AUGUST 2003 / VOLUME 2, NUMBER 2

THE CIP REPORT

MARK F. GRADY
Dean, School of Law, GMU
University Professor
Principal Investigator,
CIP Project

CIP PROJECT STAFF

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Rebecca Luria, *CIP Project Administrator / Executive Assistant*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

George Baker, *Associate Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

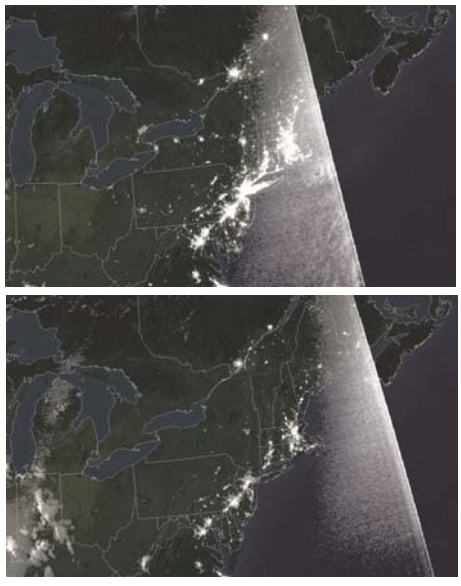
Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

Focus on the Hill

Since the terrorist attacks of 9/11, change has beset all levels of industry and government, not least of all Congress, where new committees and new legislation continue to emerge in an effort to address the threats of this new millennium. This issue of *The CIP Report* is focused on Congress and a sampling of the leaders, legislation, and organizations that are tackling homeland security and its subset of critical infrastructure protection.

This month we witnessed a major critical infrastructure event: the massive August 14 blackout that extended from Michigan to New York, wiping out power to 50 million people. As the investigation into the cause of this failure continues over the coming weeks, those in the critical infrastructure protection arena will reap lessons-learned not only on the technical aspects of electrical distribution, but on the information sharing and collaboration between state, local, and federal governments in both Canada and the U.S., private industry, and organizations such as the North American Electric Reliability Council, which was featured in *The CIP Report* in December 2002.



NOAA / Defense Meteorological Satellite Program images of the Northeastern U.S. before and during the blackout.

The House of Representative's Select Committee on Homeland Security will begin examining implications of the blackout on cybersecurity and critical infrastructure protection when it reconvenes in September. A number of proposed laws will also be debated in Congress, some of which are described in this issue. We are also pleased to include an OpEd piece co-written by Professor Vernon Smith, CIP Project Scholar and Nobel Laureate, for *The Wall Street Journal*. We hope that our readers find this issue of *The CIP Report* helpful and informative on the important work under way in the legislative branch of our government.

Homeland Security Committee Examines Implications of Power Blackouts For Nation's Cybersecurity and Critical Infrastructure Protection

Chairman Cox: Massive Regional Power Outage A Certain Terrorist Goal

WASHINGTON, DC - August 15, 2003 - Stating that a massive regional power outage such as the one that hit large portions of the greater New York area and the Midwest this week is "certainly a goal of our terrorist enemies," Homeland Security Chairman Christopher Cox (R-California) today announced the Committee will examine the implications of the blackouts for our nation's cybersecurity and critical infrastructure protection.

Cox said the Committee will hold a series of hearings investigating the vulnerability of our nation's power supply and distribution system to attack, as well as the catastrophic secondary consequences of a sustained denial to the nation's public health, food and water supply, and other vital infrastructure. The hearings, to take place when Congress reconvenes next month, will also examine the role of the Department of Homeland Security in coordinating a national response to such an attack and in ensuring adequate redundancy and emergency plans.

Chairman Christopher Cox

"The denial of electrical service for an extended period of time causes a dangerous ripple effect of death and destruction across virtually all our nation's civic and economic sectors," said Chairman Cox. "Lack of power can lead to significant fatalities and wreak tremendous havoc on our economy. This is certainly a desirable outcome to, and hence a goal of, our terrorist enemies. We must determine accurately how vulnerable our power system is to attack and sustained denial, and what steps our government is taking to reduce that vulnerability and mitigate the potential damage through contingency planning."

Potential hearing witnesses include policy experts on the nation's power system and its interdependencies, private and public officials from the public health, food quality assurance and transportation sectors, and officials from the Department of Homeland Security responsible for critical infrastructure protection, cybersecurity, and emergency preparedness.

The newly-created Select Committee on Homeland Security is designed to coordinate the efforts between Congress and the Federal agencies tasked with protecting our homeland from terrorist attack. ❖

Congressional Subcommittees Tackle Issues of Security, Critical Infrastructure

The House of Representative's Select Committee on Homeland Security has five subcommittees, two of which focus on critical infrastructure and cybersecurity issues.

The Subcommittee on Infrastructure and Border Security, chaired by Congressman Dave Camp, is charged with border security; illegal entry by foreign nationals; land borders, ports, and airspace; integration of federal, state, and local immigration law enforcement; protection of highways, bridges, waterways, airports and air transportation, energy supplies, and other critical infrastructure from attack; preservation of critical government, business, and financial institutions; and relevant oversight. Congresswoman Loretta Sanchez is the Ranking Member.
(Continued, Page 3)

Subcommittees *(Cont. from Page 2)* The Subcommittee on Cybersecurity, Science, and

Dave Camp, Chair
Subcommittee on Infrastructure and Border Security

Research & Development is chaired by Congressman Mac Thornberry, who co-sponsored the Homeland Security legislation with Senator Joe Lieberman. This subcommittee is examining security of computer, telecommunications, information technology, industrial control, electric infrastructure, and data systems, including science, research and development related thereto; protection of government and private networks and computer systems from domestic and foreign attack; prevention of injury to civilian populations and physical infrastructure caused by cyber attack; and relevant oversight. Congresswoman Zoe Lofgren is the Ranking Member.

This subcommittee held a number of hearings this year on the cyber threat environment, featuring witnesses from industry and government. The subcommittee also hosted a workshop for congressional staff to raise awareness of the issue on Capitol Hill. "Our goal," Thornberry stated, "is not only to prevent a devastating

Mac Thornberry, Chair
Subcommittee on Cybersecurity, Science, and R&D

attack on our infrastructure and cyber networks from occurring, but to better respond to the attacks which we know are being launched against our infrastructure and networks every day."

On the Senate side, the Committee on the Judiciary has a Subcommittee on Terrorism, Technology, and Homeland Security, chaired by Senator Jon Kyl. Senator Dianne Feinstein is the Ranking Democrat. This subcommittee's jurisdiction includes:

Jon Kyl, Chair
Senate Subcommittee on Terrorism, Technology, and Homeland Security

(1) Oversight of anti-terrorism enforcement and policy; (2) Oversight of Department of Homeland Security functions as they relate to anti-terrorism enforcement and policy; (3) Oversight of State Department consular operations as they relate to anti-terrorism enforcement and policy; (4) Oversight of laws related to government information policy, electronic privacy and security of computer information, Freedom of Information Act; (5) Oversight of encryption policies and export licensing; (6) Oversight of espionage laws and their enforcement. ❖

COMMENTARY

Demand, Not Supply

By VERNON L. SMITH and LYNNE KIESLING

Immediately following the failure of the electrical network from Ohio to the Northeast Coast, a cascade of rhetoric swept across news networks, blaming the blackout on an antiquated grid with inadequate capacity to carry growing demand for electrical energy. As in the California energy debacle, we are hearing the familiar call on government to "do something."

The California government response -- doing something -- left the state with a staggering and unnecessary level of debt. Meanwhile, without any additional action by the state, the demand and energy supplies in California have returned to their normal and much less stressful levels and wholesale prices are back to normal. There is no news except good news, but have we gained any deep understanding of power system vulnerability and its efficient cure from this event? Before Congress and the administration begins to follow the California model and throw other people's money at the power industry, let's have some sober and less frantic talk.

A systematic rethinking of the power demand and supply system -- not just transmissions lines -- is required to bring the energy industry into the contemporary age. Eighty-five years of regulatory efforts have focused exclusively on supply -- leaving on dusty shelves proposals to empower consumer demand, to help stabilize electric systems while creating a more flexible economic environment.

Under these regulations, a pricing system has developed that is so badly structured at the critical retail level that if it were replicated throughout the economy, we would all be as poor as the proverbial church mouse. Retail customers pay averaged rates, making their demand unresponsive to changes in supply cost. Without dynamic retail pricing, no one can determine whether, when, where or how to invest in energy infrastructure. Impulsive proposals to incentivize transmission investment, without retail demand response, puts the cart before the horse and risks expensive and unnecessary investment decisions, costly to reverse.

At the end-use customer level, the demand for energy is almost completely unresponsive to the hourly, daily and seasonal variation in the cost of getting energy from its source -- over transmission lines, through the substations and to the outlet plugs. The capacity of every component of that system is determined by the peak demand it must meet. Yet that system has been saddled with a pure fantasy regulatory requirement that every link in that system at all times be adequate to meet all demand. Moreover, the industry has been regulated by average return criteria, and average pricing.

When the inevitable occurs, as in California, and unresponsive demand exceeds supply, demand must be cut off. Your local utility sheds load by switching off entire substations -- darkening entire regions -- because the utility has no way to prioritize and price the more valuable uses of power below that relic of 1930s electronic technology. This is why people get stuck in elevators and high-value uses of power are shut off along with all the lowest priority uses of energy. It's the meat-ax approach to interrupting power flows. Between the substation and the end-use consumer appliance is a business and technology no-mans-land ripe for innovation.

When a transmission line is stressed to capacity, and its congestion cost spikes upward, the market is signaling the need for increased capacity in any of three components of the delivery system: increased investment in technologies for achieving price responsive demand at end use

(Continued, Page 5)

Demand, Not Supply *(Cont. from Page 4)* appliances; increased generation nearer to the consumer on the delivery end of the line; or increased investment in transmission capacity.

What is inadequately discussed, let alone motivated, is the first option -- demand response.

Many technologies are available that provide a dual benefit -- empowering consumers to control both energy costs and usage while also stabilizing the national energy system. The simplest and cheapest is a signal controlled switch installed on an electrical appliance, such as an air conditioner, coupled with a contract that pays the customer for the right to cut off the appliance for specified limited periods during peak consumption times of the day. Another relatively inexpensive option is to install a second, watt-hour meter that measures nighttime consumption, when energy usage is low, coupled with a day rate and a cheaper night rate. More costly is a time-of-use meter that measures consumption in intervals over all hours of the day, and the price is varied with delivery cost throughout the day. Finally, a load management system unit can be installed in your house or business that programs appliances on or off depending on price, according to consumer preferences.

More important, better and cheaper technologies will be invented once retail energy is subject to free entry and exit. No one knows what combination of technology, cost and consumer preferences will be selected. And that is why the process must be exposed to the trial-and-error experiment called free entry, exit and pricing. As in other industries, investors will risk their own capital -- not your tax dollars or a charge on your utility bill -- for investments that fail. Also, as in other industries with dynamically changing product demand, competition will force prices to be slashed off-peak, and increased on-peak to better utilize capacity.

Together with demand response technologies, a simple regulatory fix can give new entrants the incentive to provide customers with attractive retail demand options. Local regulated distribution utilities have always had the legally and jealously protected right to tie in the rental of the wires with the sale of the energy delivered over those wires. But these are distinctly separable activities. Just as rental car companies are separate from gas stations, electricity can be purchased separately from the company that delivers it to you -- provided only that they can access the wires to install metering, monitoring and switching devices that fit the budget/preferences of individual consumers.

Remember when Ma Bell would not let you buy any telephone but hers, and would not let you admit any licensed electrician into your house to access the telephone wires except those arriving in her service truck? All that has changed for the better in telecommunications, but we are still stuck in a noncompetitive world in the local utility industry.

* * *

Against the backdrop of the wars in Iraq and Afghanistan, the East Coast blackout stimulated déjà vu speculation of Sept. 11 and fears of shadowy operatives bent on disaster. Since 2002, the Critical Infrastructure Protection Project at George Mason University has worked under a Department of Commerce grant to integrate the study of law, technology, policy and economics relating to the vulnerability of key U.S. infrastructure. Prime among this continuing research is investigation of the susceptibility of the national power grid.

As it turns out, terrorist speculation, though false, did not fall far from the truth. If you were to design an electrical system maximizing vulnerability to attack, it is hard to imagine a better design than what has evolved in response to regulation. If a terrorist attack took out half the energy supply to Chicago, the only viable response would be to shut down half the substations. Demand response would allow a prioritization of energy use, shutting down only the lowest priority of power consumption while supplying high value uses -- such as production facilities, computer networks, ports, airports and elevators. Power systems badly need the flexibility to selectively interrupt lowest value uses of power while continuing to serve higher value uses. Retail price responsiveness in a competitive environment provides such a priority system. *(Continued, Page 11)*

A Glance at Legislation, Passed and Pending, Since 9/11

Legislators Address Security in Dozens of Proposed Laws

The **Terrorism Risk Insurance Act** (Pub. L. 107-297, 116 Stat. 2322) became effective November 26, 2002. Purposes of the Act include addressing market disruptions, ensuring continuing widespread availability and affordability of commercial property and casualty insurance for terrorism, and allowing for a transition period for the private market to stabilize and build capacity while preserving State insurance regulation and consumer protections.

To these ends, the Act established the Terrorism Risk Insurance Program (TRIP), which provides for combined public and private compensation for insurance losses due to acts of terrorism. Through the TRIP, the federal government covers 90% of the excess insurance costs relating to terrorist acts if the cost exceeds an annual deductible that insurance companies pay to the government each year of the program, which is effective until December 31, 2005. Other provisions of the act include disclosure of policy requirements and procedures for managing litigation.

The **Aviation and Transportation Security Act** became public law (PL 107-71, 115 Stat. 597) on November 19, 2001. Congress negotiated this statute in the weeks following 9/11 to address security planning for aircraft. The Act federalized airport security workers, mandates random deployment of armed guards on commercial flights, and requires physical security improvements in planes and airports. The Act established the Transportation Security Administration (TSA) within the Department of Transportation to manage aviation security in the passenger aircraft and cargo sectors.

The measure requires that all baggage be screened, and that passengers can be checked against law enforcement watch lists. The measure allows pilots to carry guns with the permission of their airline and the TSA after specialized training; requires mandatory training for flight crews on how to deal with hijacking attempts; and mandates strengthened cockpit doors, which would have to remain locked during flight.

The **Chemical Facilities Security Act (S 994)** is designed to regulate security and vulnerability assessments in the chemicals sector. Under the statute, Congress would require the Dept. of Homeland Security (DHS) to develop implementing regulations and programs, including the development of standards and auditing requirements. If adopted, the statute would make DHS responsible for risk assessment and security regulation in a major segment of the economy.

The Act involves the following core requirements and features:

- Vulnerability Assessments - Within one year of passage, DHS must promulgate regulations that require owners to perform vulnerability assessments. The assessment must focus on terrorist acts as well as hazards that may result from a terrorist attack.
- Security Plans - Within one year, DHS must also prepare regulations guiding development of site security plans. The security plans must address vulnerabilities identified in vulnerability assessments.

The $28.5 billion **Homeland Security Appropriations Bill (HR 2555)** is headed for a House-Senate conference. The bill would grant DHS's Information Analysis and Infrastructure Protection Directorate a total of $823.7 million to identify and assess threats, map threat information against current vulnerabilities, issue warnings, and take preventive action, including:

- $98.5 million for cybersecurity infrastructure monitoring and coordination;
- $293.9 million for critical infrastructure identification, assessments, and protection implementation; and,
- $155.1 million for the Nat'l Communications System.

The Science and Technology Directorate would receive a total of $866 million to support basic and applied research, development of prototypes, and procurement of systems to mitigate the effects of weapons of mass destruction.

- $18 million for cybersecurity;
- $70 million for rapid prototyping/technical support working group;
- $55 million for university programs; and,
- $72 million for critical infrastructure protection.

COMMENTARY

The Future of Racial Profiling in the War on Terrorism

by Nelson Lund

Before 9/11, we had what looked like a clear national consensus against racial profiling in law enforcement. Although the issue had become controversial, the disputes were almost entirely concerned with whether the police were in fact commonly using forbidden racial stereotypes, especially when choosing which motorists to pull over for traffic violations that are so common that officers necessarily ignore them most of the time.

Then came the terrorist attacks. All of the hijackers who carried out the hijackings were Middle Eastern men, and commentators began arguing that racial profiling is an appropriate tool in the war on terrorism. Judge Robert Bork, for example, has neatly distinguished ordinary law enforcement from the new threat we face: "The stigma attached to profiling where it hardly exists has perversely carried over to an area where it should exist but does not: the war against terrorism."[1] The public seems to agree. Polls have showed strong majorities in favor of subjecting those of Arab descent to extra scrutiny at airports. Interestingly, blacks and Arab-Americans were even more likely than whites to favor such policies.[2]

The Bush Administration at first resisted the pressure to employ racial profiling.[3] The Department of Justice, however, has now reversed course and adopted Judge Bork's distinction between ordinary police work and anti-terrorism activities. In June, the Department's Civil Rights Division promulgated a new directive entitled "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies." This document adopts two standards, one for "traditional law enforcement activities," and a very different one for certain other police activities.

Nelson Lund is the Patrick Henry Professor of Constitutional Law and the Second Amendment, and Foundation Professor of Law at George Mason University.

The first standard is faithful to President Bush's pre-9/11 statement that racial profiling is "wrong and we will end it in America." Federal agencies are forbidden to consider race[4] in any "traditional" law enforcement decision, except where officials have trustworthy information linking someone of a specific race to a specific crime, as for example where a credible eyewitness has described a fleeing felon as a member of a particular race, or where a criminal organization is known to comprise members who are overwhelmingly of a given race. Because these exceptions do not entail racial profiling or stereotyping, the Justice Department has effectively imposed a total ban on that practice in traditional law enforcement activities.

A completely different standard is now applicable to federal activities involving threats to "national security or other catastrophic events (including the performance of duties related to air transportation security) or in enforcing laws protecting the integrity of the Nation's borders." According to the new Justice Department guidance, racial profiling may be used in these contexts whenever it is permitted by the Constitution. This is very close to giving federal officials *carte blanche* to select targets for investigation or especially intensive attention on the basis of racial stereotypes.

The applicable constitutional test is called "strict scrutiny." As the Justice Department acknowledges, applying this test is "a fact-intensive process." That is just another way of saying that there is no clearly defined constitutional line between permissible and impermissible uses of racial profiling. And because the Justice Department makes no effort to draw a line between what it regards as permissible and impermissible, security officials are effectively encouraged to err

(Continued, Page 8)

Racial Profiling *(Cont. from Page 7)* in the direction of using racial stereotypes whenever they might seem useful.

The only examples of forbidden behavior offered by the Justice Department are two very extreme cases. First, the Department rules out using racial criteria "as a mere pretext for invidious discrimination." This is something that nobody would ever admit to doing. Second, the Department says that a screener may not pick someone out for heightened scrutiny at a checkpoint "solely" because of his race "[i]n the absence of any threat warning." This situation cannot even arise, given that the whole nation is under a constant and continuing "threat warning" that is likely to remain in place for the foreseeable future; thus, the principal implication here is that screeners may indeed focus on individuals "solely" because of their race so long as any threat warning remains in place.

In addition to being inherently "fact intensive," the constitutional test will almost certainly be applied by the courts in a way that is extremely deferential to the discretionary judgments of federal officials. The leading case, *Korematsu v. United States*, upheld the mass internment of Japanese-Americans during World War II, even though the internment program was based entirely on a generalized and unsubstantiated mistrust of Japanese-Americans. Although this decision has frequently been criticized, it has not been overruled. Similarly, the Supreme Court has held that law enforcement decisions based on racial stereotypes do not violate the Fourth Amendment.[5] And, in its most recent decision on racial discrimination, the Court gave extreme deference to the discretionary judgments of government officials who used a form of racial profiling in admissions decisions to a state law school.[6] Because the government interests at stake in this affirmative action case were clearly much less urgent than those involved in preventing terrorist attacks, one must infer that the Court has implicitly dictated a virtual hands-off policy with respect to judicial supervision of racial profiling in this context.

The Justice Department's guidance document, which encourages federal agencies involved in anti-terrorism and related activities to employ racial profiling to the full extent permitted by the Constitution, has several serious imperfections, including the following:

First, law enforcement officials now have an incentive to bring ordinary law enforcement activities under the rubric of "national security or other catastrophic events" in order to escape the very strict rules imposed by the Department for traditional law enforcement. If an agent at the DEA decides that the escape of a particular drug trafficker would be "catastrophic," the Justice Department's guidance does not clearly prohibit him from using racial stereotypes in his investigation. The same goes for many other activities that Congress has thought so threatening that they deserve to be made federal crimes.

Whether or not this bleeding of the categories occurs on a significant scale, the unbridled use of racial profiling as a tool in the war on terrorism and other "catastrophic events" could significantly undermine the unfulfilled national commitment to making citizens of all races equal under the law. Few events could have been more catastrophic than losing World War II, yet almost everyone now recognizes that massive racial profiling, albeit lawful, was a completely inappropriate and unnecessary means of preventing that catastrophe.

Finally, the Justice Department has neglected one of the most obvious and well-known pathologies of government bureaucracies. The new policy imposes virtually no controls on the use of racial stereotypes in an indeterminately large class of activities. This will encourage government officials to employ racial stereotypes, and it may foster the lazy use of such stereotypes. The actual effect could well be to impede the war on terrorism.

We have a recent example of this danger: the investigation (in which the Department of Justice participated) of the terroristic sniper attacks in the Washington, D.C. area in late 2002. Apparently relying on well-publicized "criminal profiles," according *(Continued, Page 11)*

Congressional Agencies Providing Oversight and Insight: General Accounting Office and Congressional Research Service

The U.S. General Accounting Office (GAO) is an independent and nonpartisan agency that studies how the federal government spends taxpayer dollars by studying federal programs and expenditures. GAO works for Congress, which is how the agency came to be known as the "Congressional watchdog." GAO advises Congress and the heads of executive agencies about ways to make government more effective and responsive. GAO evaluates federal programs, audits federal expenditures, and issues legal opinions. When GAO reports its findings to Congress, it recommends actions, which often turn into laws and acts that improve government operations, and save billions of dollars.

GAO supports congressional oversight by:

- evaluating how well government policies and programs are working;
- auditing agency operations to determine whether federal funds are being spent efficiently, effectively, and appropriately;
- investigating allegations of illegal and improper activities; and
- issuing legal decisions and opinions.

With virtually the entire federal government subject to its review, GAO issues more than 1,000 reports and hundreds of testimonies by GAO officials each year. GAO's familiar "blue book" reports meet short-term immediate needs for information on a wide range of government operations. These reports also help Congress better understand issues that are newly emerging, long-term in nature, and with more far-reaching impacts.

The GAO is headquartered in Washington, D.C., and has offices in several major cities across the country. The agency is headed by the Comptroller General, who is appointed to a 15-year term. The long tenure of the Comptroller General results in a continuity of leadership that is rare within government. GAO's independence is further safeguarded by the fact that its workforce is comprised almost exclusively of career employees who have been hired on the basis of skill and experience. Its 3,300 employees include experts in program evaluation, accounting, law, economics, and other fields.

The General Accounting Office was created by the Budget and Accounting Act (42 Stat. 20) in 1921. The law was aimed at improving federal financial management after World War I. Wartime spending had increased the national debt and legislators saw that they needed better information and control over expenditures. Congress passed the Budget and Accounting Act to require preparation by the President of an annual budget for the federal government and to improve accountability. The statute transferred to GAO auditing, accounting and claims functions previously carried out by the Department of the Treasury. The act made GAO independent of the executive branch and gave it a broad mandate to investigate how federal funds are spent. Later legislation clarified or expanded GAO's powers, but the Budget and Accounting Act continues to serve as the basis for its activities.

The agency has evolved from a voucher checking operation in its earliest years to a multi-disciplinary organization examining everything from missiles to medicine, from aviation safety to food safety, from national security to social security. Its highly trained staff performs financial and performance audits and program evaluations in nearly every field imaginable.

GAO and CIP

In recent years, GAO has provided Congressional testimony and performed numerous studies on Critical Infrastructure Protection. Some of the prominent themes in GAO's recommendations include public-private coordination; improved information sharing; defining roles, responsibilities, and relationships; and addressing pervasive vulnerabilities in federal information security. A list of some of GAO's critical infrastructure protection reports, testimony, and links follows.
(Continued, Page 10)

Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks
September 26, 2001
http://www.mipt.org/pdf/gao011168t.pdf

Information Sharing Practices That Can Benefit Critical Infrastructure Protection
October 2001
http://www.gao.gov/new.items/d0224.pdf

Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems
July 2002
http://www.coop-consulting.com/pdf/GAO_Report.p

Significant Homeland Security Challenges Need to Be Addressed
July 2002
http://www.gao.gov/new.items/d02918t.pdf

Efforts of the Financial Services Sector to Address Cyber Threats
January 2003
http://www.fbiic.gov/reports/gao-03-173.pdf

Challenges for Selected Agencies and Industry Sectors
February 2003
http://www.gao.gov/new.items/d03233.pdf

Information Security: Progress made, but Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures
April 8, 2003
http://www.iwar.org.uk/cip/resources/gao/d03564t.pdf

Congressional Agencies (Cont. from Page 9) The Congressional Research Service is the public policy research arm of the United States Congress. As a legislative branch agency within the Library of Congress, CRS works exclusively and directly for Members of Congress, their Committees and staff on a confidential, nonpartisan basis.

Congress created CRS in order to have its own source of nonpartisan, objective analysis and research on all legislative issues. The sole mission of CRS is to serve Congress. CRS has been carrying out this mission since 1914, when it was first established as the Legislative Reference Service. Renamed the Congressional Research Service by the Legislative Reorganization Act of 1970, CRS provides Congress with comprehensive and reliable analysis, research and information services that are timely, objective, nonpartisan, and confidential, thereby contributing to an informed national legislature.

The CRS staff comprises nationally recognized experts in a range of issues and disciplines. CRS analysts work directly with Congress on a daily basis to help the Congress identify, analyze, and formulate legislative proposals. They perform in-depth policy, legal, and procedural analyses; identify and assess policy alternatives and their implications; assist in framing legislative proposals; develop quantitative databases and analyses using the latest research tools and methodologies; identify and evaluate new research findings, data, and information sources; and deliver expert testimony before congressional committees. Their work takes the form of written analytical reports and confidential memoranda, educational seminars and workshops, and in-person briefings and telephone consultations. CRS also provides the Congress with a wide range of specialized reference and information services.

CRS and CIP

CRS has published research on critical infrastructure protection, including a 1998 report by John Moteff titled *Critical Infrastructures: A Primer*. This report, which no doubt served as an introduction to the field of CIP for many, described the work of the President's Commission as well as the details of PDD-63. More recently, another report by Mr. Moteff was published, *Critical Infrastructures: Background Policy, and Implementation*. This February 2003 report for Congress updated the 1998 report, including actions taken by the Bush administration before and after the September 11 terrorist attacks, and discusses the changes to Federal CIP efforts brought about by the creation of the Department of Homeland Security. Mr. Moteff also discusses the issues of information sharing, privacy vs. protection, and costs and priority-setting. ❖

Racial Profiling *(Cont. from Page 8)* to which random snipers are almost always white males, the police focused their attention on suspects fitting this stereotype. Duly shocked to find that the investigation had been based on a false premise, the Washington police chief memorably remarked: "We were looking for a white van with white people, and we ended up with a blue car with black people."[7] Not the least of the shortcomings in the Justice Department's new policy guidance is that it makes no effort at all to erect safeguards against repetitions of this sort of dysfunctional bureaucratic behavior. ❖

[1]Robert H. Bork, *Civil Liberties After 9/11*, Commentary, July-Aug. 2003, at 30.

[2]Milton Heumann & Lance Cassak, *Afterword: September 11th and Racial Profiling*, 54 Rutgers Law Review 283, 286-87 (2001); Jason L. Riley, *'Racial Profiling' and Terrorism*, Wall Street Journal, Oct. 24, 2001, at A22.

[3]See, *e.g.*, Michael Chertoff, Assistant Attorney General for the Criminal Division, Testimony Before the Senate Judiciary Committee Hearing on Preserving Freedoms While Defending Against Terrorism, Federal News Service, Nov. 28, 2001 [available at LEXIS, News Library, News Group File, A11].

[4]Here, and throughout, I use "race" as a shorthand for "race or ethnicity."

[5]*Whren v. United States*, 517 U.S. 806 (1996).

[6]*Grutter v. Bollinger*, 123 S. Ct. 2325 (2003).

[7]Craig Whitlock & Josh White, *Police Checked Suspect's Plates At Least 10 Times*, Washington Post, Oct. 26, 2002, at A1. For further detail, see Nelson Lund, *The Conservative Case against Racial Profiling in the War on Terrorism*, 66 Albany Law Review 329 (2003).

Demand, Not Supply *(Cont. from Page 5)* The implementation of retail demand response in the electric power industry would provide a wide range of benefits including lower capital and energy costs, fewer critical power spikes, consumer control over electricity prices, and the environmental benefits gained by empowering consumers to use electricity more wisely. Despite Milton Friedman's admonition, by adding increased flexibility to the electricity grid and sparing critical infrastructure from shutdown, demand response creates a more efficient and resilient economic structure while providing more robust security as a free lunch.

Mr. Smith, on leave at the University of Alaska Anchorage, is professor of economics and law at George Mason and the 2002 Nobel laureate in economics. Ms. Kiesling is senior lecturer in economics at Northwestern and director of economic policy at the Reason Foundation.

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by LegalNet Works, Inc. on behalf of the CIP Project. Formed in 1996, LegalNet Works Incorporated focuses on the development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. LegalNet consults both government and industry officials on legal and policy reform in these complex areas.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/archives/cipp-report-l.html.