meeting in March 2000, the Department worked closely with the Business Facilitation Steering Group (BFSG) to address the relationship and importance of infrastructure protection to e-commerce in each of the economies represented. By working closely with other APEC economies, the Department was also able to get infrastructure protection added to the APEC Telecommunication Program of Action during the Fourth Ministerial Meeting, held in Cancun, Mexico, in 2000. The Department continued to expand the APEC agenda on infrastructure protection science and technology (S&T) issues and arranged for State sponsorship of a half-day workshop at TEL 22 in October 2000 to develop a forum and advance proposals to facilitate awareness and sharing of information on critical infrastructure S&T issues in the Asia-Pacific region. At the APEC Telecommunications 22 Working Group meeting, in October 2000, the US, Australia and Canada sponsored a proposal for the development of cyber security training modules at both undergraduate and graduate level, to be used by member economies to increase the level of information security awareness and ultimately the protection of critical infrastructure. In the APEC Industrial Science and Technology Working Group, the U.S. successfully laid the groundwork for introduction of CIP technology cooperation with the aim of identifying all relevant research and development in the Asia-Pacific region.
- *OECD*. The U.S. initiated a discussion on cyber security issues within the Organization for Economic Cooperation and Development (OECD) in 2000. At the last meeting of the OECD Working Party on Information Security and Privacy (WPISP), State sponsored a presentation highlighting global aspects associated with information security, the economy's dependence on the internet, technical vulnerabilities of the internet, and possible solutions such as the concept of a center for analysis of global incidents, global intrusion detection and identification, research and development, and awareness raising through education and the media. This resulted in a discussion among economies and agreement for future work in this area. The U.S. was also successful in obtaining WPISP agreement in the Work Program for 2001-2002 to examine the present and future state of cyber security, including emerging threats and vulnerabilities. The U.S.'s efforts in subsequent meetings of the OECD have resulted in widespread agreement on the importance of cyber security and the role that OECD should take in progressing work in this area including an early review of security guidelines.

#### Bilateral Agenda

- *Canada*. The U.S. and representatives from the Canadian Government discussed CIP cooperative efforts at the national and departmental/agency levels, and in international fora at a bilateral meeting in September 2000. They agreed to establish a CIP R&D Working Group to take stock of current efforts and to identify potential synergies, and a

short list of area of further cooperation/joint action. There was also interest expressed in the idea of developing an International Center for Analysis of Global Incidents.

- *UK.* The U.S. met with representatives from the UK Information Assurance Advisory Council (IAAC) to discuss critical infrastructure protection science and technology issues and to exchange information on respective national and international policies on information assurance. The IAAC, whose membership includes the Cabinet Office, CESG, private industry and academia, has created five working groups to address CIP issues: Threat Assessment & Attack Warning, Risk Assessment & Critical Dependencies, Standards, R&D, Education and Outreach. The IAAC stressed the importance of industry involvement in addressing the increasing volume of attacks on infrastructure and expressed a desire to work cooperatively with US information sharing and analysis centers.
- *Australia.* The U.S. (Department of State) met on several occasions with Australian counterparts throughout 2000 to coordinate strategy for promoting both science and technology research and policy. Australia chairs the Working Party on Information Security and Privacy at OECD and in APEC they chair both the Business Facilitation Steering Group and the E-Security Task Force Group. Each of these forums are extremely important to U.S. outreach efforts. At present the Australian government only focuses on the information infrastructures and relies on existing arrangements to cover physical attacks on critical infrastructures. However, apart from this distinction between physical and information infrastructures, there is similarity between U.S. and Australian infrastructures and economic security interests. The Australian government has agreed to conduct a survey of all ongoing CIP R&D and meetings have already been scheduled over the next year to discuss areas for possible joint projects.

### Conclusion

The globalization of technology is a dominant force shaping today's world economy. In fact, calls for a more vigorous federal technology policy stem in large part from the recognition of this shift in the geographic distribution of the world's technological capabilities. What is not always noted, however, is that the very process of globalization calls into question the notion that technologies, industries, or even corporations have distinctive nationalities. It is impossible for any country to achieve its national science and technology objectives in isolation from other countries. Increasingly, the development of many high-payoff technologies is a high-risk, and costly venture, which exceeds the capacity and capabilities of individual firms, and even of countries. International S&T relations have become an integral part of overall U.S. foreign policy and play a vital role in meeting the challenges of infrastructure protection.

## **IX. THE MANAGEMENT CHALLENGES OF AN INFORMATION-INTENSIVE FUTURE**

There are a vast number of management challenges confronting government and society as a whole in the years immediately ahead that the advance of information technology and the growing interconnectedness of our critical infrastructures present us. Even within the R&D field, the number and magnitude is daunting. The first two presented below are the ones that the IWG believes are most important, followed by a number of others that also deserve serious attention.

### Institute for Information Infrastructure Protection

Of the five broad classes of critical infrastructures, the one that will probably be the most powerful and pervasive in the years ahead, and the one most susceptible to widespread outages, will be our information and communications infrastructure. U.S. security, prosperity, and well-being will be highly dependent on this information infrastructure. The United States must therefore be able to assure its robust, reliable, and continuous operation. The federal government and the private sector are now making substantial investments in cyber security technologies, yet neither the private nor public sectors are adequately exploring the fundamental principles that underlie complex, interconnected infrastructures, or developing key technologies or analytic methodologies crucial to protecting the information infrastructure.

The rapid – indeed, explosive – pace of technology change presents its own R&D management challenges. Commercial product cycles can be as short as three or four months, whereas government budget cycles span two to three years. It is difficult for the government to anticipate – years in advance – the technologies needed to mitigate future information infrastructure vulnerabilities and reduce future threats. Conventional government technology acquisition processes, which often require months to years to execute major procurements, may not be flexible or nimble enough to address the pressing – and rapidly evolving – technology requirements to ensure the security of our information infrastructure. Finally, the government’s time cycle for hiring (and firing) and providing incentives for employees is incompatible with everyday practices in the global information-based human resource marketplace.

Given these conditions, the President’s Committee of Advisors on Science and Technology (PCAST) recommended the establishment of a non-governmental Institute for Information Infrastructure Protection (IIIP). In response to this recommendation, the Clinton Administration proposed \$50 million for such an Institute through the National Institute of Standards and Technology (NIST) in its proposed FY2001 budget. Unfortunately, Congress did not fund this effort during 2000. Instead, Congress took three much more limited actions. The first was Section 8140 of the FY 2001 Defense Appropriations Bill, which permitted – but did not require – DoD to provide \$5 million to establish an “Institute for Defense Computer Security and Information Protection of the Department of Defense.” The second was in HR 4577, which provides \$5 million to NIST for CIP R&D grants, while the third was the provision of \$3 million in construction funds to create an Institute for Information

Infrastructure Protection at the Institute of Security Technology Studies (ISTS) at Dartmouth University in New Hampshire. Notwithstanding the name, this Institute does not necessarily share the features of the Administration's proposal for an IIP.

The original OSTP White Paper describing the Institute for Information Infrastructure Protection concept, written with input from PCAST members, industry and academia is included at Appendix E.

### Addressing the Shortage of CIP R&D Personnel

For over two years, the IWG has heard repeated stories of the shortage of trained R&D personnel available to do research in this area. The lure of high salaries in the private sector are enough to make fewer 4-year college graduates interested in pursuing advanced degrees that would better enable them to conduct such research. In 1999, the Committee on National Security, co-chaired by OSD and OSTP, called for a study of this problem. This section reports on this study and examines options for increasing the number of people both graduating with advanced degrees and teaching and performing basic research in the field of information security/assurance and critical infrastructure protection (ISA/CIP).

#### Background

The Office of Science and Technology Policy (OSTP) has examined possible solutions to the problem of insufficient numbers of researchers and professors in ISA/CIP. What follows is the view from the field – the input from experts in different fields concerned with ISA/CIP. It reflects these experts' ideas and seeks to generate discussion and policy. It is not a statement of U.S. Government policy.

The explosion in the U.S. information technology (IT) sector and the corresponding increase in demand for Information Security (IS) specialists within the past decade has caused a severe shortage in the number of academic professionals who are teaching and performing basic research in this field. According to the Marsh Commission report, *Critical Foundations: Protecting America's Infrastructure*, "There is a significant deficiency in the number of university faculty members equipped to teach information and computer security."<sup>4</sup> Dr. Corey Schou of Idaho State University has stated, "Evidence suggests that job growth in information technology fields now exceeds the production of talent. Between 1994 and 2005, more than a million new computer scientists and engineers, systems analysts, and computer programmers will be required in the United States — an average of 95,000 per year."<sup>5</sup> Additionally, graduate and doctoral students in information security are being recruited out of their academic programs and into the private sector, depriving academia of future professors and researchers. Consequently, there are not enough professors currently teaching and performing basic research in information security, nor will there be enough future professors to maintain this current number.

---

<sup>4</sup> President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: GPO, 1997), 70.

<sup>5</sup> Corey Schou, "Meeting the Information Assurance Crisis-Now," EDP Audit and Control Systems Journal, January 2001.

According to *The Supply of Information Technology Workers in the United States*, “doctoral programs are critical in the production of trained workers for both the occupations involving conceptualization and advanced development, and for faculty positions that will educate the next generation of IT workers.”<sup>6</sup> Additionally, “advanced researchers, such as faculty members in research universities or principal scientists in industrial research laboratories, almost always have a doctorate in an IT-related discipline, usually computer science or computer engineering (or occasionally in a closely related field such as physics, mathematics, or electrical engineering).” Doctoral level programs and researchers are essential to maintaining the critical U.S. lead in information technology, by supporting and conducting basic research and supporting students coming into the field.

ISA/CIP, as a sub-field of information technology, has gained importance in the past few years, as the private-sector has become more reliant on secure information systems. Consequently, private-sector demand for IS specialists has increased. However, there are only a few academic programs dedicated to advance research in this field, in turn meaning that there is a limited pool of qualified IS specialists.<sup>7</sup> The demand on the part of the private sector for this limited pool means that it is extremely difficult for dedicated academic programs to recruit IS-qualified instructors and researchers.

According to various sources, private-sector salaries and incentives are proving extremely attractive to IS doctoral students.<sup>8</sup> This has led to a further problem, the recruitment by private industry of IS doctoral students from their academic programs.<sup>9</sup> Referred to as a “seed-corn” problem, this means that not only is there a current shortage of educators in the field, but there will be an ongoing shortage into the future as long as there is a low number of doctoral students moving into academia.

A final problem is the emphasis of applied, short-term research over basic, long-term research. According to the President’s Information Technology Advisory Committee (PITAC), “during the past decade both industry and Government have altered the balance between basic research and the later stages of technology development and commercialization,” leading to “a serious decline in basic research activities.”<sup>10</sup> As basic research is critically important to long-term scientific advances, this decline threatens the current U.S. lead in secure information systems.

Although market forces will gradually increase the number of people going into this field, they will not solve the problem. The focus of private-sector research is on applied

---

<sup>6</sup> Peter Freeman and William Aspray, *The Supply of Information Technology Workers in the United States* (Washington, D.C.: Computing Research Association, 1999), 71.

<sup>7</sup> According to the National Security Agency, fourteen academic institutions have been labeled as “Centers of Excellence” in the teaching of information security (Vic Maconachy, National Security Agency, Interview, July 6, 2000). However, this estimate has proved controversial, with some sources stating that there are as few as five academic programs that are focused directly on information security (Gene Spafford, Purdue University, Interview, July 24, 2000).

<sup>8</sup> Various interviews with respondents.

<sup>9</sup> Freedman and Aspray, 117.

<sup>10</sup> President’s Information Technology Advisory Committee, *Information Technology Research: Investing in our Future*, 22.

research that emphasizes getting products to the market. According to the PITAC, “American businesses, in an ever-shrinking and more highly competitive world, have devoted less and less of their precious resources to long-term R&D, directing their efforts instead to reducing costs and getting new products in the pipeline today at the expense of the future.”<sup>11</sup> Neither is the private-sector focused on security issues that do not directly translate into marketable products and services or avoided costs. Accordingly, the influence of the private-sector will not directly increase the number of researchers and educators in the IS field.

In summary, there are not enough information security/critical infrastructure protection (ISA/CIP) experts currently teaching and performing basic research to meet the current demand; there are not enough doctoral students currently specializing in information security and intending to pursue academic careers to meet future demand; short-term applied research is being emphasized over long-term basic research; and industry-efforts alone will not solve these problems.

*Summary of ISA/CIP Education Recommendations:* The CIP IWG, under the leadership of OSTP and in cooperation with other federal efforts in the area of information technology research and education, set out to develop a list of recommendations designed to provide a solution to the shortage in ISA/CIP researchers and educators. Various members of academia, the private-sector, and government were interviewed to determine options for solving this problem. A brief summary of their recommendations includes the issues presented below. Details will need to be worked out, but any program developed should reflect their recommendations, which are briefly presented below:

- Support for ISA/CIP Education and Basic Research
- Support for Students Concentrating on ISA/CIP
- Support for Faculty Early Career-Development in ISA/CIP
- Support for Faculty Teaching and Research in ISA/CIP
- Support for Faculty Development in a New Area
- Support for Industry and Government Partnerships with Academia in Developing/Expanding ISA/CIP Education
- Support for IS Programs
- Consider New Business Models for CIP Education Programs, especially at the Graduate Level

---

<sup>11</sup> Ibid., 79.

## Other Management Challenges

The characteristics of the proposed R&D program, coupled with the sheer size and significance of the critical infrastructure assurance problem, virtually mandate new and innovative management concepts and structures to carry out the federal government's CIP R&D agenda. This gives rise to a number of management challenges that OSTP and the larger IWG process must address on an ongoing basis. Some of these are highlighted below.

- *Relations with the Private Sector.* While the government will fund a significant portion of the research, the private sector will probably perform the bulk of the developmental work. Market forces will drive this development and direct it toward products that have a market. Coordinating federal R&D with ongoing private sector programs will be complicated by industry's desire to guard proprietary programs and trade secrets. Performing the right research at the right time, synchronizing government programs appropriately with those in industry, and ensuring timely transfer of government-developed technologies to industry will require close coordination and partnership with the private sector.
- *Coordination of Federal Efforts.* The government CIP R&D agenda by its very nature cuts across a large number of federal departments and agencies. Ensuring proper coordination of individual R&D programs within agencies, let alone across agency boundaries, is an important task for the IWG to address. Likewise, the IWG should ensure that technologies are rapidly transferred among the agencies, and out to the private sector. In its activities to date, the IWG has already observed cases in which agencies had specific R&D needs yet were unaware that such programs were ongoing elsewhere within the federal government. In addition, a variety of federal government working groups manage related programs, such as the Technical Support Working Group<sup>12</sup> and the Weapons of Mass Destruction Protection IWG.<sup>13</sup> It will be crucial to ensure proper coordination and communications among such groups. The crosscutting nature of critical infrastructure protection R&D budgets further complicates program management and demonstrates the need for innovative, new approaches.
- *Emergency Law Enforcement Sector (ELES).* The proliferation of e-mail, the internet, and other cyber activity has placed demands on our law enforcement and national

---

<sup>12</sup> The Technical Support Working Group (TSWG), which conducts the national interagency R&D and rapid prototyping program for combating terrorism, contributed \$4.5 million to research and development in support of CIP during Fiscal Years 1999 and 2000. TSWG projects supporting CIP requirements included development of an electric power infrastructure database and analysis tool, characterization of the effects of Radio Frequency Weapons on infrastructure systems, development of the water pipeline database and analysis tool referred to in the VHS section, development in cooperation with the natural gas industry of an encryption algorithm for pipeline SCADA systems, the ongoing development of improved computer forensic tools for use by law enforcement, and development of improved physical protection and blast mitigation capabilities that could be used to protect critical infrastructure facilities. TSWG is also exploring collaborative CIP research and development programs with our allies through its International Program.

<sup>13</sup> The WMDP is a parallel effort to the CIP effort. It, too, falls under the policy auspices of the National Coordinator for Security, Critical Infrastructure and Counterterrorism, and the OMB National Security Crosscut.

security processes, straining our traditional legal structures and challenges our accepted thinking on the interplay between law enforcement and national security. Continued Law Enforcement R&D on the legal and forensic implications of emerging technologies would help reduce unrecognized vulnerabilities and dependencies and ensure new and innovative investigative techniques. These steps would also ensure that the right tools and methodologies are available at the time of attack. This would mean that we do not simply investigate and respond to attacks after they occur, but we try to learn about them and prevent them beforehand. In addition, better methods of accountability tracing could allow us to find the perpetrators of cyber crime while fully protecting the rights of others. In the course of 2000, the IWG became more aware of the challenges that CIP issues pose in the law enforcement realm, along with the potential of CIP R&D to deal with these challenges. Accordingly, the IWG plans to address these issues in 2001 and to make R&D recommendations to the CIG and NSTC.

- *Keeping Abreast of the Technology.* The technology, vulnerabilities, and threats to U.S. critical infrastructures are evolving extremely rapidly, such that it will quickly outpace the traditional lengthy budgetary process. This year's technological fix to a vulnerability could be obsolete within a few years, if not months. Entirely new systems could evolve in this time period, with their own vulnerabilities. Indeed, members of the Defense Science Board's 2000 Task Force on Defensive Information Operations have noted that as good as the 1996 DSB recommendations were, they already were out of date just four years later. Given the three-year nature of the government budget cycle (one year to develop the budget, one year to pass agency funding bills in Congress, and one year to begin to execute the programs), the rapid pace of technological innovation in critical infrastructures will stress any system put in place to develop and coordinate a government-wide R&D program. The federal R&D agenda should have the flexibility to deal with rapid changes in technologies and threats.
- *Interaction with State and Local Government.* The federal R&D program should be coordinated with state and local governments. In particular, the needs of "first responders" to emergencies and other assistance providers will determine many of the research directions in the vital human services sector. Factoring these needs into the federal R&D agenda is a step that can only be done through innovative management and partnership with the state and local levels.
- *Managing a Large Program.* The sheer magnitude of the program alone will require close attention, coordination, and dedicated management. Given the estimated FY2001 program resources (in excess of \$600 million), the federal CIP R&D program could easily exceed \$1 billion annually before long if future budgets place greater emphasis on this issue. These factors demonstrate the need for innovative management concepts and structures in order to effectively develop and administer a successful R&D agenda.
- *Data Sharing.* A general problem that every infrastructure faces is how to encourage the sharing of vulnerability and incident information in a way that does not deter companies from doing so and that does not run afoul of anti-trust concerns, competitive concerns, and

other issues. Cooperation would in theory help everyone involved, but there are clear risks involved in cooperation that to date have been major obstacles.

## **X. UPDATING THE CRITICAL INFRASTRUCTURE PROTECTION R&D AGENDA**

The IWG has identified the following thirteen tasks that will need to be performed on an annual basis to keep the R&D agenda current and to ensure that the federal government remains abreast of current technology in infrastructure protection:

1. Identify and update threats to and vulnerabilities in the nation's critical infrastructures that are amenable to technological solutions.
2. Identify and maintain a database of ongoing and proposed federal government CIP R&D programs and known private sector, academic, and international programs.
3. Develop and update a comprehensive, conceptual agenda of R&D programs required to address known and emerging infrastructure vulnerabilities.
4. Identify and update gaps and shortfalls in the existing programs based upon the comprehensive program and vulnerabilities. Develop an appropriate set of criteria for judging the priorities for federal government action.
5. Work in close conjunction with relevant department and agency personnel and sector liaison officials and recommend R&D areas for increased focus and resources. Identify budget requirements needed to fulfill the recommendations of the CIP R&D agenda. Coordinate this activity closely with Administration annual budget cycles.
6. Provide a forum and develop proposals to facilitate collaboration and the sharing of information on ongoing and planned CIP R&D programs among government agencies.
7. Develop and maintain means to harmonize federal CIP R&D with other existing federal R&D programs with which there may be overlaps or similar interests (such as those related to weapons of mass destruction, high performance computing, and force protection). Coordinate with other interagency forums and working groups (such as the Technical Support Working Group [TSWG], high performance computing, etc.) as appropriate.
8. Develop and maintain means to harmonize federal CIP R&D with programs in the private sector, state and local governments, academia, and the international community.
9. Develop proposals to facilitate technology transfer among government agencies and between the government and the private sector.

10. Establish and utilize a review group of outside industry and academic experts in critical infrastructure protection R&D disciplines to review existing and proposed programs.
11. Propose mechanisms to encourage and provide the environment to foster a partnership among the government, private sector, and academia for CIP R&D.
12. Develop an maintain means to coordinate public outreach on R&D issues.
13. Monitor foreign program and policy developments that may affect the direction or effectiveness of the federal program, and address possible relevant international cooperation.

The IWG should perform the first nine steps between January and May of each year. In June, the IWG should transmit an updated R&D agenda to the NSTC and the CIG for their review and use, which will allow the agencies and OMB sufficient time for the updated agenda to be integrated into the budget process.

In the period of July through November, the IWG should monitor the process of developing agency budgets. Synchronizing with agencies should help improve agency support for the agenda and avoid program disruption during the summer/fall period.

#### Oversight of Existing Programs

This will be an ongoing process, involving the monitoring of ongoing programs and new starts. The IWG will initiate a three-step oversight program to coordinate current programs, monitor their implementation, and assess their effectiveness against simulated or actual infrastructure outage events:

1. *Coordination of current programs*
  - Work closely with other IWGs (such as Weapons of Mass Destruction and Information Technology) – invite members of these IWGs as observers of the CIP R&D IWG.
  - Share/coordinate program information with other IWGs as appropriate.
2. *Implementation monitoring*
  - Maintain/update the database on a continuing basis.
  - Coordinate with agency program shops.
  - Recognize that status of program implementation may influence next FY agenda.
3. *Infrastructure outage events*
  - Coordinate with intelligence community on evolving threats.
  - Monitor actual attacks and draw lessons from these attacks for CIP R&D, and determine technological fixes if applicable.

- Use these inputs in developing future agendas – crash programs if necessary (e.g., a new, significant vulnerability appears that requires immediate attention).

### Outreach

Outreach to the private sector, academia, and other countries will be an ongoing process throughout each year. However, the IWG will emphasize outreach during the October – February period. The IWG will work closely with sector coordinators and sector liaison officials from each sector and agency in conducting its outreach efforts.

The IWG has held a number of workshops on CIP R&D over the last two years. Topics discussed include interdependencies, information assurance, and others. IWG members have also participated in a number of workshops and conferences on CIP R&D sponsored by industry associations, universities, government labs, and others. The IWG will also deepen its contacts with industrial associations (e.g., IEEE, computer security associations, etc.) and advisory committees such as NSTAC, PITAC, and others.

### IWG Organization

At present, the IWG plans to maintain its current structure of six subgroups, organized around the five major infrastructures, plus interdependencies.

## **XI. OBSERVATIONS**

Based on the three years' work of the R&D IWG to date, the IWG has made a number of observations on CIP R&D and the interagency budget and program process that may be useful to the Bush Administration.

- The IWG is prepared to address FY2002 budget issues in CIP R&D. The issue of 21<sup>st</sup> century threats is a daunting one, especially cyber attacks and other attacks directed at the critical infrastructures that underpin the U.S. economy. R&D, as well as effective management, will be key to the 21<sup>st</sup> century solutions to these problems.
- Determining the appropriate level of increased funding for CIP R&D will need to take into account existing budgeted activities and proposals for increases from the other CIGG groups. In addition, it will need to be considered in the context of other new budget initiatives such as weapons of mass destruction, counter-terrorism, and information technology.
- Opportunities for individual programs to respond to this IWG's recommendations and those of other groups should be grasped to maximize the benefits for given levels of spending.
- Important R&D needs will be foregone at FY2002 funding levels below the FY2001 baseline.
- Shortages of R&D professionals in disciplines relevant to CIP R&D could constrain our ability to execute a major increase in CIP R&D funding, not to mention our ability to provide IT professionals.
- There is a potential problem in ensuring that our academic institutions will be able to conduct the basic research needed in this area and to train the numbers of scientists and engineers needed for critical infrastructure protection, in no small part due to the appealing opportunities in the private sector. Steps such as outlined above, as well as others, will be needed to address this problem.
- The IWG believes this report's CIP research agenda will need continuing review and revision in the years ahead because of the dynamic nature of the technological environment it seeks to harness. The IWG also should monitor the research underway to ensure that the objectives for the research are being met.
- The extent to which agencies have experience in CIP R&D management will affect the pace at which they can ramp up their efforts on the programs identified in this agenda. The wide variation in CIP R&D management experience across different agencies underscores the importance of coordinated R&D oversight and innovative management solutions for addressing the CIP R&D agenda.

- Critical infrastructure protection presents one of the most demanding federal management challenges of the post-Cold War era. The pace of technological change in information technology and microelectronics ensures that the technological landscape of infrastructures and infrastructure protection will likely transform itself much faster than in the Cold War, for many years to come. The two-edged sword nature of this rapid pace of change will mean that the benefits from these changes will be accompanied by new avenues for hostile and non-hostile disruption.
- Any R&D process to manage our response to these new challenges should be sufficiently flexible and nimble enough to keep pace with this revolutionary environment.

## **XII. RECOMMENDATIONS**

- The IWG believes that a proper balance between fiscal restraints and responsiveness to the threats to the nation's critical infrastructures calls for greater levels of funding in the future over current FY2001 levels of CIP R&D. Either of the funding options presented in this report would be an important step forward.
- Existing and planned CIP R&D activities need to be coordinated with other technology initiatives to preclude overlap and promote synergy among these initiatives.
- The new Administration should explore options for R&D management models embodying the flexibility and nimbleness needed to ensure that the CIP R&D process can keep pace with the revolutionary technology environment for critical infrastructure protection in the years ahead. Following the PCAST recommendation, an "Institute for Information Infrastructure Protection," or something like it, should be established.
- The new Administration should receive a briefing in the very near future from the Intelligence Community on the nature of the critical infrastructure threat to the U.S. and its allies.
- A program to strengthen university training and research in disciplines that support CIP R&D should be proposed in the FY2002 or FY2003 budget cycle.

## APPENDIX A

### Glossary of Acronyms and Terms

**Advanced Technology Development** – research that includes efforts to develop technologies and test their feasibility, effectiveness, and interoperability. Cooresponds to the Department of Defense 6.3 research category.

**Applied Research** – research that investigates the feasibility and practicality of proposed technological solutions. Cooresponds to the Department of Defense 6.2 research category.

**Basic Research** – research that increases the fundamental knowledge necessary for developing infrastructure assurance technologies. Cooresponds to the Department of Defense 6.1 research category.

**CIAO** – Critical Infrastructure Assurance Office

**CICG** – Critical Infrastructure Coordination Group

**CIP** – critical infrastructure protection

**CIP R&D IWG** – Critical Infrastructure Protection R&D Interagency Working Group

**CNS** – Committee on National Security

**Critical Infrastructure** – those infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security.

**CT** – Committee on Technology

**GPS** – global positioning system

**I&C** – Information and Communications infrastructure

**Infrastructure** - a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.

**IWG** – interagency working group

**LNG** – liquified natural gas

**NSC** – National Security Council

**NSTAC** – National Security Telecommunications Advisory Committee

**NSTC** – National Science and Technology Council

**OMB** – Office of Management and Budget

**OSTP** – Office of Science and Technology Policy

**PCCIP** – President’s Commission on Critical Infrastructure Protection

**Proof of Principal and Validation** – research that evaluates the effectiveness of technologies in an infrastructure environment and assesses the performance, cost-

effectiveness, and practicality of the technology from the perspective of the infrastructure. Cooresponds to the Department of Defense 6.4 research category.

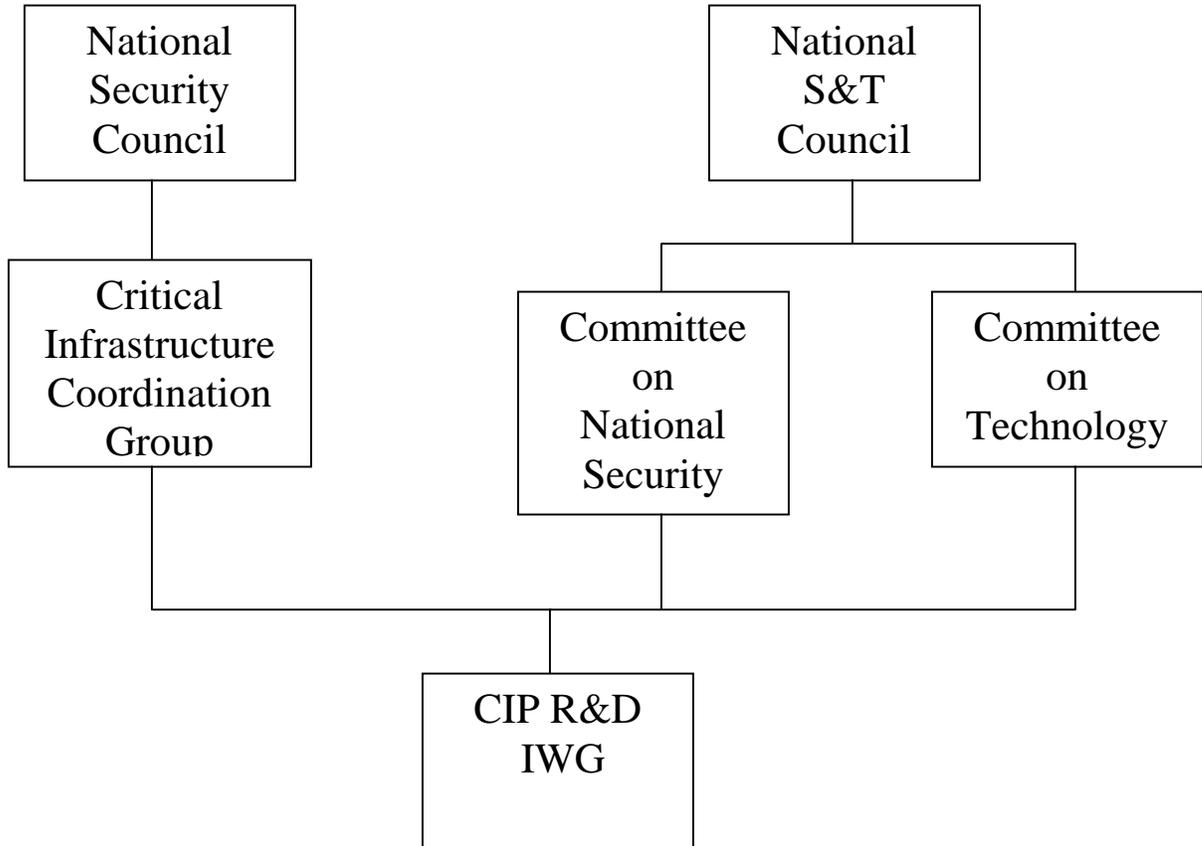
**PTN** – public telephone network

**R&D** – research and development

**SCADA** – supervisory control and data acquisition system. A computerized control system that automates many infrastructures such as oil and gas pipelines, electrical grids, etc.

**APPENDIX B**

**CIP R&D IWG in the  
S&T Structure of the Executive Branch**



## APPENDIX C

### CIP R&D IWG Agency POC Roster

Brigham	Edward	DOT	202-366-4434
Clark	Bill	HHS	301-443-9464
			202-619-0193
Clark	Steve	EPA	202-260-7159
Coyne	A. Heather	OMB	202-395-4545
Edwards	Betsy	NASA	202-358-4639
Gergely	Curt	TSWG/NSR	202-462-7161
Greene	Jim	FEMA	202-646-4302
Hagerling	Don	Treasury	202-622-2780
Kelly	Terry	OSTP	202-456-6057
King	Steven	DOD/ODUSD(S&T)	703-588-7414
LeBlanc	Mark E.	State	202-647-3517
Potter	Marshall	FAA	202-267-9828
Rosenthal	Robert	DOC/NIST	301-975-3603
Scalingi	Paula	DOE/OCIP	202-586-0588
Wright	Robert	NIPC	

## APPENDIX D

### Policy and Procedures Statement on International Research and Development Cooperation in Critical Infrastructure Protection

#### Introduction

Research and development (R&D) plays a key role in addressing the challenges posed by the Critical Infrastructure Protection (CIP) issue. The rapid evolution of technology, particularly in the information and communications sector, requires robust public and private CIP R&D programs to keep pace. International cooperation is an important component of an overall strategy to help meet this challenge. On one hand, such cooperation:

- Provides a way to make our R&D dollars go further.
- Brings a larger number of minds to bear on technical problems.
- Recognizes that U.S. infrastructures are becoming increasingly interconnected and interdependent with those of other countries.
- Helps to build an international constituency for the issue.

On the other hand, if not carefully managed, cooperative R&D in some technical areas could inadvertently reveal U.S. infrastructure vulnerabilities to potentially hostile parties. Once revealed, those parties could exploit this information to our detriment. Inappropriate R&D collaboration could also place the United States in a position where it is dependent upon foreign organizations for development of vital technologies, and cause other adverse effects as well. To counter such risks, this R&D policy establishes a mechanism to coordinate and monitor international cooperation with U.S. government-sponsored CIP R&D, and provides guidelines for program managers and review groups to use in making decisions on the suitability of R&D programs for international cooperation.

#### Background

Presidential Decision Directive 63 states in Section V that "the Federal Government shall encourage international cooperation to help manage this increasingly global problem." Section VIII of PDD-63 states that "there shall be a plan to 'expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations, and multinational corporations:" In Annex B of PDD-63, the National Coordinator for CIP is tasked to commission a study, *inter alia*, of the implications of sharing information with foreign entities.

## **General Procedures for International Research and Development Cooperation**

The CIP R&D Interagency Working Group (IWG) will review proposals for international collaboration that federal agencies seek to initiate in CIP R&D programs. Upon receipt of a proposal, the IWG shall circulate it among its member agencies. Any international R&D cooperation that may have existed prior to the effective date of this policy, and procedures statement need not be reviewed. For cooperative agreements in which agencies or departments have statutory authority, the CIP guidelines on international cooperation shall be incorporated into the policy documents on international cooperation of the respective agency or department. The review of critical infrastructure protection issues shall be conducted within the normal review process for these agreements. The record of this review will be provided to the CIP R&D IWG.

In preparing proposals for international collaboration in CIP R&D, federal agencies shall ensure that the proposals meet guidance contained in this policy and procedures statement. Federal agencies shall also be governed by provisions and guidance contained in Presidential Decision Directive 63 (PDD-63) on Critical Infrastructure Protection and guidance from the Critical Infrastructure Coordination Group (CICG).

In addition, agencies should:

- Follow future R&D cooperation guidelines issued by the CIP R&D IWG to cover specific situations.
- Evaluate and be prepared to address the cumulative effect of international R&D cooperation with foreign entities in the area they propose for cooperation.
- Maintain a permanent, retrievable record of all decisions concerning international CIP R&D cooperation with foreign entities including a description of the cooperation.
- Proposals for international cooperation in CIP R&D should:
  - Serve a specific U.S. national purpose.
  - Be driven by analyses of the benefits to the U.S. from the R&D collaboration against the risks to U.S. technology leads and security of information sharing.
  - Support the mission of the overall U.S. CIP R&D program.

Agencies should recognize that R&D proposals will not be approved which involve:

- The release or disclosure of information that would be contrary to U.S. law or to agreements or treaties between the U.S. and foreign nations.

- Information that reveals the existence of specific collection, counterintelligence, or special activities such as information operations capabilities that are not publicly known<sup>14</sup>.
- R&D the disclosure of which could reasonably be expected to jeopardize ongoing U.S. diplomatic, military, or law enforcement activities.
- R&D on specific U.S. vulnerabilities that are not publicly known<sup>15</sup>.

### **Oversight and Record-keeping Provisions**

As noted, Federal agencies should maintain a permanent, retrievable record of all international CIP R&D cooperation including a description of the decisions concerning such cooperation. Additionally, this record will identify essential information including the parties involved; the sectors) for cooperative activity; the CIP R&D topic areas) to which the cooperation applies; the type of research (basic, applied, advanced technology development, or demonstration and validation); description of R&D cooperation; expected research products) and, estimated funding by each party by fiscal year. This information should be kept current and a copy provided to the Chair, CIP R&D IWG.

---

<sup>14</sup> May be approved on a case-by-case basis, subject to appropriate controls

<sup>15</sup> May be approved on a case-by-case basis, subject to appropriate controls.

## **APPENDIX E**

### **White Paper**

**on the**

### **Institute for Information Infrastructure Protection**

July 11, 2000

Information technologies have revolutionized virtually every aspect of life during the past decade, affecting our Nation in ways as diverse as how business is transacted, to how our government functions, to the manner in which the military responds to crises. Importantly, every critical infrastructure upon which our security, our economy, and our way of life depend is linked to or reliant upon the information infrastructure. The United States must therefore be able to assure the robust, reliable, and continuous operation of the national information infrastructure.

Our nation's information infrastructure is a tightly coupled, highly complex, highly nonlinear system – and our current understanding of its robustness, resilience, and behaviors is rudimentary at best. New features and software are continually being developed and deployed on this complex system, without understanding their potential interactions or unintended operating characteristics. The susceptibility of the information infrastructure to cascading failures, the network architectures or operating conditions that would foster such breakdowns, and the theoretical basis for understanding and analyzing the infrastructure's operation are not well known. System architectures that would improve survivability, allow graceful degradations under stress, and ease reconstitution following failures – whether due to attacks, natural disasters, or human error – could dramatically improve the robustness, resilience, and security of the infrastructure.

The federal government and the private sector are now making substantial investments in cyber security technologies. However, neither the private nor public sectors are adequately elucidating the fundamental principles that underlie complex, interconnected infrastructures, or developing key technologies or analytic methodologies crucial to protecting the information infrastructure. Despite the fact that it owns and operates the vast majority of the information infrastructure, the private sector will not invest in security-related technologies if those technologies are too long-term, too high risk, too easily adopted by competitors, or otherwise unlikely to generate returns that can be captured by an investor. Such technologies are “public goods” – their development and adoption would benefit the nation as a whole, but they would not benefit any single firm enough for that firm to shoulder their investment cost. Therefore, government becomes the only realistic underwriter to ensure that these technologies are developed – a need that extends beyond funding, since these technologies will serve no useful purpose if they are not adopted and deployed. Just as our government defends the nation's highways, airways and sea lines of communications, so too must it play a leadership role in defending the nation's information and communications highways.

The obligation to ensure that these technologies are placed into operational practice differentiates infrastructure protection R&D from other areas where government invests in development of industrially relevant R&D. Existing government technology programs do an excellent job of developing and implementing new technology in those areas where industry is eager to participate, and where the risk of failure affects only the original investment. In infrastructure protection, however, failure to adopt new security technologies means that vulnerabilities in the nation's information infrastructure will persist. To eliminate these vulnerabilities, the government cannot afford to deal only with those firms that are highly motivated to collaborate – it must also engage those private sector owners, operators, providers, and users of information technology products and services that may not know of, or may not be particularly motivated to adopt, technologies developed through government investment. To enlist the participation of these more reluctant partners, government must adopt innovative business incentives that provide the private sector with a greater degree of visibility, participation, and “buy-in” than is associated with many traditional government agency programs and procedures.

The rapid – indeed, explosive – pace of technology change presents its own R&D management challenges. Commercial product cycles can be as short as three or four months, whereas government budget cycles span two to three years. It is difficult for the government to anticipate – years in advance – the technologies needed to mitigate future information infrastructure vulnerabilities and reduce future threats. Conventional government technology acquisition processes, which often require months to years to execute major procurements, may not be flexible or nimble enough to address the pressing – and rapidly evolving – technology requirements to ensure the security of our information infrastructure. Finally, the government's time cycle for hiring (and firing) and providing incentives for employees is incompatible with everyday practices in the global information-based human resource marketplace.

Given these conditions, the President's Committee of Advisors on Science and Technology (PCAST) has recommended the establishment of a non-governmental Institute for Information Infrastructure Protection (IIIP). In response to this recommendation, the Administration proposes to create such an Institute, funded through a cooperative agreement with the National Institute of Standards and Technology (NIST). The Institute will be an innovative public/private partnership that will have the required agility to address these pressing needs with the best talent the Nation has to offer. Given our ever-growing dependence upon information technologies, the increasingly sophisticated threats to information systems and networks, the ongoing possibility of natural disaster or human error, and the extraordinarily rapid pace of information technology change, the Institute offers the greatest promise of rapidly creating, disseminating, and ensuring the early adoption of those technologies and fundamental knowledge most urgently needed to protect our information infrastructure.

## **I. Background**

In late 1998, PCAST's Security Panel became concerned that existing government research mechanisms were not responsive enough to address security challenges in the rapidly growing and evolving information infrastructure. In a December 10, 1998, letter to the President, PCAST expressed its concerns and proposed that the government establish a "Laboratory for National Information Infrastructure Protection" (LNIIP). PCAST noted,

At present there is no technical organization dedicated to developing the know-ledge and common technology base required to successfully address this problem and provide the basis for long-term protection. The private sector does not have the incentive to develop the public knowledge and technology base required for the development of competing interoperable proprietary systems--thus federal support is needed. The justification for acquiring the needed knowledge and technology through government support of a new not-for-profit laboratory is that while most of the critical infrastructure lies outside the government, only the government is in a position to derive and make broadly available the information needed to assure the integrity of our nation's information network.

In his February 22, 1999, response to PCAST, the President agreed with the importance of protecting the Nation's critical infrastructures, including interconnected electronic networks. He directed the Office of Science and Technology Policy (OSTP) and the National Security Council (NSC) to perform a priority review of PCAST's proposal. This review, supported by an analysis of the concept by the Institute for Defense Analyses, concluded that there is a need for such an Institute. During an OSTP-PCAST meeting with the chief technology officers of 15 leading information and communications corporations, the private sector representatives unanimously endorsed the concept of a non-governmental, not-for-profit Institute to develop and disseminate technologies addressing urgent information infrastructure security issues of the type not normally addressed by individual private sector firms. In January 2000, the President announced his intent to establish an Institute for Information Infrastructure Protection, and in February he requested \$50 million in fiscal year 2001 funding for the Institute in the NIST budget.

## **II. Strategic Objective**

The Institute will foster the creation and dissemination of knowledge and technologies that are crucial to protecting the information infrastructure, and that will not otherwise be sufficiently developed by the private sector, government, or academia.

### **III. Guiding Principles**

- The Institute must stay abreast of the rapid evolution of information technology. This requirement has direct implications for Institute operations and funding procedures: the Institute must be able to identify, fund, develop, disseminate, and encourage the early adoption of technologies on time scales rapid enough to keep pace with evolving vulnerabilities in and threats to the information infrastructure.
- The Institute must define and assure the execution of an R&D portfolio that will help protect the national information infrastructure. It must therefore have broad access to both executive and technical leadership in government and the private sector. Likewise, the Institute must be aware of relevant ongoing and planned research in the private sector, government, and academia.
- The Institute must reach out broadly to the nation's technical community to seek solutions to the problems it and others have identified, complementing and leveraging the very substantial base of R&D already being conducted in separate but related fields. Moreover, it must be organized and operated in a way that maximizes the implementation of technologies developed under its auspices. Consequently, it must enlist the active and widespread participation of the largely-private sector owners, operators, vendors, and users of information infrastructure equipment and services in defining and executing the Institute's R&D agenda. It must not restrict its research support to a small or a closed set of institutions, particularly institutions that may be involved in its own management.
- The federal government must retain ultimate oversight, strategic guidance, and accountability for the expenditure of public funds. Technologies developed under the auspices of the Institute must support the protection of personal privacy and civil liberties.

### **IV. Organizational Structure**

- The Institute will be a nongovernmental organization funded through a cooperative agreement with NIST.
- NIST will select the management organization for the Institute through a full and open competition, using criteria that include ones discussed in the following section. NIST will re-compete the cooperative agreement every five years.
- Through its cooperative agreement with the Institute, NIST will exercise strategic guidance and oversight over the Institute without becoming involved in the Institute's day-to-day management or activities.

- NIST will also coordinate with other Federal Government Departments and Agencies to ensure that the Federal Government's interests as a major developer and user of information technologies are conveyed to the Institute.
- The Institute's management organization shall be a non-profit entity, a for-profit organization, a university, or some consortium or association of institutions in one or more of these categories. The Institute shall be governed by a private sector Board of Directors, as described in the following section. The Board of Directors, among other duties, shall be responsible for selecting the Institute's Chief Executive Officer.
- The Institute will strive to have the highest caliber technical experts on its small staff, which will consist of employees of the management organization as well as recognized experts from government, industry, academia, and other personnel who have been detailed or assigned to the Institute. The Institute's Chief Executive Officer shall be authorized to hire and fire employees of the management organization and shall be able to approve or terminate on short notice details or assignments of personnel from other organizations. Staff will rotate through the Institute on 3 to 5-year terms, thus constantly renewing itself and ensuring that staff members have the requisite subject matter currency and expertise. Subject to Board approval, the Institute will set its own personnel practices and standards that will be binding on employees of the management organization and that will set a standard that employees of other organizations who have been assigned or detailed to the Institute would be expected to follow where appropriate.
- The Institute will heavily focus its R&D funding on extramural research at those organizations most qualified to perform it, whether in the private sector, government, or academia. It will conduct little or no research in-house.
- The Institute's staff shall include an analytic core with the intellectual capability not only to manage the current research portfolio but to integrate and synthesize the disparate research activities supported by the Institute and elsewhere; to chart the course for future work; and to recommend modifications to the information infrastructure, taking into account technical findings as well as legal/social considerations. The staff shall also develop, for approval by the Board of Directors, long-term strategic plans, R&D roadmaps, and proposed research "Grand Challenges."
- The Institute will cultivate and maintain close relationships with organizations responsible for related, non-R&D missions such as setting standards, promulgating best practices, evaluating products, etc. Although the Institute will not directly set standards or develop best practices, it will ensure that relevant research results are made available to the appropriate organizations.

- Given the nature of its organizational structure and mission, the Institute must establish a set of policies related to intellectual property rights. The Institute must carefully balance the need to protect intellectual property and to provide incentives for the implementation of technology developed under its auspices, with the need to disseminate as broadly and rapidly as possible the research results and technologies developed under its programs.

## V. Award Selection Criteria

Proposals by entities seeking to manage the Institute shall be evaluated according to criteria that include the following:

- **Preference for Consortia.** Proposals from consortia that include academic institutions will be preferred. For-profit firms and non-profit institutions would also be eligible to bid, either alone or as a member of such a consortium.
- **Breadth of Representation on the Board.** The proposal will specify a Board of Directors providing widespread participation from academia and from the private sector. No more than one-third of the Board shall be affiliated with any of the institutions involved in managing the Institute. Private sector participants would represent – or have experience with – firms that manufacture, provide, and operate information infrastructure-related products and services; they would also represent customers of those products and services. Board members would recuse themselves from actions pertaining to institutions they were personally associated with, and they should not have potential conflicts of interest that would be so pervasive as to preclude effective contributions to the Board.
- **Quality, Openness, and Flexibility of Research Agenda.** The proposal should describe the general research agenda to be supported by the Institute, delineating the topics to be addressed and time scale over which results would be anticipated. This research agenda should not be so detailed that it overly constrains the Institute's flexibility to follow the rapid evolution of information technology. The proposal should delineate what areas of research, if any, would be done internally to the Institute, what would be done outside the Institute but by organizations involved in the Institute's management, and what would be supported through subcontracts or grants from the Institute to outside parties. One evaluation criterion for award – and renewal – of the Institute contract would be the degree to which the Institute engaged a wide and open pool of potential contributors and resisted the tendency to support a small and restricted set of participants. Ability to respond in a flexible and timely manner to new developments would also be important.
- **Replenishing the Pool of Information Security Researchers.** Given the importance of developing an adequate supply of information security researchers, one selection criterion for proposals will be the degree to which they support

multi-year, university-based research that provides a sufficiently stable funding stream to support graduate students and faculty hiring.

- **External Review.** Proposals shall discuss the review mechanisms to be used to ensure the relevance and technical excellence of the Institute’s R&D agenda, such as provision for independent external review by bodies such as the President’s Information Technology Advisory Council, the National Infrastructure Assurance Council, and/or the National Research Council. External reviews provided to the Board of Directors shall be shared with NIST.
- **Technology Transition.** Another selection criterion would be the expectation that research results or new technologies supported by the Institute would be adopted by firms or entities that are appropriate to implement them. Factors such as the participation of relevant firms in the research would be one way to demonstrate this. However, this criterion must be balanced against the need to conduct fundamental research that may be more difficult to translate directly into the marketplace.
- **Headquarters Location.** Proposals shall specify a location for the Institute’s headquarters that will facilitate accomplishment of the Institute’s mission. The headquarters should be located convenient to centers of information infrastructure R&D, easily accessible for travel, and attractive to the type and caliber staff that will need to be recruited to make it effective. The Institute’s headquarters are not envisioned to be located on federal government property.
- **Cost-sharing by industry, while acceptable, is not intended to be a selection criterion.** The Institute is intended to support research that is not being done in the private sector and for which there is little expectation of economic return to a particular firm. Therefore, at least initially, it is not expected that industry will contribute significant financial support. The Institute will, however, make provision to accept contributions and/or in-kind support from such non-federal sources.

## VI. Research Agenda

- The Institute’s staff shall periodically propose, for review and approval by the Board of Directors, updates to the Institute’s general R&D agenda.
- The agenda should include a set of research Grand Challenges, centering on research themes crucial to protecting and enhancing the security of the information infrastructure that are not likely to be sufficiently supported by the private sector or by government in the absence of the Institute. Examples are provided in the Annex. Ideally, Grand Challenges would pose questions whose solutions will drive significant advances in scientific understanding and technology development. While Grand Challenges may complement existing

research programs, they should not duplicate ongoing or planned government, private sector, or academic research.

- The defining characteristic for Grand Challenges and other Institute-sponsored R&D is that they address important concerns that would not otherwise be sufficiently addressed. This characteristic does not necessarily imply a time horizon for the research – although it is expected that a considerable portion of the Institute’s work portfolio will consist of high payoff/high risk endeavors, it would also be appropriate for the Institute to support important shorter-term R&D that the private sector has little incentive to conduct.
- The research agenda shall include development of a better fundamental understanding, including theoretical work, of the general properties of the information infrastructure, such as how it degrades and how it can be made resilient under stress.
- Given the global nature of the information infrastructure, the multinational character of many leading information technology vendors and service providers, and world-class research institutes abroad, the Institute shall draw on the global technology base in the absence of specific reasons to limit such participation, and it shall pursue international collaborative research programs when desirable.
- The Institute is not anticipated to sponsor any classified activity. However, the Institute must have provisions to handle, safeguard, and restrict the dissemination of sensitive or proprietary research results, information, or data. Moreover, it would be inappropriate to exclude the possibility that special circumstances calling for security classification could arise.
- The education of the next generation of researchers and professors in information assurance and security technologies is of critical national importance. One task of the Institute is to encourage support of research in university settings, which will help develop this next generation of information security researchers and educators. For example, this could include sponsorship of significant multi-year research activities at universities in collaboration with corporations and national laboratories, or equipment grants to establish test beds and laboratories for these collaborations. These actions would provide opportunities for graduate student support and a sufficiently stable research environment to justify and support faculty hiring.

**ANNEX: CANDIDATE TOPICS TO BE SUPPORTED BY THE INSTITUTE  
FOR INFORMATION INFRASTRUCTURE PROTECTION**

**A number of high priority research areas to meet the needs of both public and private components of the national information infrastructure have been identified in the process of planning the Institute for Information Infrastructure Protection, and the Institute’s initial R&D agenda might include any of the following. These topics, either individually or combined in technically related groups, could constitute candidate “Grand Challenges”:**

- Robustness, resilience, and behavior of tightly coupled, highly complex, highly nonlinear systems
- Network system interactions and vulnerabilities to cascading effects
- System architecture to ensure survivability; graceful degradation under stress; ease of reconstitution
- Develop fundamental principles, scientific basis, methodologies, and metrics for information assurance as an engineering discipline
- Next-generation intrusion and malicious code detection
- Visualization of system security information
- Self-healing systems
- Security and forensics toolkits
- Increasing resistance to penetration
- Concepts for high-confidence systems and software
- Information assurance for emerging information technologies
- Design of “testbeds” and other means for experimentally validating network security technologies
- Physical/cyber/human interfaces

Filename: Report on Federal CIP R&D.doc  
Directory: C:\Program Files\Adobe\Acrobat  
4.0\Acrobat\plug\_ins\OpenAll\Transform\temp  
Template: C:\WINNT\Profiles\shoemakes\Application  
Data\Microsoft\Templates\Normal.dot  
Title: DARPA Critical Infrastructure Protection Interdependencies Research  
Program  
Subject:  
Author: Rachel Lozano  
Keywords:  
Comments:  
Creation Date: 1/19/01 10:57 AM  
Change Number: 3  
Last Saved On: 1/22/01 11:44 AM  
Last Saved By: EOP  
Total Editing Time: 3 Minutes  
Last Printed On: 5/2/01 9:54 AM  
As of Last Complete Printing  
Number of Pages: 70  
Number of Words: 22,138 (approx.)  
Number of Characters: 130,617 (approx.)