5th Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 29-30, 2002

Chemical Plant Security: National Security for the Chemical Industry

William A. Anderson, II
Thomas C. Poindexter[1]
Winston & Strawn
1400 L Street, NW
Washington, DC 20005, USA
(202) 371-5986, wanderso@winston.com

I. Introduction

The events of September 11, 2001, have given new urgency to warnings that terrorist strikes could transform chemical plants into weapons of mass destruction. Of the estimated 15,000 chemical sites[2] subject to EPA's Risk Management Plan ("RMP") requirements[3] under section 112(r) of the Clean Air Act,[4] roughly 3,000 report that there are populations of 10,000 or more people within their calculated "vulnerability zone," and over a fifth of those, or some 700, report that 100,000 people are within that defined zone.[5] At perhaps 123 sites, it includes over a million people each.[6] The Army Surgeon General has estimated that a well-planned terrorist attack against a single chemical facility near a densely-populated area could kill or injure as many as 2.4 million people.[7]

These observations have accelerated the call for action, and have spawned sharp disagreement over what that action should be. Disagreement threatens paralysis; haste, inappropriate and ineffective measures. The reaction to September 11 has found familiar opponents contradicting not only each other, but even themselves. The disagreements have been in two main areas: the need for more mandatory requirements and whether public availability of RMP information affords what one observer dubbed "terrorism for dummies."[8]

On the need for further measures, the chemical industry rushed to issue non-binding site security guidelines in October 2001,[9] only to decide in June 2002 to make vulnerability assessments mandatory for members of the American Chemical Council ("ACC").[10] EPA initially said that additional regulations were unnecessary.[11] However, EPA recently announced that it was sending a package of proposed regulations to the Office of Management & Budget for review prior to publication in the *Federal Register*.[12] Some have called for addressing the risk levels by reducing volumes of chemicals on site by reliance on just-in-time deliveries,[13] while others have pointed out that this practice results in greater risk: it disperses the chemicals to unprotected transportation terminals and rail sidings.[14] Additionally, the Senate Committee on Environment

& Public Works has passed a bill, S. 1602, that would extend the "general duty" of covered RMP facilities to require, on pain of criminal liability, all measures necessary to prevent criminal attacks on their plants.[15] The Ranking Minority Member of that Committee objected that this bill "would put the government in charge of chemical manufacturing and chemical manufacturers in charge of fighting terrorism."[16]

The disclosure or protection of critical information has been no less contentious. EPA and the Administration have been withdrawing information from the public domain and taking down Internet sites that posted chemical plant information.[17] At the same time, Greenpeace's Toxics Campaign and the Right-to-Know Network have been actively promoting the release of critical "worst-case scenario" information, or off-site consequences analysis ("OCA") data from RMPs.[18] Greenpeace posted on the Internet OCA data from three Dow Chemical plants, and it plans to publish similar information about chemical plants near New York, Philadelphia and Wilmington, DE.[19]

The President of the American Chemical Council says that the $450 billion U.S. chemical industry[20] is one of the safest industries in the world.[21] As safe as the industry may be, there is clearly room for improvement. The National Response Center logs approximately 25,000 reportable spills and releases of oil or hazardous chemicals annually.[22] Not all of these reported spills and releases are within the chemical industry, and some involve oil rather than chemicals, but many of them do occur in the chemical industry. When data from several sources are combined, they indicate that in 1998 chemical production, handling and usage resulted in over 100 deaths and almost 5,000 injuries in the U.S.[23] During that same year of 1998, by comparison, the 104 licensed commercial nuclear power reactors in the $44 billion nuclear power industry[24] reported among them a total of one release exceeding Nuclear Regulatory Commission criteria at 10 C.F. R. § 50.73(a)(2)(viii).[25] This comparison suggests that the nuclear industry may hold some lessons for those trying to decide how the threat of terrorism against chemical plants should be addressed. Of course, chemical plants are far more varied in scale and process than commercial nuclear reactors and few can compare to the asset or revenue value represented by a functioning power reactor, but there are useful lessons to be drawn from the experience of the nuclear industry.

This paper reviews briefly the current status of process safety regulation and programs in the chemical industry and describes publicly-available pending proposals for change. It then considers the present state of the debate on community right-to-know versus chemical information security and a legislative proposal to restrict availability of chemical-risk information. The paper then describes the comparable security programs in place in the nuclear industry and some important principles that have been established there. It concludes with recommendations of elements and approaches that we believe can advantageously be transferred to the chemical industry. An underlying premise of the paper is that the $450 billion chemical industry is an asset that is vital to the national security and worth protecting from the threats, not only of terrorists, but also from the zealots who would kill it to save us. As the industry itself must show, safety does not require such sacrifice.

II. Site Security Measures

A. Current Standards

Current site security standards in the chemical industry are a combination of regulatory requirements and more-or-less voluntary industry standards.

1. Regulatory Requirements

The Occupational Safety & Health Act ("OSHA Act") imposes upon all covered employers a general duty to keep the workplace "free from recognized hazards that are causing or are likely to cause death or serious physical harm to . . . employees."[26] In addition, pursuant to provisions enacted as part of the Clean Air Act Amendments of 1990 the Occupational Safety & Health Administration ("OSHA"),[27] OSHA has also promulgated chemical process safety management ("PSM") standards[28] "to protect employees from hazards associated with accidental releases of highly hazardous chemicals in the workplace."[29] The stated purpose of those PSM standards is to set requirements "for preventing or minimizing consequences of catastrophic releases of toxic, reactive, flammable or explosive chemicals."[30]

The OSHA PSM program begins with the compilation of information about hazards posed by the particular chemicals present above threshold quantities, the process technology, and the process equipment.[31] It proceeds to a process hazard evaluation that considers process design and technology, operations and maintenance, abnormal activities and procedures, training programs, emergency preparedness and response and other elements.[32] The PSM program must itself include written operating procedures, employee training programs, pre-startup reviews where appropriate, integrity of equipment, emergency response planning and administrative controls including hot work permits, management of change procedures and compliance audits.[33] Aside from those provisions that are specifically designed to mitigate the effects of catastrophic releases, however, the PSM standards do not address risks or hazards from the threat of terrorism. They are focused on the prevention of chemical releases "that could occur as a result of failures in process, procedures or equipment."[34]

The same 1990 Amendments that called for PSM standards also added to the Clean Air Act a new § 112(r)[35] to require programs to prevent, and to minimize the effects of, accidental releases of hazardous chemicals.[36] Congress borrowed the concept of the "general duty" clause from the OSHA Act and extended it to create and impose a general duty on chemical facility owners to identify hazards, to design and maintain a safe facility, and to minimize the consequences of any accidental releases.[37] The general duty for a safe facility design includes "taking such steps as are necessary to prevent accidental releases."[38] Pursuant to § 112(r), EPA promulgated comprehensive Chemical Accident Prevention ("CAP") regulations.[39] The CAP program takes PSM requirements and extends them offsite to public receptors.[40] It applies to all facilities that have on site more than a threshold quantity of a regulated substance.[41] The regulations divide covered facilities into three tiers, based on the offsite effects of prior releases, distance to public receptors, industrial classification, applicability of the OSHA PSM standard, and status of emergency response plans.[42] Chemical plants generally fall into the third category subject to the most rigorous requirements ("Program 3"), due to their industry category and applicability of the OSHA PSM standard.[43] The core requirement of the EPA CAP regulation, which applies to all covered facilities, is the requirement for a risk management plan ("RMP").[44] The RMP must register all covered processes, provide detailed data on each and present a hazard assessment that includes a worst-case release scenario and off-site consequence analysis ("OCA").[45]

The RMP must describe the worst-case accidental release, defined to mean simply "an unanticipated emission of a regulated substance or other extremely hazardous substance into the ambient air."[46] Although this definition could be broad enough to include a release occasioned by a terrorist attack, the focus of the rule is on spills and releases caused by inadvertent events, mishandling, or failure of process equipment components such as piping, fittings, vessels or valves, not by intentional terrorists strikes.[47]

2. Industry Voluntary Standards

The chemical industry is involved in several initiatives to address chemical site security issues. In January 2002, the American Chemistry Council ("ACC") made enhanced security measures mandatory for all of its approximately 180 member companies.[48] In June 2002 the ACC went even further, making vulnerability assessments pursuant to a Department of Justice ("DOJ") methodology or an equivalent methodology, mandatory for all of its members.[49] Although the ACC's members account for over 90 percent of the nation's chemical products by volume, its members represent only 10 percent of the approximately 15,000 chemical facilities in the U.S.

a. The Site Security Guidelines for the Chemical Industry ("SSG")

Through its trade associations, the chemical industry issued its first post-9/11 voluntary standards on October 23, 2001. The ACC, along with the Chlorine Institute ("CI") and the Synthetic Organic Chemical Manufacturers Association ("SOCMA"), issued Site Security Guidelines for the U.S. Chemical Industry ("SSG").[50] The SSG were developed by chemical industry experts and company security professionals to help chemical companies build on their existing site security programs. The SSG outline important elements of security programs and encourage managers to tailor the suggested security practices to best fit their particular site. They do not provide an exhaustive list of security considerations nor address transportation security issues. They are a tool, not a standard.

The principle areas addressed in the SSG are: (1) risk assessment and prevention strategies; (2) management issues; (3) physical site security issues; (4) employee and contractor security issues; and (5) information, computer and network security. Sample security policies are included in the SSG as a helpful resource for companies devising their own security policies. But the elements of the site security plan provided by the SSG do not claim to be only an in-depth discussion of these areas, but merely a brief description of each and the issues to be assessed. The SSG points the reader to the potential of different solutions and strategies.

The SSG describe the types of risk assessments that a company should perform, including assessments in the areas of chemical hazards, process hazards, physical hazards, security issues and mitigation possibilities.[51] Once the threats, vulnerabilities and related consequences are assessed in these areas, the SSG suggest prevention strategies for consideration in addressing these issues.

In line with the approach in EPA's CAP rule, the SSG suggest that the responsibility for security management at a chemical facility should be handled by one person.[52] This person would have plenary responsibility for security management functions. He would determine site security policies, increase employee and contractor awareness and training regarding security issues,

establish and coordinate cooperative relationships with law enforcement and the community regarding security matters, develop and oversee incident reporting protocols, handle security breaches and their investigation as well as emergency response procedures, and periodically review the policies and procedures in each of these areas.[53]

The physical site security aspect of the SSG is concerned with protecting a facility and its people, property and physical information sources from outside attack and infiltration.[54] This involves security efforts to manage and control access to the site, to protect the perimeter of the site, to deploy and use intrusion detection methods, the use of security officers, and other measures.[55]

The SSG note that employees and contractor personnel may present site security threats. Therefore, hiring and termination policies should be established with this in mind.[56] These policies should include pre-employment and background screening as well as voluntary and involuntary termination procedures.[57] Workplace violence prevention policies and measures should also be established.[58]

The SSG recommend that information, computer, and network security measures should be in place to prevent any information about site operations contained in documents, computers, and networks, or transmitted by voice from being intercepted or accessed.[59] The SSG suggest an assessment of critical information, an assessment of threats, a vulnerability analysis, a risk analysis, and the use of countermeasures to address the risks and threats determined.[60] The results of this analysis should be reflected in company policies regarding how information is labeled, stored, conveyed, and accessed in all information communication and storage mediums.[61] Regardless of how lawful a company may be, however, information submitted to the government may be disclosed through the Freedom of Information act ("FOIA"), unless it is exempt. And no element of the SSG is mandatory for members of ACC, SOCMA or the CI.

b. The Responsible Care Security Code ("RCSC")

The SSG build upon the ACC's broad Responsible Care initiative for its members, which encompasses the areas of health, safety and the environment. The Responsible Care initiative was established almost 15 years ago and has gained wide acceptance. The ACC is scheduled to implement changes to the Responsible Care initiative beginning in January 2003. On the security front, on June 5, 2002, the ACC board approved the Responsible Care Security Code ("RCSC") in order to continue the enhancement of industry-wide workplace safety and site security in the post-9/11 world.[62]

The RCSC contains obligations that include the following: (1) senior leadership commitment to continued improvement evidenced by published policies, the provision of the necessary resources, and accountability; (2) training and drills for employees, contractors, customers and suppliers; (3) decision-making processes that include consideration of using inherently safer approaches like materials substitution and process changes; (4) communication and information exchange with stakeholders on security issues; (5) proper investigation, evaluation, analysis, response, reporting and corrective action for security threats and incidents; and (6) internal audits for the continual improvement of processes.

ACC members adhering to the standards have prioritized their facilities into four tiers of risk and have assessed security at all their facilities, according to risk prioritization. Once the security measures identified in the assessments are implemented by company members, the implementation of the security measures will be verified by independent third parties. The methodologies to be used in assessing chemical sites must be the methodologies developed by either the Sandia National Laboratories, the Center for Chemical Process Safety, or an equivalent approach.

c. Chemical Sector Information Sharing and Analysis Center ("ISAC")

The ACC and the National Infrastructure Protection Center ("NIPC") signed an agreement on April 24, 2002 in support of the Chemical Sector Information Sharing and Analysis Center ("ISAC"), which has just been established and is based in Washington, DC at the FBI headquarters. This partnership agreement between the public and private sectors will facilitate the sharing of key security-related information between the NIPC agencies and chemical companies. Participation in ISAC is open to ACC members, members of other chemical industry associations, and other groups related to the chemical sector. Participation is offered free of charge.

The NIPC, established in 1998, is the federal government's center for threat assessment, warning, criminal and security investigation and response. NIPC is charged with the protection of the nation's essential systems and services. The electronic communication network provided under ISAC will facilitate the quick exchange of information and analysis between NIPC and chemical companies regarding critical threats and incidents. ISAC will also provide chemical sites and related transportation facilities with timely information and alerts about possible threats so that preemptive measures can be employed. Additionally, ISAC will provide experts to the NIPC for consulting purposes as they are needed.

The ACC's 24 hour emergency response communications center, the Chemical Transportation Center ("CHEMTREC"), will operate ISAC. CHEMTREC has 30 years of experience and resources to deal with emergency responders, manufacturers, distributors, transporters and local communities. Through CHEMTREC, companies can report any incidents directly to the NIPEC.

d. The Chemical Facility Vulnerability Assessment Methodology ("VAM")

On June 17, 2002, the Department of Justice ("DOJ") issued the initial version of the Chemical Facility Vulnerability Assessment Methodology ("VAM").[63] The final version is forthcoming.[64] The VAM is a security assessment tool that provides a methodology for assessing the security of chemical facilities. The tool is geared towards addressing the threat of terrorist or criminal activities or attacks that may have a nationally significant impact or may cause a release of hazardous chemicals that injures facility employees or community members.[65] The use of the VAM is focused on chemical facilities required to submit risk management plans, but the tool was developed to be useful in preventing impacts of a lesser magnitude as well.[66]

The prototype VAM was developed by the Office of Justice Programs' ("OJP") National Institute of Justice ("NIJ"), which is the DOJ's agency for research and development, and the Department

of Energy's Sandia National Laboratories ("SNL").[67] SNL boasts expertise in security and counter terrorism and extensive experience in protecting nuclear weapons and radioactive materials.[68] The ACC had been waiting for the VAM to be released.[69] Now this DOJ tool, or an equivalent approach, can be used in order to satisfy the mandatory security enhancements required of all ACC members.[70]

The VAM compares relative security risks.[71] Risk is analyzed as a function of 3 factors: (1) the severity of the consequences of an event, (S); (2) the likelihood of attack by an adversary, (L_A); and (3) the likelihood that an adversary would be successful in causing a catastrophic event, (L_{AS}).[72] Recommendations are then made for measures that can be developed to reduce any risks determined to be unacceptable under this analysis.

The VAM calls for a 12-step process which is: (1) screen for the need for a vulnerability assessment; (2) define the project; (3) characterize the facility; (4) derive severity levels; (5) asses threat; (6) prioritize cases; (7) prepare for analysis; (8) survey the site; (9) analyze system effectiveness; (10) analyze risk; (11) make recommendations; and (12) prepare the final report.[73]

The first step of the VAM is to determine whether a vulnerability assessment is needed for a chemical facility or not, based on the potential consequences of a terrorist attack on that facility.[74] If an entity has several chemical facilities, the screening step includes a prioritization of those facilities that are determined to need a vulnerability assessment into one of four levels, based on the number of people that might be affected by the Worst-Case Scenario from the toxic substances RMP.[75] If the loss of a facility will have a national impact, the vulnerability assessment information may need to be classified.[76] If the facility has a total onsite inventory of chemicals covered under 40 CFR 69.30 that is at or above threshold quantities, a vulnerability assessment is probably needed in order to avert unacceptable off-site consequences that may result from a terrorist attack.[77] Vulnerability assessments should be conducted beginning with the facilities with the higher priority ranking, with number one being the highest priority ranking.[78]

After the screening process, the second step is to define the vulnerability assessment in terms of the characteristics of the facility or facilities being assessed, which includes defining the purpose of the assessment, the tasks to be completed, the resources and the team to be used as well as the schedule to be followed.[79]

The third step is to characterize the facility's operating states and condition which requires gathering a vast amount of information and developing a thorough description of the facility itself, the processes used in the facility, and the existing physical security features at the facility.[80] During this step, a list of reportable chemicals for undesired events must be made. The VAM provides a Facility Characterization Matrix to help organize security factors for each step in a facility's processes, which helps determine the risks involved in each processing node and aids in their prioritization in order of most to least critical.[81] Process flow charts must also be developed.

The fourth step is to determine the severity of the consequences of each undesired event at each facility, the "S" factor of analysis.[82] The VAM provides a chart of severity levels that range from one to four with one being the most severe.[83] Each undesired event should be assigned a severity

level based on the consequences involved.[84] Chemical facilities that are required to submit RMPs will most likely have a severity level of one.[85]

A description of the threat must be developed before a vulnerability assessment can be made. In order to perform this fifth step, information on the threat must be obtained on the type of adversary involved and the adversary's motivations, capabilities, and potential actions.[86] Adversaries are generally grouped into three categories: (1) outsiders, including terrorists, criminals, extremists, gangs or vandals; (2) insiders, including employees taking both voluntary and involuntary actions; and (3) outsiders in collusion with insiders.[87] The information gathered on these potential adversaries forms the basis of adversary scenarios which are developed and used to predict a spectrum of threat and are assigned a "likelihood of attack" level on a scale of one to four based on past statistical data, the "(L_A)" factor.[88]

The sixth step is to prioritize cases by developing a matrix that combines the likelihood of attack by levels, the "(L_A)" factor, versus the severity of the consequences by levels, the "S" factor, to derive the likelihood and severity factor, (L_S), ranking matrix.[89]

An analysis of the site's protection system effectiveness is the seventh step.[90] A site's physical protection system should be able to detect any adversaries and then delay them long enough for a response force to arrive at the point of interception and neutralize them.[91] A series of protective devices should be in place to deter an adversary in their mission.[92] The effectiveness of these devices and measures will determine the likelihood of adversary success factor, (L_{AS}).[93] A priority ranking matrix should then be developed comparing this factor to the likelihood of attack and severity factor, (L_S).[94] This matrix is later used to estimate risk levels. Mitigation features which reduce the consequences of an undesired event, like automatic system shut down, can be used to address areas where the risk of undesired events is high or the effectiveness of protection systems is low.[95]

In step eight, the information and exhibits developed in the previous steps is reviewed by the entire assessment team for accuracy and is verified.[96] A walk-through site survey is conducted as a part of this evaluation.[97]

Step nine requires analyzing and estimating the effectiveness of both physical and process protection systems and features to assess their effectiveness in avoiding undesired events.[98] An additional estimate of mitigating forces is made if the undesired event cannot be prevented through physical and process control systems.[99] Adversary attack and success scenarios are analyzed as a part of these estimates.[100]

Step ten is a risk analysis based on all three factors, likelihood of attack, likelihood of success, and severity of consequences, which were developed in steps one through nine.[101] Risk levels, ranging from one to four, are established for each adversary group and undesired event based on the previously determined risk levels for these three factors.[102] Risks categorized higher than risk level four, risk levels one through three, should be decreased. Recommendations for decreasing these higher risks are made in step eleven. These risk reduction recommendations include recommendations on low-cost, high-return upgrades in the areas of adversary detection and delay, response, mitigation, and safety features that better address vulnerabilities.[103]

Vulnerabilities that all undesired events have in common should be addressed first.[104] Risk reduction upgrades should provide balanced protection throughout the site and protection features should be layered in order to delay the adversary.[105]

The twelfth and final Step is the preparation of a final report which summarizes the results of the previous eleven steps of chemical site assessment and analysis.[106]

B. Proposed Approaches to Chemical Industry Safety

1. Administration/Office of Homeland Security Proposals

On October 8, 2001 President Bush issued the Executive Order Establishing the Office of Homeland Security ("OHS") and the Homeland Security Council.[107] Their functions are outlined to include addressing the hazards posed by chemicals, specifically, (1) the coordination of the development of monitoring protocols for the detection of a chemical hazard release; (2) the coordination of the containment and removal of chemicals in the event or threat of a terrorist attack; and (3) the coordination of efforts to mitigate the effects of a terrorist attack should one take place.[108]

The Homeland Security Presidential Directive-3 was issued by President Bush on March 12, 2002 establishing the Homeland Security Advisory System ("HSAS")

> to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. Such a system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert. [109]

The HSAS is binding on the executive branch but is voluntary for all other levels of government and the private sector.[110]

The HSAS consists of five color-coded Threat Conditions progressing from low threat condition to high threat condition.[111] The risk levels represent both the probability that an attack will occur and the potential gravity of that attack.[112] Threat Conditions will be determined by the Attorney General in consultation with the Assistant to the President for Homeland Security and may be assigned for the nation as a whole or for a particular geographic area or industrial sector.[113] The assigned Threat Conditions will be reviewed regularly and adjustments made as appropriate.

Each Threat Condition has a correlating set of Protective Measures that are to be implemented to reduce vulnerability to a terrorist attack or increase the ability to respond during a heightened Threat Condition. These Protective Measures are cumulative as the Threat Condition level increases in severity. The Low Threat Condition level includes the Protective Measure of

institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks and that all reasonable measures are taken to minimize any vulnerabilities.[114] Because the Protective Measures are cumulative, all threat levels contain this element of vulnerability assessments.[115]

The ACC sent Attorney General John Ashcroft a letter dated April 26, 2002 offering its support and making five recommendations for the HSAS.[116] The first recommendation was that the OHS should "consider a formal process to integrate known interdependencies into the HSAS" so that critical information can be provided and shared amongst interdependent industries, within the chemical business, for example.[117] Secondly, the ACC recommended that a vulnerability assessment system be used instead of a threat-based system for the chemical industry and other capital-intensive infrastructure sectors.[118] The ACC also recommended that the OHS retain the response flexibility in the proposed HSAS that allows the private sector to respond as appropriate to each increased threat level.[119] Fourthly, the ACC encouraged the support of communication programs like ISAC that facilitate the exchange of information between government and the private sector.[120] Lastly, it urged the OHS to designate an agency to be the lead organization.[121]

2. The Corzine Bill, S. 1602

In the wake of September 11, Senator Jon Corzine introduced S. 1602 on October 31, 2001. The Chemical Security Act of 2001 was introduced to address the threat of terrorist or criminal attacks on chemical sources and facilities.[122] On July 25, 2002 the Senate Environment and Public Works Committee unanimously approved a version of that bill.[123]

a. Site Security Measures

The bill would require EPA, to promulgate regulations within one year to place certain chemical facilities into a "high priority" category based on the severity of the threat posed by an accidental or criminal release from that chemical facility.[124] One year later, EPA would have to implement regulations that would require every owner and operator of a high priority category chemical source to conduct vulnerability assessments, identify potential hazards, and take preventative measures to control and minimize the possible consequences of any related release.[125]

The bill would impose on facility owners and operators a general duty to prevent terrorists attacks directed at them. Specifically, they would be required to: (1) use appropriate hazard assessment techniques to identify the hazards that may be posed by any release by accident or by criminal act; (2) prepare a plan of actions and procedures to prevent any accidental or criminal release by ensuring safer design and maintenance of the chemical source; and (3) minimize the potential consequences of any such release that may occur.[126] Harm arising from a terrorist attack would show that the owner of the facility violated its general duty. Since the requirement is backed by criminal penalties, this feature of the bill has prompted the industry to object that it would make criminals out of victims of terrorism.[127]

All plans, due one year after implementation of the regulations, would be reviewed by the EPA and the Homeland Security Department.[128] Facilities would be required to comply with these plans within 18 months of submitting them to the EPA.[129] Once approved, compliance with these plans would be certified by the EPA.[130] Both the vulnerability assessments and the plans

would be required to be reviewed every three years and would be considered classified.[131] The regulations would be reviewed and revised within five years of promulgation.[132]

The bill gives EPA the authority to do what it deems necessary, including administrative and court orders, to address any danger or threat of a potential accidental or criminal release that it determines to be an imminent and substantial danger to the public health, welfare or environment.[133] The same authority applies should a chemical source fail to provide requested information or access to covered premises.[134] The EPA would also have the power to require any person to keep records, make reports, provide information, and grant entry to any chemical source.[135] The bill would make records and information obtained by the EPA, excluding information pertaining to national security and trade secrets, available to the public.[136] Civil and criminal penalties would be available for violations of the Act.[137]

b. The Chemical Industry's Reaction

The chemical industry maintains that federal imposition of standards is unnecessary since it is already engaging in its own self-regulation. Like S. 1602, ACC initiatives and suggested methodologies are aimed at the same goals of reducing and counteracting threats posed by accidental or criminal acts directed at chemical sites. The ACC argues that it has a long history of meeting difficult deadlines for establishing measures to protect the safety of employees, neighboring communities and the environment and that the federal government should accept the industry's security initiatives instead of trying to impose similar ones by law.[138]

The ACC argues that use of its industry standards will accomplish chemical security goals faster and more effectively than enactment of S. 1602.[139] The adoptation of S. 1602 may halt or delay chemical companies beyond 2005 in their progress towards greater site security under ACC initiatives, while they await new federal regulations geared to accomplish the same essential goals as the ACC initiatives.[140] However, the substitute version of S. 1602 passed by the Senate Committee tries to avoid this problem by providing that facilities would be permitted to submit plans to the EPA for a determination on compliance with the Act before the regulations were published.[141] If the plans are determined to be in compliance with the law, no further revisions of the assessments or plans would be required.[142]

c. The Administration's Views

In May 2002 the EPA was drafting legislation that would contain some of the requirements found in S. 1602, but by June EPA had changed its position and decided to issue guidelines and not attempt to give them the force of law.[143] By July, the Bush Administration was stating that it would generally prefer voluntary measures and hoped to avoid legislation as a means to achieving chemical site security, but it had not expressed an official position on S. 1602.[144] More recently, an EPA official acknowledged that the EPA does have a problem with some of the provisions in the proposed legislation, including S.1602 and its companion bill H.R. 5300.[145] At a July 10, 2002 Senate Environment and Public Works Committee hearing on the proposed Office of Homeland Security, the director of Homeland Security, Tom Ridge, agreed that the chemical industry acknowledges its responsibility to protect chemical facilities, employees and community.[146] However, he went on to state that the administration is in favor of avoiding legislation as the means of enhancing chemical site security, but "we need to keep our options

open."[147] On the same day a top White House officially also proclaimed the administration's desire to avoid legislation.[148]

By early August, however, an agency official reportedly stated that EPA plans to issue regulations to require chemical facilities to perform vulnerability assessments and to make "mandatory fixes."[149] EPA is still considering the classification of facilities into tiers in order to prioritize the facilities that pose a greater risk.[150] While a proposed rule is expected in the near future there are doubts about EPA's authority to adopt such a rule.[151] Reportedly, EPA is considering using the same compliance milestones contained in the ACC's recently-adopted Security Code.[152]

The EPA official said the Agency moved away from voluntary security measures and toward federal regulation because it wants to ensure that the entire industry is participating.[153] The official acknowledged the ACC's efforts to address security needs but stated that approximately 15,000 facilities are at risk and ACC members represent only 1,000 to 1,500 of them.[154] For one, EPA does not have the resources to certify all required assessments, therefore EPA would not include that provision in its regulations.

d. Other Views

Some committee Republicans still have concerns regarding some of the bill's provisions even though it was passed unanimously.[155] Senator James Inhofe (R-Okla.) expressed his concerns that the EPA does not have the capacity or the expertise to review the security plans and that those assessments and plans may not be secure after they are received by the EPA.[156] The Committee approved an amendment offered by Senator Bond to limit access to assessments and plans to authorized individuals, such as local emergency planners.

3. The Companion House Bill, H.R. 5300

The companion bill to S. 1602, H.R. 5300, the Chemical Security Act of 2002, was introduced by Representative Frank Pallone Jr. on July 26, 2002. Like S. 1602, this bill would require EPA, to promulgate regulations within one year of passage to place certain chemical facilities into a "high priority" category based on the severity of the threat posed by any unauthorized release from that chemical facility.[157]

Also within one year after the enactment of H.R. 5300, EPA would have to implement regulations that would require every owner and operator of a high priority category chemical source to consult with local law enforcement, first responders, and employees in conducting vulnerability assessments.[158] Hazards posed by an unauthorized release would be required to be identified using appropriate hazard assessment techniques.[159] A prevention, preparedness and response plan would also be required to be prepared in light of the assessments of vulnerability and hazards.[160] This plan would have to include safer design and maintenance actions and procedures in order to reduce the potential hazards identified.[161] The head of the Department of Homeland Security would supply chemical facility owners and operators with relevant threat information according to the assessments and plans prepared by that facility.[162] EPA would have to review and revise these regulations, if necessary, within five years of promulgation.[163]

Owners and operators of chemical sources designated "high priority" would be required to certify to the EPA that they conducted assessments and completed prevention, preparedness, and response plans according to regulations.[164] Written copies of the assessments and plan would have to be submitted to the EPA.[165] Between three and five years after submitting these to the EPA, both the vulnerability assessments and the plans would have to be reviewed by the owner or operator of the chemical source to assess the adequacy of the assessment or plan.[166] The owner or operator would then have to certify this review to EPA, as well as any changes deemed appropriate.[167]

Under H.R. 5300, information submitted to EPA would be exempt from production to the public under Title 5 section 552 of FOIA.[168] Additionally, within a year of enactment, EPA would be required to develop the necessary protocols to protect copies of the assessments and plans it received under the measure. The protocol must provide that information be kept in a secure location, that only EPA-designated persons would have access to it, and that no copies be made available to anyone else.[169]

EPA would be required to review all assessments and plans submitted under the Act in order to determine the compliance of the assessments and plans with the regulations.[170] EPA's compliance determination would have to be made in writing and include a checklist of the four elements of a safer design and maintenance that are outlined in the bill.[171] Determinations are to be a decision by the EPA that (1) the assessment or plan does not comply with regulations (2) a threat exists beyond the scope of the plan submitted; or (3) the current implementation of the plan is insufficient to address the results of the assessment or a threat. The EPA is to establish a schedule for the review and certification of assessments and plans which is to be within three years of the deadline for submission of such assessments and plans.[172]

In order to avoid delaying implementation of the CAP's ACC program, chemical sources would be allowed to comply with the regulations even before the proposed regulations are published.[173] EPA could review assessments and plans and determine compliance with the Act's requirements.[174] The EPA may certify compliance if the assessments and/or plans submitted were determined to be in compliance with requirements.[175] If they were not in compliance, EPA could require revisions to any assessment or plan submitted.[176] Chemical sources would be required to bring their assessments and plans into compliance with regulations with 30 days of receiving notice that their assessment or plan was not in compliance, otherwise, EPA could issue an order directing the source to comply.[177] The EPA may also issue a compliance order if a chemical source had not complied with a request for entry or information.[178]

If the Office of Homeland Security were to determine that a terrorist threat existed outside of a chemical source's plan, or that current implementation of a source's plan were insufficient, it would have to notify the source.[179] If the response by the chemical source were insufficient after notification, the Head of Homeland Security would also have to notify the source.[180] The EPA or Attorney General would be able to take any necessary measures to protect the public health or welfare.[181]

EPA would have the same rights of entry and access to information as provided in S. 1602.[182] Administrative, as well as civil and criminal, penalties would be available.[183]

3. A Comparison of S.1602 and H.R. 5300

Some basic provisions of S. 1602 and H.R. 5300 are similar. Both provide for the designation of chemical facilities into a "high priority" category based on the threat posed, vulnerability assessments for these "high priority" facilities, the use of appropriate hazard assessment techniques, and the development of a plan of actions and procedures to prevent and address the threat of chemical release.[184] Differences that make H.R. 5300 preferable to S. 1602 are highlighted in Part V of this paper.

III. Information (In)Security Measures

A. Protection of Sensitive Information

1. EPA's approach under Section 112(r) of the Clean Air Act: "Terrorism for Dummies"?

Congress stipulated in § 112(r) of the Clean Air Act that the RMPs it required "shall be available to the public under [§ 114(c)]" of the Clean Air Act.[185] Section 114(c) provides broadly that "any reports, records or information" obtained by EPA "shall be available to the public."[186] The only exception is for information that EPA determines "would divulge methods or processes entitled to protection as trade secrets."[187] Consequently, as it developed and issued the § 112(r) regulations, EPA communicated its intent to make RMPs, including the OCA information they contained, publicly available on the Internet.[188] Not only was that action consistent with the statute, but it would further the general public interest in communities' right- to-know of chemical hazards, according to EPA's reasoning.[189]

The chemical industry and law enforcement agencies, notably the FBI, raised objections that the OCA information could provide handy blueprints for terrorism.[190] They raised grave concerns over posting that information on the Internet, where it could be accessed anonymously from anywhere in the world. As a result of these objections and similar concerns, EPA omitted the OCA information from the RMPs that it nevertheless proceeded to post on the Internet. Yet the OCA information remained available in electronic format and could be obtained under the Freedom of Information Act.[191] And those who obtained it could themselves readily post it on the Internet.

Congress enacted a one-year moratorium on access to the OCA information under FOIA in the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act ("CSISSFRA").[192] It directed the President, within one year, to assess the relative risks and benefits of making the full OCA information publicly available and to decide how best to make that OCA information available to the public.[193] It spelled out particular requirements and limitations on the methods and extent of access to be provided.[194]

Pursuant to the delegation of this authority, EPA and the Department of Justice jointly proposed and published final regulations within that one-year period.[195] Those regulations provided for OCA information not to be posted on the Internet, but to be made available to the public upon request at 50 reading room locations to be established by EPA around the U.S. EPA and DOJ found that other information available on the Internet did not pose the same risk as OCA information, because it did "not furnish the type of targeting data (such as the distance a

chemical release would travel and the population that lives within that area) that could be used to plan terrorist events."[196] The rule provides for "read-only" access by any individual to paper copies of OCA information on up to 10 facilities per month, without regard to location.[197] In addition, an individual may access OCA information for any number of facilities in the vicinity of his home or work. In addition, the rule encouraged designated local and state emergency planning and response authorities to make paper copies of OCA information available to the members of the local community on a "read-only" basis.[198] Thus EPA and DOJ sought to assure and advance the community's right to know.

It is not at all clear that the community wanted to know. During the 21 months that EPA's 50 reading rooms around the country made copies of OCA information from the § 112(r) RMP's available to the public, there were 33 visits to all of them combined, and 25 of those were to the Washington, D.C. reading room.[199] That means the other 49 saw 8 visitors altogether.

2. Other Approaches to National Security Information

a. Classified National Security Information

Established legal doctrine protects from the disclosure of information that is related to the national security. Despite its general thrust toward the disclosure of information held by the government, the Freedom of Information Act,[200] exempts from disclosure information authorized by an Executive Order to be kept secret "in the interest of national defense or foreign policy."[201] In keeping with the tenor of the times, the current Executive Order governing classified National Security Information[202] represented a liberalization over its predecessor.[203] Yet it recognizes that

> [T]hroughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions and our participation within the community of nations. Protecting information critical to our nation's security remains a priority. . . . [D]ramatic changes have altered, although not eliminated, the national security threats that we confront.[204]

Unfortunately, the current Executive Order does not reach as far or wide as the "dramatic changes" in national security threats it recognizes.

The Executive Order extends to "classified national security information" or just "classified information," for short.[205] The determination depends upon a decision by a duly-designated "classification authority"[206] that unauthorized disclosure of the information would result in "damage to the national security." That term is defined to mean

> harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value and utility of that information.[207]

Information that could facilitate terrorist attack on chemical plant targets obviously could result in harm to the national defense. Of the specific classes of information that may be classified, those most germane to chemical plant RMP data and vulnerability analyses would be: (1)

scientific, technological, or economic matters relating to the national security; and (2) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.[208]

Although chemical plants and their vulnerabilities may be relevant to the national security, and the disclosure of information about them may result in damage to the national security, that information may not be eligible for protection as "classified" under the current Executive Order. Its protection is limited to information that is "owned by, produced by or for, or is under the control of the United States Government."[209]

b. The State Secrets Privilege

In addition to protection from disclosure by the Executive Order and statutes,[210] national security information is protected from discovery in litigation by the judicially-created "state secrets privilege." The modern version of this doctrine was set forth by the United States Supreme Court almost 50 years ago in *United States v. Reynolds*.[211] If it is properly invoked, this privilege allows the Government to withhold information from discovery if "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged."[212] Where the privilege applies, it is absolute. It prevails, even where it completely prevents a litigant from proving its case.

In *Kasza v. Browner*,[213] for instance, the widow of a former employee at an Air Force installation had brought a citizens' suit for alleged hazardous waste violations.[214] The Air Force invoked the state secrets privilege and moved for summary judgment because the plaintiff had no other way to prove her case.[215] After a private review of the sensitive information, the district court upheld the assertion of the privilege and granted the Air Force's motion to throw out the case.[216] The court of appeals affirmed. It explained that, while the result might be harsh, "[T]he state secrets doctrine finds the greater public good -- ultimately the less harsh remedy -- to be dismissal."[217] Thus, under the state secrets doctrine, information will be protected in the interest of national security, even if it means that an individual may lose on a legitimate claim.[218]

B. Proposals for Change

1. Administrative Steps

Following the events of 9/11, Caps PA removed RMP data from the Internet and closed off access to the Caps OCA data in the reading rooms.[219] In March it restricted access to the non-public portions of its extensive Envirofacts database that had previously been opened to environmental researchers and academics.[220] Also in March, White House chief of Staff Andrew Card instructed all executive agencies and departments immediately to reexamine all their public documents for information that could aid terrorists or threaten national security.[221] In a concurrent memorandum from DOJ and White House information security officials, agency heads were directed to include within the review "sensitive but unclassified" information.[222] The existence of such a category of information and any legal basis for its protection was attacked by right-to-know advocates.[223] A spokesman for the Federation of American Scientist expressed concern that the category of "sensitive but unclassified" was ill-defined and could become a catch all that invited abuse.[224]

2. Proposed Community Protection from Terrorism Act, S. 2579

In an apparent attempt to extend national security logic to OCA portions of RMP information, Senator Bond introduced S.2579 in June. Entitled the "Community Protection from Terrorism Act," the bill begins with a series of findings, including

> [G]overnment-mandated publicly available information on worst-case scenario accidents at chemical facilities provides a blueprint that terrorists may use to plan and carry out terrorist attacks; [and]
>
> * * * *
>
> [w]hile communities have a right to know about the use of chemicals in their communities, [they] have the right not to allow terrorists to use such information to destroy the communities.[225]

The bill would amend § 112(r) of the Clean Air act by replacing subparagraph (7)(H), the provisions added by Congress in 1999 to forestall EPA's posting of OCA information on the Internet.[226]

The replacement proposed by S.2579 would take two major steps to protect OCA information. First, it would provide flatly that OCA information, regardless of when obtained or developed by EPA, "shall not be made available" under the Freedom of Information Act.[227] Second, it would prohibit access to OCA information by any member of the public, except as provided in the bill,[228] and "notwithstanding any other provision of law (including any regulation)."[229] It would authorize only read-only access to a paper copy of OCA information that has been sanitized of facility identity and location.[230] It would also mandate restricted access procedures that require government-issued identification and a signature from any member of the public seeking access.[231] The EPA employee granting access would be required to record the date and identity of each source for which OCA access was sought.[232] In addition, EPA would be required to establish an information technology system in consultation with the Attorney General to provide read-only access.[233] And it would make unauthorized disclosure by any official user a crime.[234] The bill would preempt state law regarding OCA information obtained pursuant to § 112(r) but leave unaffected any state OCA information collected separately under state law.[235]

IV. Nuclear Industry Approach

The chemical industry is embarking on a journey that ultimately will lead to increased security-related expectations and capabilities to protect from and respond to a hypothetical security threat. This section of the paper reviews measures that already have been taken by the commercial nuclear power industry to thwart similar threats. Many of the approaches taken by the nuclear industry are the result of many years of analysis and negotiation with the federal government regarding the definition of the threat and who is accountable and responsible for protecting public health and safety regarding the threat. In sum, there is no need for the chemical industry to start from the beginning regarding how to respond to this issue. Quite the contrary -- the

commercial nuclear industry has provided a general roadmap for industries that may be susceptible to low probability threats that may have high impact outcomes.

A. Legal and Regulatory Authority

1. Applicable Laws and Regulations

Existing federal statutes and regulations set strict standards for commercial nuclear plant operators to protect the public health and safety.[236] Section 161 of the Atomic Energy Act of 1954 grants broad authority to the U.S. Nuclear Regulatory Commission ("NRC") to issue rules and to take actions necessary to ensure public health and safety and the national defense.[237] The NRC has specific responsibility to ensure that the peaceful uses of nuclear energy "make the maximum contribution to the common defense and security and the national welfare, and . . . provide continued assurance of the Government's ability to enter into and enforce agreements with nations or groups of nations for the control of special nuclear material" ("SNM").[238]

Pursuant to its authorities, the NRC regulates all phases of licensees' operations, including: (1) accounting systems for SNM and source materials, and (2) security programs and contingency plans for dealing with threats, thefts, and sabotage relating to SNM, high-level radioactive wastes, nuclear facilities, and other radioactive materials and activities that the NRC regulates. Programs that promote the common defense and security and protect public health and safety by guarding against theft and sabotage are generally referred to as "safeguards" and "security" programs. Specifically, 10 C.F.R. Part 73 contains the majority of security and safeguards-related requirements for commercial nuclear facilities.

Security programs for commercial nuclear power reactors are designed to protect against a specified level of threat called the Design Basis Threat ("DBT"),[239] which characterizes the adversary force against which NRC licensees must design their physical protection systems and response strategies. The DBT must be well-defined, so that licensees do not have to design and protect against myriad, ever-changing scenarios. The current DBT assumes a suicidal, well-trained paramilitary force, armed with automatic weapons and explosives, that is intent on forcing its way into a nuclear power plant to commit radiological sabotage.[240] The DBT also assumes that the attackers will have insider knowledge of plant systems and plant security plans and even insider assistance. This assumed threat forms the basis for security response plans and training drills. The DBT premise is key to limiting what an NRC-licensed facility must do in an effort to deter potential threats.

As part of its oversight responsibilities, the NRC regularly tests these DBT-based plans and drills and reviews the adequacy of the DBTs. In close coordination with the national intelligence and law enforcement community, the NRC also continually assesses the threat environment.

a. Tests & Exercises

The NRC has conducted force-on-force security exercises, formally known as Operational Safeguards Response Evaluations ("OSRE"),[241] at nuclear reactor sites since 1991, and it carried out similar tests before that time. An OSRE is a simulated commando-style raid, designated to

identify shortcomings in security personnel performance or strategy. The drills and exercises are based on a pre-defined level of danger presented by the aggressor, i.e., the regulatory DBT. The OSRE program identifies areas where security can be improved and enhanced. As a result, the industry recognizes that force-on-force drills are an important means to assess security readiness. Identification of a weakness during an exercise typically leads to immediate corrective or compensatory measures.

Following the September 11 attacks, OSRE force-on-force exercises were temporarily suspended because, in the heightened threat environment, the conduct of exercises would be a significant distraction to the site security forces. The NRC staff is currently preparing options for Commission consideration on how to reinstate security exercises. In the interim, table-top style drills are being initiated in preparation for resumption of the physical exercises. In the future, the NRC and the industry may look at beyond-design basis threats and the ability of licensee actions to mitigate any hypothetical damage caused by a beyond-DBT attack.

b. Current DBT Reassessment

In consultation with other Federal agencies, the NRC is currently considering long-term revisions to the DBT to reflect changes in the threat environment. It has long been settled that threats posed by enemies of the state are the responsibility of the Federal Government, not the applicant-operator. The NRC made this clear by rule:

> An applicant for a license to construct and operate a production or utilization facility, or for an amendment to such license, is not required to provide for design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U.S. defense activities.[242]

This division of responsibility was challenged by an intervenor in the construction permit proceeding for the Turkey Point plant in south Florida, who urged the licensing board to consider the potential effects of sabotage or enemy attack due to the proximity of the site to Communist Cuba. The Commission found that enemy-of-the-state threats were not within the scope of the threats for which licensees would be responsible to provide protection, and it denied intervenor Siegel's contention. He appealed to the D.C. Circuit, which held that "the Commission was well within the limits of the powers delegated to it by Congress when it decided to limit petitioner's cross-examination [on the risk of an enemy attack or sabotage] in the license proceeding, and to embody the policy of limitation in its regulation."[243] The court recognized that protection against enemy attack would be an impossible burden to place on the applicant:

> Did the Commission step over the bounds of the authority committed to it by excluding the dangers latent in possible enemy action from the inquiry into the merits of a license application? If it did, then it would appear that anyone seeking permission to employ nuclear energy for peaceful industrial uses must shoulder a burden of showing that his proposed

> facility is adequately protected, now and throughout its entire life, against the various kinds of attacks which might be made upon it by foreign enemies of the United States. What the Commission has essentially decided is that to impose such a burden would be to stifle utterly the peaceful utilization of atomic energy in the United States. Such a decision hardly seems to us to conflict with the Congressional purposes underlying the Act, nor to exceed the scope of the authority given the Commission by Congress to realize those purposes.[244]

Since *Siegel*, the nuclear industry has enjoyed a stable, consistent division of security responsibility between the licensee's and the Federal Government's protection responsibilities regarding a localized security threats versus an enemy-of-the-state type attack.

Potential revision of the DBT to change that allocation is one of the most debated issues in the industry following the terrorist attacks. Some public interest groups believe that the DBT should be revised to include 9/11-type activities involving larger, fuel-laden airliners. While nuclear facilities are among the most hardened commercial industrial facilities within the United States,[245] none has been specifically designed to withstand a deliberate, high-velocity, direct impact of a modern, large commercial airliner.[246] Consequently, any fundamental change to the DBT may have a profound effect on the industry. If substantial fundamental changes with associated high costs are required of commercial nuclear plant operators, there is a risk that some plants may no longer be economically feasible for continued facility operation.[247]

2. Pending Congressional Bills

Currently, security-related actions at specific commercial nuclear facilities are taken by the private licensees of the nuclear facilities with oversight and enforcement by the NRC.[248] Commercial nuclear power plants have rigorous emergency preparedness programs that include security forces[249] and biennial, evaluated exercises.[250] In the event of a serious problem, including a terrorist attack around a nuclear power plant, the plans and procedures that have been routinely exercised would be activated.

Nevertheless, pending legislation in both houses of Congress seek to federalize security forces at commercial nuclear facilities and to modify the DBT to include act-of-war threats. On November 29, 2001, the two most significant pieces of pending legislation dealing directly with security-related issues at nuclear power plants were introduced. H.R. 3382, the "Nuclear Security Act of 2001," was introduced in the House by Congressman Edward Markey (D-MA). The bill was referred to the House Committee on Energy and Commerce with little action at the time of this writing.[251] The companion bill in the Senate, S. 1746, was introduced by Senator Harry Reid (D-NV) and was referred to the Committee on Environment and Public Works.[252] Based on the text of the proposed legislation, both bills would increase the nuclear industry's security-related burdens, if not actual security.[253]

The bills would require the NRC to establish and maintain a federal security force at each power reactor facility. This concept has been discouraged by both the regulator and the regulated. NRC Chairman Richard Meserve has raised a conflict of interest issue regarding the oversight of the force and how both implementing and overseeing nuclear plant security forces may

compromise the objectivity of the NRC in fulfilling its mission.[254] Additionally, the schemes proposed by the bills pose a threat to the overall command and control activities of the responding forces to a security or other off-normal situation. Currently, the security forces report to the licensee organization and coordinate efforts with various other entities within that organization, such as the control room crews and maintenance crews, to mitigate accidents or defend and restore functions in the plant following a potential attack. Under the proposed bills, the federalized security force would be an independent organization taking orders from the NRC. This division would create potential communications barriers and delays in coordinating important protective and recovery actions.

Another adverse feature in both bills is the requirement to reconsider the DBT, including 9/11-type attacks, on a periodic basis. These bills, as proposed would reverse the policy in *Siegel* and risk imposing on industry the responsibility for enemy-of-the-state threats. Any marked expansion of the DBT, if enacted, would present the possibility for a re-engineering of many facilities, not only once, but every three years.

For decades, the major focus area for the NRC and the industry's commercial licensees was to enhance and ensure protection against industrial accidents. Recent events have caused nuclear security concerns to become a major contender in the arena for NRC and industry resources.

B. Key Elements of Nuclear Plant Security

The security scheme at commercial nuclear facilities consists of programs, procedures, physical protection zones with associated physical barriers, specially-trained and screened personnel, law enforcement-type firearms and equipment, access authorization and control mechanisms, fitness-for-duty screening, continuous behavior observation, and coordination with federal and local agencies.[255] For the sake of simplicity, we describe these means below in two categories: personnel and hardware-related.

1. Personnel-Related

Commercial nuclear power plant licensees maintain a highly trained, well-equipped security force to guard each facility. Security personnel, many of whom have prior law enforcement or military experience, are subject to extensive background checks[256] and rigorous training requirements.[257] Annual force-on-force training covers such topics as threat assessment and tactical response, response force deployment and interdiction, protection of specified vital equipment and protected areas, multiple target acquisition and engagement, and the use of armored body bunkers, ballistic shields, and other specialized security equipment.[258]

Personnel screening is augmented at nuclear facilities by a computer system used to control access to badge personnel at individual sites. Many licensees share access to a protected computer data base called PADS (Plant Access Database System). This system allows tracking and sharing of access authorizations and denials at various nuclear facilities. Each site also has its own self-supported computer system increasingly equipped with biometric technology which governs who can access what areas of the plant. Finally, everyone granted unescorted access must pass a test focused on general nuclear concepts and site-specific requirements.

As a further protection for the public, each nuclear power plant has an extensive and well-honed emergency response organization ("ERO") and systems in place to respond to and mitigate any emergency that may arise.[259] The security force is a vital element of this emergency response organization; however, the ERO consists of both non-security personnel and security personnel. During any significant security-related event at a facility, one of four Emergency Action Level classifications ("EALs") will be declared, and the ERO will staff various facilities to mitigate adverse actions associated with the plant's emergency response plan.[260] The plans are tightly integrated with local, state, and federal regulatory and emergency authorities.[261] The emergency planning zone for actions to be taken typically includes an area within the 10-mile radius of the plant (*i.e.,* an area encompassing roughly 314 square miles).

2. Physical Barriers/Hardware/Technology

A number of physical defenses exist to counter a security-related threat. Nuclear plants, by their very design, provide a redundant set of physical barriers designed both to keep radiation and radioactive materials in and to keep intruders out.[262] A facility built to protect against high winds, earthquakes, and tornado-generated missiles has fortress-like qualities. The reactor core is protected by a sealed containment structure constructed of several feet of reinforced concrete walls, a steel liner, additional concrete walls within the structure for separation of important structures, and a several inches-thick high-tensile strength steel reactor vessel. The metal cladding on the fuel itself also serves as an additional protective barrier. In addition, there are multiple systems of the safety equipment needed to safely shut down the reactor.

Nuclear plant sites have three distinct zones, each of which has different levels of physical defense.[263] The largest zone, called the "owner-controlled area," includes all of the property surrounding the facility over which the licensee exercises legal control. The owner controlled area serves as an effective buffer zone around the critical areas of the plant and may be fenced.

The second zone, encompassed within the owner-controlled area, is the "protected area." This is a physically enclosed area surrounding the plant into which access in controlled.[264] Physical barriers include barbed wire and razor wire fences, microwave and electronic intrusion detection systems, closed circuit television systems, isolation zones, extensive lighting, system monitoring by redundant alarm stations, and vehicle barrier systems. Access to the protected area is restricted to a select subset of site personnel with a need for entry. To access the protected area, employees and visitors must pass through metal and explosives detectors. X-ray machines are also used to screen material brought into the protected area by employees and visitors.[265] In addition, employees must utilize a card-reader system and typically a hand-geometry device to confirm their identity before entering the protected area.

The third, innermost zone is the "vital area." It contains vital equipment essential for operating the plant safely and for shutting down and cooling the plant safely.[266] Additional barriers are in place to protect vital areas of the plant, including concrete floors, walls, and ceilings; locked and alarmed metal doors; and key-card access doors. Access to the vital area is even further restricted to a select subset of site personnel. Access lists are routinely reviewed to confirm the continuing need for access. Defensive contingency plans used by security forces are geared towards protection of these critical areas.

3. Post 9/11 Measures

For decades before September 11, 2001, U.S. nuclear power plants were among the best defended and most hardened facilities of the nation's critical infrastructure. Within hours of the 9/11 attacks, the NRC issued the first of a series of security advisories to power reactor licensees.[267] That advisory placed the facilities on the highest level of security-related alert, as established by the NRC in a 1998 Generic Letter which provided a hierarchy for security-related states of readiness.[268] Approximately 30 of these "advisories" have been issued to ensure that licensees are apprised of the current threat situation and informed of voluntary actions requested by the NRC to reinforce existing security measures. In February, the NRC moved to make these additional measures mandatory, and in April it established the Office of Nuclear Security and Incident Response ("NSIR"). NSIR serves as a centralized security organization by consolidating certain NRC security, safeguards, and incident response responsibilities and resources formerly divided among other offices.[269]

Although no confirmed threats have been made regarding U.S. nuclear facilities, President Bush's January 29, 2002 State of the Union address included a brief mention of U.S. nuclear facility diagrams being among the items found by U.S. forces during a sweep of a terrorist camp in Afghanistan.[270] Licensees have taken a variety of protective measures in conjunction with NRC guidance. These included actions to harden site access, to increase security resources, and to improve operational readiness and coordination (with local law enforcement agencies) capabilities.

a. NRC Interim Compensatory Measure Order

On February 25, 2002, the NRC issued an interim Order[271] to each power reactor licensee.[272] The actions prescribed, officially known as Interim Compensatory Measures ("ICMs"), are to be taken pending the completion of a more comprehensive review by the NRC of safeguards and security program requirements. The purpose of the Order was to provide for a more prescriptive, rather than voluntary, method to ensure that many of the measures discussed in the earlier security advisories were being implemented. The Order was an exercise of authority that assuaged concerns of certain members of Congress and intervenor groups regarding the adequacy of NRC authority and action in response to the threat of terrorist attacks.

While many of the specifics regarding the NRC Order are classified as safeguards information and therefore cannot be disclosed to the public, issues addressed by the Order generally include security officer staffing levels, protection against potential vehicle and waterborne threats, protection of spent fuel, enhanced access authorization controls, and mitigation efforts in the event of an attack. Licensees had to provide legal responses to the Order within twenty days, and full implementation of those commitments to the ICMs is expected to occur on or before August 31, 2002.

b. NRC Licensee Response

Since September 11, many licensees have conducted security briefings for state and local officials to reinforce the coordination and response plans in the event of an emergency. Nuclear plants have also extended the point of initial screening of persons and vehicles entering the plant

site from the protected area boundary to some point within the owner-controlled area. This initial screening includes an identification check, confirmation of the purpose for entering the site, and a thorough vehicle inspection for visitors or vehicles capable of being used as part of a revised ground-blast standard. In addition, armed security forces have extended their patrols to include a larger portion of the owner controlled area. These patrols are coordinated with onsite personnel to enhance detection and to deter potential threats.

The industry has responded in earnest to the specific ICMs. It has expended large (and unforeseen) amounts of capital to comply with the provisions of the Order. No licensee has formally challenged an Order or requested a hearing related to the imposition of the Order. Unfortunately, these efforts might be preempted by a revised DBT that imposes even more burdensome enemy-of-the state requirements on facilities.

C. Information Control

1. Safeguards

Safeguards Information is a special category of sensitive, unclassified information authorized by the Atomic Energy Act of 1954, as amended, to be protected.[273] Safeguards Information ("SGI") concerns the physical protection of operating power reactors, spent fuel shipments, strategic SNM, or other radioactive material. While SGI is considered to be sensitive unclassified information, its handling and protection more closely resemble the handling of classified Confidential information than other sensitive unclassified information.[274]

The categories of individuals who are permitted access to SGI and the protections afforded SGI are provided in 10 C.F.R. § 73.21. Controls over SGI include training of individuals prior to access and a "need-to-know" prior to that access. SGI materials cannot be discussed over normal telephone lines and cannot be transmitted over typical Internet connections. Nor can SGI be mailed by normal means. Written SGI materials must be appropriately marked and kept in a locked and rated safe if left unattended. Any violation of these requirements could subject the individual to civil and criminal penalties.[275]

Information classified by the NRC and by power reactor facilities at a level beyond SGI is primarily classified in two rarely used categories:

- National Security Information ("NSI"): Information classified by an Executive Order, the compromise of which would cause some degree of damage to the national security.
- Restricted Data ("RD"): Information classified by the Atomic Energy Act of 1954, as amended, which if compromised would assist in the design, manufacture, or utilization of nuclear weapons.[276]

The lowest level of classified information is Confidential; the next is Secret. Confidential and Secret information will also be either NSI or RD, and may be marked C-NSI or S-RD, for example. The NRC seldom deals with Restricted Data because the NRC does not regulate nuclear weapons production. Much classified material at NRC and at power reactors is classified by order of other government agencies (*e.g.*, Department of Energy). The NRC is not empowered to declassify such information without the permission of the originating agency.

Additionally, information about a licensee's physical protection program not otherwise designated as SGI (or otherwise classified as restricted or protected information) is required by 10 C.F.R. § 2.790(d) to be protected in the same manner as commercial or financial information (*i.e.*, they are exempt from public disclosure under of the Freedom of Information Act. 5 U.S.C. § 552(b)). Therefore, many avenues exist in the regulations for protection of potentially sensitive information.

2. Internet

In an abundance of caution, the NRC restricted public access to its web-site on October 11, 2001, and then began to restore limited access in a deliberate sequence.[277] The reason given for the restriction was to limit access to material items of information that a terrorist organization could potentially use to target or select a nuclear facility. A review of internet-accessible information by the NRC is still in progress, and select information periodically becomes available to the general public. A full evaluation of the approximately 50,000 web-pages is expected to conclude at or near the end of 2002.

A letter from the NRC Commissioners to the NRC Staff provides guidance to evaluate whether a document or other item of information should be released.[278] This guidance relates to yet another classification of material that is considered Sensitive Homeland Security Information ("SHSI"). This category is considered for removal from public disclosure, even if the information may not have been considered SGI. Examples of information meeting this new, protected information category include: plant drawings and construction details, schematics, and related information that could be used by an adversary to determine facility vulnerabilities. Need-to-know has replaced right-to-know as a guiding principle.

D. Special Measures for Public Nuclear Liability

Another feature that distinguishes the nuclear industry is a statutory insurance pool and caps on public nuclear liability. Congress passed the original Price-Anderson Act in 1957[279] to provide an insurance scheme for the emerging nuclear industry and to limit liability for any off-site damage to persons or property. Any legal damage awards above that limit would be covered by the government. This action was deemed necessary to enable private companies to enter into the industry without the fear of unlimited liability from a major nuclear incident. Following several amendments to the Act and adjustments for inflation, the amount of liability coverage for a single incident, and therefore, the liability limit, today is approximately $9.4 billion.[280]

Coverage is provided by two layers, one commercial insurance and the other funded retrospectively as a pool by all reactor operators. Each operator of a large nuclear power plant licensed by the NRC must maintain an amount of primary financial protection against public liability claims equal to the maximum amount of liability insurance available at reasonable cost and on reasonable terms from private sources (the "primary insurance amount").[281] As of this writing, the primary insurance amount is $200 million.[282]

Each large reactor licensee also must participate in a secondary insurance plan, under which a deferred (*i.e.,* retrospective) premium of not more than $83.9 million, subject to a surcharge of

up to $4.195 million for a total of $88.095 million, for each nuclear reactor may become payable following a major nuclear accident (the "secondary insurance amount").[283]

In addition, the Commission is authorized to enter into contracts to indemnify each licensee from public liability arising from nuclear incidents for the difference, if any, between the sum of the licensee's primary and secondary insurance and the liability imposed.[284]

The Price-Anderson Act lapsed on August 1, 2002. While existing licensees remain covered, any new licensees would not receive the protection. Although both houses of Congress have passed separate bills[285] reauthorizing Price-Anderson, the provisions are nested in the same energy bills that contain the controversial provisions dealing with the Alaska National Wildlife Refuge ("ANWR") drilling issue. Therefore, approval of a compromise bill into law is being delayed. Price-Anderson has lapsed and been reinstated before.[286] It is expected to be reinstated following the current lapse as well.

E. Nuclear Industry Cohesiveness

Perhaps much of the nuclear industry's survival and success in dealing with Congress and the regulatory agencies is attributable to its cohesiveness. The relative homogeneity of its product and plants, along with federal preemption, have undoubtedly helped foster that cohesiveness. But the nuclear industry formed an organization, the Nuclear Energy Institute ("NEI"), through which it can voice one opinion to both the NRC and to other government bodies, such as Congress, on matters inherently important to owners and operators of commercial nuclear facilities.[287] With member participation, the NEI develops policy on key legislative and regulatory issues affecting the industry.[288] NEI then serves as a unified industry voice before Congress and federal regulators. Such an approach provides strength in numbers, and promotes consistency among facilities owned by many different entities with differing priorities. In addition, NEI shields its membership from accusations directed towards individual members when politically charged issues are being addressed.

NEI has over 260 corporate members, which include operators of nuclear power plants, design and engineering firms, fuel suppliers, and service companies. The success of NEI is based in great part on total participation by all commercial nuclear power plant owners. The organization is headquartered in Washington, D.C., and employs a staff of about 120. Its 60-member board of directors includes representatives from the nation's 42 nuclear utilities, plant designers, architect/engineering firms, and fuel cycle companies.[289] Members provide financial resources for the organization, as well as participants to assist in various project initiatives.

Members of NEI have formed a Security Working Group ("SWG") to share information and to interface more effectively with the NRC following the events of September 11, 2001. The SWG routinely proposes oversight standards and generates interpretive documents to ensure a more uniform application of the existing regulations, regulatory guidance, and draft criteria to which power reactor licensees will be held in the future. The SWG is viewed by the industry as beneficial due to its proposing more realistic requirements to the NRC Staff, rather than the Staff's potentially drafting ultra-conservative, and perhaps unrealistic security-related criteria. This same philosophy holds true regarding other working groups sponsored by NEI (*e.g.*, a group

devoted to license renewal work). Although the NRC still retains control over final regulations and guidance documents, the cooperative and proactive efforts through NEI have led to more appropriate and more well-defined standards.[290]

V. Conclusion

Protection from terrorist attacks is an inherent aspect of providing for the common defense of the Nation. The Preamble to the U. S. Constitution declares that among the purposes of establishing the Federal Government were to "insure domestic Tranquility [and] provide for the common defence [sic]." To that end, Article I, Section 8 vests in Congress the power "to pay the Debts and provide for the common Defence [sic]." It is, therefore, Congress that is empowered "To raise and support Armies"; "To provide and maintain a Navy"; "To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions"; and "to provide for organizing, arming, and disciplining the Militia."[291] The threat of terrorist activity is akin to the risk of insurrection or of an invasion of foreign forces bent on hostilities against the United States. The NRC rule upheld in the *Siegel* decision properly recognizes that an industry should not bear the burden of defending against enemies of the state. Congress should learn from that example. It should reject the proposal in Corzine's bill S.1602 to impose on the chemical industry a general duty to prevent acts of terrorism.

Three characteristics of CAPs H.R. 5300 differentiate it from S. 1602 and make it a far preferable measure to its Senate counterpart. First, H.R. 5300 would not created a general duty for facility owners and operators to prevent terrorist attacks on their facilities. Therefore, H.R. 5300 would not risk making criminals out of those who, despite their best efforts, become unwitting victims of terrorism. Second, H.R. 5300 would protect sensitive information from disclosure and dissemination. H.R. 5300 provides that information submitted to the EPA would not be made available to the public under the Freedom of Information Act.[292] Additionally, the EPA and the Department of Homeland Security are to develop the protocols necessary to protect the information the EPA receives under the Act from being accessed by unauthorized parties.[293] No such information security protocols are required to be developed under S. 1602.

Third, in contrast to the adversarial relationship set up by its Senate counterpart, H.R. 5300 would foster cooperation between government and industry. Under H.R. 5300 the head of the Department of Homeland Security would be required to supply chemical facility owners and operators with relevant threat information based on the assessments and plans prepared by the facilities themselves. Additionally, if the Department of Homeland Security were to determine that a terrorist threat existed or that the implementation of a current facility's plan were insufficient, the facility would be notified of this threat or insufficiency so that the situation could be addressed. This type of information-sharing and compliance assistance fosters cooperation between government and regulated facilities.

The common defense far outweighs any desire to make sensitive OCA data common knowledge. Information that could assist terrorists in targeting attacks against chemical plants must be accorded protection from uncontrolled dissemination by whatever avenue, whether the Internet, reading rooms, or release by state or local emergency planning and response authorities. This protection might be created by Executive Order extending national security classification to such

information, or it could be done by congressional action. The category of information recognized by the NRC as "sensitive but unclassified" would lend itself especially well to the protection of that OCA information. While the procedures for its protection are not as cumbersome as for classified information, the restrictions on its dissemination seem especially appropriate. The concept of "sensitive but unclassified" information has already surfaced in the Administration's post-9/11 proposals. Whether by legislation or executive action, the OCA information should continue to be exempt from disclosure under FOIA, by means of either recognizing that it falls into an existing exempt category or by reliance upon the exemption in § 112(r)(7)(H)(iii)(II) of the Clean Air Act. In addition, § 112(r)(7)(iii) should be amended to clarify that the information that "shall be made available to the public" does not include information that comprises a blueprint for terrorists.

Congress should consider establishing a retrospective insurance pool for the chemical industry on the model of the program under the Price-Anderson Act. It would be intended to cover catastrophic losses and public liability arising from terrorist strikes directed against chemical facilities. The threat of claims and liability arising from terrorist attacks has interrupted the availability of insurance coverage at a reasonable price. Bills that have passed both Houses of Congress would provide a Federal backstop by capping insurance companies liability for a limited time. While they differ in particulars, such as the amount of the Federal share and the exclusion of punitive damages, both bills are temporary palliatives aimed primarily at the commercial real estate market.

The chemical industry needs a more enduring insurance and terrorism liability protection program. The Price-Anderson model of two-tiered coverage comprised of a primary layer of commercial insurance protection and a secondary layer of a retrospective-premium pool commends itself. Beyond those layers, public liability in the event of a terrorist strike should be capped or covered by the Government. Qualification for the retrospective premium pool, the liability caps or Government backstop insurance could be conditioned upon compliance with defined industry standards. Of course, given the complexity and diversity of the chemical industry, no one-size-fits-all standard would be appropriate. Because of the need for an insurance program for the chemical industry and the nature and magnitude of such a program, we urge Congress to create a national commission to evaluate the needs and options and to formulate a recommendation.

These recommendations would represent an ambitious agenda for the chemical industry. They cannot be realized without a concerted and cohesive push by the industry speaking with one voice. The nuclear industry has taken the initiative to work in partnership with the NRC to develop regulatory requirements and reform initiatives, when appropriate. The nuclear industry has learned through its experiences at Three Mile Island[294] and subsequent regulatory initiatives that it cannot wait for a government entity to determine its destiny when a politicized challenge to industry viability is involved. To do so leads to requirements that are unrealistic and therefore, very difficult to satisfy.[295] The nuclear industry has realized that (1) it knows the industry much better than the regulator, (2) it understands its facilities' vulnerabilities much better than a regulator, and as a result (3) the industry is much more likely to develop viable and effective solutions. The chemical industry is no different in these respects than its nuclear counterparts.

The nuclear industry does, however, enjoy a definite advantage. It has persuaded the NRC to draw the line on ratcheting up regulatory requirements. Politically-charged, reactive rules are seldom the final solution. The regulator may adopt an initiative, demand compliance, only to alter its course later. For example, after Three Mile Island, the NRC issued a plethora of regulatory requirements and guidance documents that were thought to address plant vulnerabilities and to respond to the public outcry. Many years after the accident, and well into the implementation of these requirements and guidance, the industry recognized that it could not respond to every regulatory whim. The NRC was compelled to issue 10 CFR 50.109, otherwise known as the Backfit Rule.[296] The Backfit rule applies to the NRC itself, not its licensees. It prevents the NRC from modifying its positions, unless the increased benefit is shown to justify the cost.

The nuclear industry's experience suggests that the chemical industry must take the leadership role to promote site security to accomplish an acceptable result. Working with, instead of apart from, EPA would better ensure that the upcoming rulemaking is tenable and achieves mutually agreed-upon objectives. An umbrella organization in the chemical industry could assist EPA in developing the rulemakings, show EPA the limitations of the industry, and stand with it as challenges arise. Also, this same industry organization could coordinate the industry's response to EPA initiatives, Congressional fact-finding, and expert testimony situations. Current circumstances that appear to be adverse to the industry, with proper effort, could be an opportunity for constructive compromise and positive results.

[1] The authors are partners in the Washington, D. C. office of the law firm of Winston & Strawn. They wish to thank and acknowledge the assistance of Carey W. Fleming and Yolanda R. Oliver in the preparation of this paper. Responsibility for errors or omissions, however, is solely that of the authors.

[2] Cheryl Hogue, *Chemical Security Site Plan*, Chem. and Eng. News, Aug. 12, 2002, at 7. Senator Corzine's statement at hearing on his bill S. 1602 on November 14, 2001, put the number at 18,800. *Chemical Security Hearings: Hearing on S. 1602 Before the Subcommittee on Superfund, Toxics, Risk and Waste Management of the Senate Environment and Public Works Committee*, 107th Cong. (2001) (statement of Jon S. Corzine, Senator) [hereinafter *Chemical Security Hearings*]

[3] 40 C.F.R. Part 68 (2001).

[4] Clean Air Act, 42 U.S.C. § 7412(r)(7)(A)(ii) (2000).

[5] *Chemical Security Hearings, supra* note 2, (testimony of Paul Orum, Director, Working Group on Community Right-to-Know).

[6] *Id.*

[7] Eric Pianin, *Study Assesses Risk of Attack on Chemical Plant*, The Washington Post, Mar. 12, 2002, at A8.

[8] Nick Nichols, *Tips for Terrorists on Web,* The Baltimore Sun, Jan. 24, 2002, at 13A.

[9] *Site Security Guidelines for the U.S. Chemical Industry*, Hallcrest Systems, Inc, Oct. 23, 2001, http://www.americanchemistry.com/cmawebsite.nsf/s?readform&nnar-53rkt8 [hereinafter *Site Security Guidelines*].

[10] It apparently embraced, sight unseen, an assessment methodology developed for the Department of Justice by Sandia National Laboratories. News Release, American Chemistry Council, Chemical Industry Commits to Mandatory Enhanced Security, (June 5, 2002), http://www.americanchemistry.com/cmawebsite.nsf/s?readform&nnar-5a6kkh, [hereinafter *Mandatory Enhanced Security*].

[11] Ann Davis, *New Alarms Heat Up Debate On Publicizing Chemical Risks*, The Wall Street Journal, May 30, 2002, at A1 [hereinafter *Publicizing Chemical Risks*].

[12] Meredith Preston, *EPA to Publish Proposed Rule Governing Security at Chemical Plants*, 26 Chem. Reg. Rep. 1021 (Aug. 12, 2002), http://ippubs.bna.com/ip/BNA/CHE.NSF/15f97eb6efb53d3085256743006dcbde/4004685377e890d585256c1100095279?OpenDocument.

[13] *Publicizing Chemical Risks, supra* note 11 at A6. Right-to-Know Network's "The Safe Hometown Guide" calls for just-in-time deliveries.

[14] Carl Prine, *Toxins Often Vulnerable During Transit*, Pittsburgh Tribune-Review, Apr. 7, 2002, at 2,3, http://www.pittsburghlive.com/x/search/s_64614.html.

[15] Chemical Security Act of 2001, S. 1602 107th Cong. § 4(b) (2001).

[16] *Chemical Security Hearings, supra* note 2, (opening statement of Senator Bob Smith, Ranking Member, Environment and Public Works Committee).

[17] Patricia Ware, Nancy Ognanovich, and Linda Roeder, *White House Directs Agencies to Review Material That Could Threaten U.S. Security*, 56 Daily Environment Report A-12 (Mar. 22,2002), *at* http://ippubs.bna.com/ip/BNA/DEN.NSF/33973f565fe8e8e085256743006dd9e3/670b0a0d3149935885256b8400108553?OpenDocument, [hereinafter *White House Directs Agencies to Review*]; Nichols, *supra* note 8.

[18] *Chemical Security Hearings, supra* note 2, (testimony of Paul Orum, Director, Working Group on Community Right-to-Know).

[19] *Publicizing Chemical Risks*, *supra* note 11, at A6.

[20] *Id.*, at A1.

[21] *Chemical Security Hearings, supra* note 2, (testimony of Fred Webber, President and CEO, American Chemistry Council).

[22] *Id.*, (testimony of Paul Orum, Director, Working Group on Community Right-to-Know).

[23] *Id.*, citing Sam Mannan, M. Gentile & M. O'Connor, *Chemical Incident Data Mining and Application to Chemical Safety Data Trend Analysis*, M.K. O'Connor Process Safety Center, Texas A&M University (2001).

[24] Energy Information Administration, Electric Sales & Revenue 2000, DOE/EIA-0540(00) (Jan. 2000). The figure for nuclear-generated electric revenues is derived by multiplying total U.S. electricity sales of $224.24 billion in 2000 by the nuclear percentage of generation.

[25] Nuclear Regulatory Commission Licensee Event Report (LER) Summaries, 10 C.F.R. §50.73(a)(2)(viii) (1998).

[26] Occupational Safety and Health Act (OSHA), 29 U.S.C. § 654(a)(1) (2000).

[27] Pub. L. 101-549, § 304, (1990), set forth as a note at 29 U.S.C. § 655 (2000).

[28] 29 C.F.R. § 1910.119 & App. A-D (2001).

[29] Pub. L. 101-549, § 304(a)

[30] 29 C.F.R. § 1910.119 (2001).

[31] *See* 29 C.F.R. § 1910.119 (d).

[32] *See Id.* §1910.119(e) & App. C.

[33] *See Id.* § 1910.119(f)-(o).

[34] *Id.* § 1910.119 App. C.

[35] Pub. L. 101-549, Title III, § 301, Nov. 15, 1990.

[36] Clean Air Act, § 112(r)(1), 42 U.S.C. § 7412(r)(1) (2000).

[37] *Id.*

[38] *Id.*

[39] 61 Fed. Reg. 31717 (1996), codified, as amended at 40 C.F.R. Part 68 (2001)

[40] The rule defines "public receptor" to mean

[offsite . . . [quote]]

40 C.F.R. § 68.3.

[41] 40. C.F.R. § 68.10(a). The chemicals listed as regulated substances and the threshold quantities differ from those under the OSHA PSM standard.

[42] 40 C.F.R. § 68.10(b)-(d).

[43] Only those that have had no off-site consequences from releases during the prior five years and otherwise qualify for "Program 1" may be subject to reduced requirements.

[44] *See* 40 C.F.R. § 68.12.

[45] *See id.*, & § § 68.20, 68.25, 68.160, 68.165.

[46] 40 C.F.R. § 68.3.

[47] *See Cf.* 40 C.F.R. § 68.28(b).

[48] News Release, American Chemistry Council, Chemical Makers Adopt Tough Security Measures, (Jan. 30, 2002), http://www.americanchemistry.com/cmawebsite.nsf/s?readform&nnar-56vjye.

[49] *Mandatory Enhanced Security, supra* note 10.

[50] *Site Security Guidelines*, *supra* note 9.

[51] *Id* at 5-10.

[52] *Id* at 11.

[53] *Id* at 11-16.

[54] *Id* at 17.

[55] *Id* at 17-19.

[56] *Id* at 21.

[57] *Id.*

[58] *Id* at 22.

[59] *Id* at 23-25.

[60] *Id.*

[61] *Id.*

[62] *Mandatory Enhanced Security, supra* note 10.

[63] Mike Ferullo, *Justice Department Releases Sandia Tool For Chemical Plants to Assess Vulnerability*, 117 Daily Environment Report A-1 (June 18, 2002), *at* http://ippubs.bna.com/ip/BNA/den.nsf/33973f565fe8e8e085256743006dd9e3/8814837627f372d685256bdc000756eb?OpenDocument [hereinafter Ferullo].

[64] *Chemical Facility Vulnerability Assessment Methodology*, (National Institute of Justice, Washington, DC), June 2002, http://www.ojp.usdoj.gov/nij/pubs-sum/195171.htm [hereinafter *Methodology*].

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] Ferullo, *supra* note 63.

[70] *Mandatory Enhanced Security, supra* note 10.

[71] *Methodology*, *supra* note 64.

[72] *Id* at 24.

[73] *Id.*

[74] Id. at 5.

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *Id* at 6.

[81] *Id* at 8.

[82] *Id* at 11.

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id* at 12-13.

[87] *Id.*

[88] *Id* at 14.

[89] *Id* at 15.

[90] *Id.*

[91] *Id.*

[92] *Id* at 15-19.

[93] *Id* at 18.

[94] *Id* at 19.

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id* at 19-24.

[99] *Id.*

[100] *Id.*

[101] *Id* at 24.

[102] *Id.*

[103] *Id* at 25.

[104] *Id.*

[105] *Id.*

[106] *Id* at 26.

[107] Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 10, 2001).

[108] *Id.*

[109] Homeland Security Presidential Directive-3, 38 WEEKLY COMP. PRES. DOC. 394 (March 18, 2002).

[110] *Id.*

[111] News Release, Office of the Press Secretary, Gov. Ridge Announces Homeland Security Advisory System, (March 12, 2002), http://www.whitehouse.gov/news/releases/2002/03/20020312-1.html.

[112] Homeland Security Presidential Directive-3, *supra* note 109 at 394.

[113] *Id.*

[114] *Id.* at 396.

[115] *Id.* at 396, 397.

[116] Letter from Frederick L. Webber, President and CEO, American Chemistry Council, to John Ashcroft, Attorney General, Department of Justice. Comments on the Proposed Homeland Security Advisory System, (Apr. 26, 2002).

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] Chemical Security Act of 2001, *supra* note 15.

[123] Meredith Preston, *Senate Committee Approves Legislation On Safety Measures at Chemical Plants*, 144 Daily Environment Report AA-1 (July 26, 2002), *at* http://pubs.bna.com/ip/BNA/DEN.NSF/33973f565fe8e8e085256743006dd9e3/08b9bef46b8d565885256c020006e234?OpenDocument [hereinafter *Senate Committee Approves Legislation*].

[124] Chemical Security Act of 2001, *supra* note 15 at § 4(a)(1).

[125] *Id.* at § 4(a)(3).

[126] *Id.* at § 4(b)(1)-(3).

[127] Meredith Preston, *Chemistry Council Urges Federal Government To Keep Member Facilities' Actions On Track*, 142 Daily Environment Report A-8, (July 24, 2002), *at* http://ippubs.bna.com/ip/BNA/DEN.NSF/33973f565fe8e8e085256743006dd9e3/4066b239eecec3df85256c000008869a?OpenDocument.

[128] *supra* note 15 at § 4(a)(4).

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.* at § 5(1), (2).

[134] *Id.*

[135] *Id.* at § 6(a).

[136] *Id.* at § 6(b).

[137] *Id.* at § 7.

[138] *The American Chemistry Council on the Chemical Security Act*, (American Chemistry Council, Arlington, VA), July 26,2002, http://www.americanchemistry.com/cmawebsite.nsf/s?readform&jtir-5cdsxs.

[139] *Id.*

[140] *Id.*

[141] *Senate Committee Approves Legislation*, *supra* note 123.

[142] *Id.*

[143] Meredith Preston, *Administration Wants to Avoid Legislation Requiring Safety Measures at Chemical Sites*, 133 Daily Environment Report A-6 (July 11, 2002), *at* http://pubs.bna.com/ip/BNA/DEN.NSF/33973f565fe8e8e085256743006dd9e3/5b7491b43ee1044585256bf30007aed2?OpenDocument [hereinafter *Administration Wants to Avoid Legislation*].

[144] *Senate Committee Approves Legislation*, *supra* note 123; *Administration Wants to Avoid Legislation, supra* note 143.

[145] *Id.*

[146] Meredith Preston, *Agency Plans to Publish Proposed Rule Requiring Facilities to Access Vulnerabilities*, 152 Daily Environment Report A-5 (Aug. 7 2002) *at* http://pubs.bna.com/ip/BNA/DEN.NSF/f67b41b17d1df0e68525649900681368/7f1e29eb79fdaa7b85256c0e00039ce9?OpenDocument [hereinafter *Agency Plans to Publish Proposed Rule*].

[147] *Administration Wants to Avoid Legislation, supra* note 143; *Senate Committee Approves Legislation, supra* note 123.

[148] *Senate Committee Approves Legislation, supra* note 123.

[149] *Agency Plans to Publish Proposed Rule, supra* note 146.

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Senate Committee Approves Legislation, supra* note 123.

[156] *Id.*

[157] Chemical Security Act of 2002, H.R. 5300, 107th Cong. § 4(a)(1) (2002).

[158] *Id.* at § 4(a)(3)(A)(i).

[159] *Id.* at § 4(a)(3)(A)(ii).

[160] *Id.* at § 4(a)(3)(A)(iii).

[161] *Id.* at § 4(a)(3)(B).

[162] *Id.* at § 4(a)(3)(C).

[163] *Id.* at § 4(a)(4).

[164] *Id.* at § 4(b)(1)(A), (2)(A).

[165] *Id.* at § 4(b)(1)(B), (2)(B).

[166] *Id.* at § 4(b)(3)(A).

[167] *Id.* at § 4(b)(3)(B)(i), (ii).

[168] *Id.* at § 4(b)(4)(A).

[169] *Id.* at § 4(b)(4)(B)(i)-(iii).

[170] *Id.* at § 5(a)(1).

[171] *Id.* at § 5(a)(2)(A), (B).

[172] *Id.* at § 5(a)(2)(D)(ii).

[173] *Id.* at § 5(c)(1).

[174] *Id.* at § 5(c).

[175] *Id.*

[176] *Id.*

[177] *Id.* at § 5(c)(1), (2).

[178] *Id.* at § 5(c)(1), (2).

[179] *Id.* at § 5(c)(1).

[180] *Id.* at § 5(c)(2).

[181] *Id.* at § 5(c)(3)(A).

[182] *Id.* at § 6(2)(A), (B).

[183] *Id.* at § 7(a), (b)(1), (2).

[184] Chemical Security Act of 2001, *supra* note 15 at § 4 (a)(1)-(4), (b)(1)-(3); Chemical Security Act of 2002, *supra* note 157 at § 4(a)(1)-(5).

[185] 42 U.S.C. § 7412 (r)(7)(iii).

[186] 42 U.S.C. § 7414 (c).

[187] *Id.*

[188] *Publicizing Chemical Risks, supra* note 11, at A6.

[189] *See, e.g.*, 58 Fed. Reg. 54190, 54192 (1993); 61 Fed. Reg. 31667, 31673 (1996); 65 Fed. Reg. 48108 (2000).

[190] *See* 65 Fed. Reg. 48108, 48109 (2000).

[191] *See* 65 Fed. Reg. 48109.

[192] Pub. L. 106-40 §§ 2(a), 3 (Aug. 5, 1999), which added a sub paragraph (H) to § 112(r)(7).

[193] 42 U.S.C. § 112(r)(7)(H)(ii), (iii) (2000).

[194] *Id.*

[195] 65 Fed. Reg. 48108 (Aug. 4, 2000), *codified at* 40 C.F.R. Part 1400.

[196] 65 Fed. Reg. at 48112.

[197] 40 C.F.R. § 1400.3.

[198] *Id.* § 1400.b.

[199] *Chemical Security Hearings, supra* note 2 (testimony of Paul Orum, Director, Working Group on Community Right-to-Know).

[200] Freedom of Information Act, 5 U.S.C. § 552 (2000).

[201] *Id.* § 552(b)(1).

[202] Exec. Order No. 12,958, 3 C.F.R. (1995) as *reprinted as amended in* 50 U.S.C. § 435 app. (2000).

[203] *See Halpern v. Federal Bureau of Investigation*, 181 F.3d 279 (2d Cir. 1999).

[204] Exec. Order No. 12,958, *supra* note 202.

[205] *Id.* at § 1.1(c).

[206] *See id.* § 1.4. The classification authorities are the President, those agency heads and officials specially designated by the President, and their delagees. *Id.* at § 1.4(a).

[207] *Id.* at § 1.1(*l*).

[208] *Id.* at § 1.5(e). Subsection (f), while not directly germane, is also interesting because it reflects the Government's commitment to the protection of nuclear information, above and beyond that related to "military plans, weapons systems or operations." *Id.* § 1.5(a). It includes Government programs for safeguarding nuclear materials or facilities." *Id.* § 1.5(f).

[209] *Id.* § 1.2(a)(2).

[210] Freedom of Information Act, *supra* note 200; Exec. Order No. 12,958, *supra* note 202.

[211] 345 U.S. 1 (1953).

[212] United States v. Reynolds, 345 U.S. at 10.

[213] 133 F.3d 1159 (9th Cir. 1998).

[214] *Id.*

[215] *Id.* at 1165.

[216] *Id.* at 1166

[217] *Id.* at 1167 *quoting Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1144 (5th Cir. 1992).

[218] Criminal defendants' access to and use of classified information that may be related to their defense is governed by the Classified Information Procedures Act, 18 U.S.C. App. 3 (2000). *See United States v. Pappas*, 94 F.3d 795 (2d Cir. 1996).

[219] Jeff Johnson, *The Vanishing Risk Management Plan*, Chemical and Engineering News, Feb. 25, 2002, at 27; *White House Directs Agencies to Review Material, supra* note 17.

[220] Meredith Preston, *Researcher Says Work May Be Impeded By Restrictions on Environmental Database*, 60 Daily Environment Report A-5, (March 28, 2002), *at* http://ippubs.bna.com/ip/BNA/DEN.NSF/33973f565fe8e8e085256743006dd9e3/db5c572ae0663fb885256b8a000a0466?OpenDocument; *White House Directs Agencies to Review Material, supra* note 17.

[221] *White House Directs Agencies to Review Material, supra* note 17.

[222] Bill Sammon, *Websites Told To Delete Data,* The Washington Times, March 21, 2002.

[223] *Id.*

[224] Id.

[225] Community Protection from Terrorism Act, S. 2579, 107th Cong., 2d Sess. § 2 (2002).

[226] Chemical Safety Information, Site Security and Fuels Regulatory Relief Act, P.L. 106-40, 113 Stat. 207 (Aug. 5, 1999).

[227] Community Protection from Terrorism Act, *supra* note 225 at 7, proposed § 112(r)(7)(H)(ii).

[228] *Id.* at 7-8, proposed § 112(r)(7)(H)(iii). The bill would lend extra punch to this provision by defining "member of the public" to include an official user who is not carrying out an official use. *Id.* at 3, proposed 112(r)(7)(H)(i)(III).

[229] *Id.* at 7-8, proposed § 112(r)(7)(H)(iii).

[230] *Id.* at 8, proposed § 112(r)(7)(H)(iii)(II).

[231] *Id.* at 9, proposed § 112(r)(7)(H)(iii)(IV).

[232] *Id.*

[233] *Id.* at 10, proposed § 112(r)(7)(H)(iv)

[234] *Id.* at 11-12, proposed § 112(r)(7)(H)(vi)

[235] *Id.* at 13, proposed § 112(r)(7)(H)(vii)

[236] Section 271 of the Atomic Energy Act of 1954, as amended, generally provides for federal preemption of state laws related to the licensing and operation of commercial power reactors. 42 U.S.C. § 2018. *See* County of Suffolk v. Long Island Lighting Co., 728 F.2d 52, 59 (2d Cir. 1984) (action seeking inspection and prohibition on operation of reactor was precluded by § 221). Citizens for an Orderly Energy Policy v. Suffolk County, 1604 F. Supp. 1084, 1090 (E.D.N.Y. 1985) (the Act "does not provide for private enforcement of its terms").

[237] *See generally* 10 C.F.R. Chapter I (2000).

[238] The Atomic Energy Act of 1954, as amended (*e.g.*, Sections 3(c) and (e)), and the Energy Reorganization Act of 1974 (Section 204(b)(1)), 42 U.S.C. § 2011, *et seq.* and 42 U.S.C. § 5801 *et seq.* (2000), respectively.

[239] *See* 10 C.F.R. § 73.1(a) (2002).

[240] 10 C.F.R. § 73.1(a) (2002).

[241] *See* NRC Manual Chapter 0609, "Significance Determination Process," Appendix E.

[242] 10 C.F.R. § 50.13 (2002).

[243] *Siegel v. Atomic Energy Commission*, 400 F.2d 778, 784, 130 U.S. App. D.C. 307, 313 (1968).

[244] *Siegel v. Atomic Energy Commission*, 400 F.2d 778, 781, 783 (D.C. Cir. 1968).

[245] Statement Submitted by Chairman Richard A. Meserve (NRC) to the Committee on Environment and Public Works, United States Senate, Concerning Nuclear Security Infrastructure, p.3 (November 1, 2001). In addition, the defense-in-depth philosophy used in nuclear facility design means that plants have redundant and physically separated systems to ensure the availability of required safety functions that protect public health and safety. 10 C.F.R. Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants" (2002).

[246] NUREG/CR-2859, "Evaluation of Aircraft Crash Hazards Analysis for Nuclear Power Plants," June 1982, p. 11. The Three Mile Island units were designed to withstand the accidental crash of a Boeing 727 jetliner, which is a smaller aircraft than the ones used in the September 11, 2001, terrorist attacks.

[247] During a speech at the National Press Club in Washington, D.C., Homeland Security Director Tom Ridge, when questioned about security at nuclear power plants, stated that "the threat design of nuclear facilities has to be reconsidered" and there may ultimately be "bricks-and-mortar adjustments that are made to some of these facilities." National Press Club Luncheon Remarks by Tom Ridge, Director of the Office of Homeland Security, The National Press Club, Washington, DC, February 7, 2002.

[248] 10 C.F.R. § 73.55 (2002).

[249] *Id.*

[250] *See* 10 C.F.R. § 50.47 and 10 C.F.R. Part 50, Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities" (2002).

[251] 147 Cong. Rec. H8731 (daily ed. Nov. 29, 2001).

[252] 147 Cong. Rec. S12,167-S12,169 (daily ed. Nov. 29, 2001).

[253] Section 3 of the Senate bill (S.1746) and Section 3 of the House bill (H.R. 3382) propose federalizing plant security forces and re-evaluation of the DBT at intervals not to exceed three years to include at least threats equivalent to the events of September 11, 2001. The effect of such action would be to reverse the precedent set by Siegel and hold moot the provisions of 10 C.F.R. § 50.13.

[254] Transcript of testimony by NRC Chairman Richard A. Meserve before the Senate Environment and Public Works Committee (107th Congress) concerning nuclear power plant security (June 5, 2002).

[255] *See generally, supra* note 248.

[256] *See generally* 10 C.F.R. Part 73, Appendix B, "General Criteria for Security Personnel" (2002). These include fingerprint submittal for an FBI criminal record check; physical and psychological testing and screening; credit and reference checks; education and work history verification; and routine drug and alcohol screening.

[257] 10 C.F.R. Part 73, Appendix B, Criterion II, "Training and qualifications" (2002). Initial training includes NRC requirements for nuclear facility physical security, recognition of sabotage devices and equipment, contraband detection devices and operation, firearms proficiency, and tactical response training. Annual supplemental training covers areas such as weapons proficiency, physical readiness, stress fire course, force-on-force drills, and table top drills.

[258] 10 C.F.R. Part 73, Appendix B, Criterion II.e, "Requalification" (2002).

[259] *See* 10 C.F.R. § 50.47 and 10 C.F.R. Part 50, Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities" (2002).

[260] *See* NUREG-0654, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparations in Support of Nuclear Power Plants," Rev. 1 (Nov. 1980).

[261] 10 C.F.R. § 50.47(b)(4) (2002).

[262] 10 C.F.R. Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants" (2002).

[263] Two of these areas, the Protected Area and the Vital Areas, are specifically discussed in 10 C.F.R. § 73.55; however, the third area, the owner controlled area, is not addressed by regulation. The owner controlled area is used by licensees as an area of control (*i.e.*, exclusion) outside the perimeter of the Protected Area. The Protected Area encompasses the Vital Areas, and the owner controlled area contains the Protected Area.

[264] 10 C.F.R. § 73.2 (2002).

[265] *supra* note 248.

[266] 10 C.F.R. § 73.2 (2002).

[267] National Press Club Speech by Dr. Richard A. Meserve, Chairman, U.S. Nuclear Regulatory Commission, The National Press Club, Washington, DC, January 17, 2002. NRC Office of Public Affairs Speech No. S-02-001.

[268] NRC Information Notice 98-35, "Threat Assessments and Consideration of Heightened Physical Protection Measures" (September 4, 1998). The notice describes additional physical protection measures that the NRC suggests be considered for threat conditions detailed in the document. The document is marked "Safeguards Information" and must be accorded the protection required under 10 C.F.R. § 73.21.

[269] NRC Press Release No. 02-04, "NRC Forms Office of Security to Streamline Security, Safeguards and Incident Response Activities" (April 5, 2002).

[270] Weekly Compilation of Presidential Documents, Vol. 38, No. 5, "Address Before a Joint Session of the Congress on the State of the Union, January 29, 2002," p. 134 (Feb. 4, 2002).

[271] 10 C.F.R. § 2.202 provides for the issuance and required response to such Orders.

[272] 67 Fed. Reg. 9792, "All Operating Power Reactor Licensees; Order Modifying Licenses (Effective Immediately)" (March 4, 2002).

[273] Atomic Energy Act of 1954, as amended, Section 147, "Safeguards Information," as codified at 42 U.S.C. § 2167 (2000).

[274] 10 C.F.R. § 73.21 (2002).

[275] 10 C.F.R. §§ 73.80 and 73.81 (2002).

[276] *See* 10 C.F.R. Part 95 (2002).

[277] *See* 67 Fed. Reg. 60,266 "Deployment of the NRC's Redesigned Public Web Site: Notice of Availability" (Dec. 3, 2001).

[278] *See* COMSECY-02-0015, "Withholding Sensitive Homeland Security Information From the Public," April 4, 2002.

[279] Pub. L. No. 85-256, *adding, inter alia,* §§ 2(i), 170 to the Atomic Energy Act of 1954, codified at 42 U.S.C. §§ 2012(i), 2210. The majority of the amended Act is now codified in 42 U.S.C. § 2210 (2000).

[280] This total is based on the following calculation: There are 104 licensed power reactors subject to retrospective premiums. At up to $88.095 million for each, pursuant to the requirements of 10 C.F.R. § 140.11 , there potentially would be ($88.095 million x 104) = $9,161,800,000 in the secondary layer of insurance. Adding the $200,000,000 in primary insurance, total insurance, and the corresponding liability limit, for 104 reactors would be just under $9.4 billion.

[281] 42 U.S.C. § 2210(b).

[282] 10 C.F.R. § 140.11(a)(4).

[283] The figures given in the text include two inflation adjustments by NRC in 1993 and 1998 pursuant to 42 U.S.C. § 2210(t), as reflected in 10 C.F.R. § 140.11.

[284] 42 U.S.C. § 2210(c).

[285] H.R. 2983 passed the House of Representatives on November 27, 2001. The House bill extends both NRC and DOE Price-Anderson authority for fifteen years. The Senate bill, S. 517, passed on April 25, 2002, extends NRC authority for only ten years while making DOE Price-Anderson authority permanent. The bills have other differences that are being addressed in the conference.

[286] Protection for new facilities had lapsed on August 1, 1987, but the Act was reauthorized on August 22, 1988, Pub. L. No. 100-408, 100th Cong., *reprinted in* 1988 U.S.C.C.A.N. 1476.

[287] *See* the Nuclear Energy Institute's "About NEI" page *at* http://www.nei.org/doc.asp?catnum=2&catid=136.

[288] The Nuclear Energy Institute was founded in 1994 from the merger of several nuclear energy industry organizations, the oldest of which was created in 1953. Specifically, in 1994, NEI was formed from the merger of the Nuclear Utility Management and Resources Council (NUMARC), which addressed generic regulatory and technical issues; the U.S. Council for Energy Awareness (USCEA), which conducted a national communications program; the American Nuclear Energy Council (ANEC), which conducted government affairs; and the nuclear division of the Edison Electric Institute (EEI), which handled issues involving used nuclear fuel management, nuclear fuel supply, and the economics of nuclear energy.

[289] *See* the Nuclear Energy Institute's "About NEI" page *at* http://www.nei.org/doc.asp?catnum=2&catid=136.

[290] As an example, NEI has generated documents that have been found acceptable (*i.e.*, endorsed) by the NRC Staff which are typically very comprehensive and contain examples on which licensees can rely.

[291] Article II, Section 2 names the President the Commander in Chief of the Army, the Navy, and of the Militia, when it is called to national service.

[292] *Id.* at § 4(b)(4)(A).

[293] *Id.* at § 4(b)(i)-(iii).

[294] The Three Mile Island accident occurred on March 28, 1979.

[295] After the accident, the NRC issued additional requirements documents governing the design of certain accident systems such as, human factors engineering, environmental qualification, and post-accident sampling. Many of these reactive requirements did not provide a true safety benefit, but did require focused effort by licensees.

[296] 53 Fed. Reg. 20610 (June 6, 1988), *as amended at* 54 Fed. Reg. 15398 (Apr. 18, 1989).