



Special Committee on Homeland Security Newsletter

Vol. 2, No. 1

July 2006

WELCOME!

Joan Krajewski
Newsletter Editor
Microsoft Corporation

Scott Mitchell
Committee Chairperson
Gunster, Yoakley & Stewart P.A.

Welcome to this edition of the Special Committee for Homeland Security's Newsletter! The newsletter is designed to provide you with articles that provide important information and insightful analysis on selected topics in this new and rapidly expanding area of the law.

The mission of our committee is to provide a forum for discussion of homeland security measures and addresses national and state developments and evolving policy. The scope of our focus is grouped into four general areas: (1) the emergencies and disasters practice including risk-based emergency management planning and prevention, response and recovery, and assistance efforts; (2) the travel and transportation area focusing on customs inspections, border protection, airport security and dangerous goods; (3) the research and technology practice area addressing procedures for preparing for and responding to the full range of terrorist threats; and (4) the threats and protection practice area including the National Advisory System, protection of public buildings and critical infrastructure, health and safety, and related government enforcement.

In this newsletter, we focus on perspectives from industry related to implementation of Inherently Safer Technology by chemical companies and the balance between privacy rights and security struck by the Department of Homeland Security. Finally, we provide a summary of a recent decision by the Ninth Circuit Court of Appeals in which the court addresses the relationship between an agency's consideration of environment impacts of a proposed federal action under the National Environmental Policy Act (NEPA) and the potential for terrorist acts. We hope that you'll find the newsletter to be a good read and beneficial to your practice.

We encourage you to become involved and welcome letters to the editor, comments and article submissions. Interested in more? Our committee continues to be very active, and we welcome your participation. Our committee recently co-sponsored a "Quick Teleconference" entitled: *Sustaining America's Infrastructure in the Face of a Pandemic: What Environment, Energy & Resources Lawyers Need to Know*. Additionally, the Section of Environment, Energy, and Resources has formed a Special Task Force in response to hurricanes Katrina and Rita, in which a number of our committee members are active. Our vice chair for Programs, Michael Penders, is currently soliciting assistance and ideas for our next program. Finally, be sure to check out an excellent update of homeland security jurisprudence in the Section's *2005 The Year in Review*, authored by our vice chair, Charles Wagner.

**Special Committee on
Homeland Security Newsletter
Vol. 2, No. 1, July 2006
Joan Krajewski, Editor**

In this issue:

Welcome!

Joan Krajewski and Scott Mitchell 1

Chemical Plant Security Legislation and
“IST”: The Misperception Surrounding
“Inherently Safer Technology”

Ava A. Harter 2

Achieving Both Privacy and Security—
Improving the DHS Approach

Lisa E. Funk 6

NRC Required to Consider Terrorist
Attack in NEPA Analysis

Joan Krajewski 9

© 2006. American Bar Association. All rights reserved. The views expressed herein have not been approved by the ABA House of Delegates or the Board of Governors and, accordingly should not be construed as representing the policy of the ABA.

This newsletter is a publication of the ABA Section of Environment, Energy, and Resources, and reports on the activities of the committee. All persons interested in joining the Section or one of its committees should contact the Section of Environment, Energy, and Resources, American Bar Association, 321 N. Clark St., Chicago, IL 60610.



Please feel free to contact us (Joan Krajewski at joankr@microsoft.com; Scott Mitchell at smitchell@gunster.com). You can join our committee by filling out the on-line committee preference form at [www.abanet.org/environ/committees/!](http://www.abanet.org/environ/committees/)

**CHEMICAL PLANT SECURITY
LEGISLATION AND “IST”:
THE MISPERCEPTIONS SURROUNDING
“INHERENTLY SAFER TECHNOLOGY”**

**Ava A. Harter
The Dow Chemical Company**

Policy analysts, the Justice Department, homeland security experts and the President of United States have all recognized that chemical facilities are a potential target for a terrorist attack and should be uniformly regulated by the national government. Multiple bills have been introduced over the past five years to complete this critical task, but they continue to languish in Congress. Members of the American Chemistry Council (ACC), however, did not wait for governmental direction to enhance security at their chemical plants. Since the events of 9/11, ACC members have spent over \$3 billion strengthening chemical security and have adopted a rigorous security code requiring completion of vulnerability assessments and implementation of security enhancements at all U.S. sites. Although the efforts of ACC members and those that followed suit cover the vast majority of the chemical industry, there are laggards that must be brought up to the same level and this can only be done by federal legislation. It is imperative that the U.S. government act now and charge the Department of Homeland Security (DHS) with exclusive control to administer clear, strong and consistent chemical security measures. Such actions must preempt state and local piecemeal legislation and fulfill the national security need for uniform regulations to protect our facilities national commerce while building upon the extensive work undertaken by DHS and private industry.

The Dow Chemical Company (Dow), a leader in the chemical industry, supports implementation of federal

security measures and is pushing for uniform U.S. legislation to establish stringent, risk-based performance standards for all chemical manufacturers to meet. Unfortunately, the chemical industry's call on Congress for effective and meaningful regulations has been sidetracked by misplaced focus on the role and definition of Inherently Safer Technology (IST). IST refers generally to one of several approaches (see Table 1) that are perceived to eliminate or significantly reduce risks associated with petrochemical or refining processes.

The philosophy behind IST has been long championed and espoused by chemical companies as part of the essential arsenal of risk management and process safety strategies. IST, however, is not a panacea for safe operations or site security. Implementation of inherent safer technology approaches must complement other risk reduction strategies and be evaluated by the professionals who understand the chemistry. It should not be mandated by federal law as favored by some. It is neither feasible nor practical.

It is not the consideration of IST that is the issue; it is the mandating of select and prescriptive IST requirements and using an incongruous definition. The experts in the field are best suited to identify, discover, determine and deploy the methods needed to meet or exceed governmental standards to secure our chemical sources. Professionals who know and understand the chemistry and manufacturing processes should be the ones who decide what safeguards are most effective based upon relative risk and the hazards associated with the entire supply chain of the chemical or process being reviewed. Misapplying or manipulating the purpose or definition of IST could unwittingly lead to creation of greater risks or merely shift risk at a cost to the public. Further, granting the authority to agencies allowing them to make business decisions and to mandate the phase-out of chemicals with important consumer benefits is not proper. Such actions could stifle innovation and compromise intellectual property needs and competition while interfering with industrial productivity essential to our national economy. It is the government's appropriate role to set significant standards requiring comprehensive vulnerability assessments and security and emergency response

plans and for chemical businesses to determine how best to meet those requirements.

IST is an Intrinsic Part of Everyday Safety and Security

All processes and materials are made up of multiple hazards, and safety and security are only achieved when all the risks are evaluated by the experts and not with the short-sighted emphasis on one chemical or one process. It is critical that companies utilize a holistic approach based upon expertise, experience, technology know-how and continuous assessments to improve and secure processes based upon governmental and industry-defined performance standards. In combination with federal regulations that would require facilities to manage risk, the following types of strategies demonstrate how IST can be used as part of a company's overall approach and commitment to security and safety.

As examples, Dow applies these processes and others to the extent the chemistry allows and the risk assessment supports:

- Inherently safer technologies are considered at a very early stage of designing any new chemical manufacturing facility per the Dow Global Project Methodology (GPM).
- The hazards of the existing process technology and the potential to reduce risks utilizing more inherently safer technologies are evaluated each three to five years as part of the Dow Reactive Chemical/Process Hazards Analysis for each Dow plant.
- Dow utilizes Process Safety experts in conjunction with Security experts in performing the Security Vulnerability Assessments (SVA) which are required per the ACC Responsible Care Security Code. In these SVA reviews, the use of IST alternatives is considered in addition to traditional security alternatives as mechanisms to reduce potential off-site chemical impacts associated with a security incident.

Assessing and implementing inherently safer designs and processes are standard operating procedures for

- Intensification: This calls for using smaller quantities of hazardous substances within a process.
- Substitution: This calls for replacing one material with a less hazardous substance.
- Attenuation: This calls for using less hazardous conditions such as lower temperature or pressure or a less hazardous form of material.
- Limitation of effects: This calls for designing a plant or process to minimize the impact of a release of material or energy. For example, Dow uses small diameter piping in some of its processes to limit the flow rate in the event of an accidental release, making it almost impossible for an adverse reaction to occur too quickly.
- Simplification and error tolerance: This calls for designing a process to reduce or better tolerate operating errors by making the plant more user-friendly and reliable, such as using hard piped connections in lieu of hoses to reduce risk of leaking.

Table 1: Inherently Safer Technology Strategies.

chemical companies, but process safety is exceedingly complicated, and there is no one reliable measurement or standard. When evaluating IST options, the risk management professional must also consider strategies such as passive safeguards, active controls and mitigation, physical enhancements and formal operating disciplines. It is important that government does not step in to prescriptively define what the professional or company must do in the name of security or safety, but rather, that it sets risk-based performance standards that covered companies must meet or exceed.

The Misperception of IST as a Perfect Solution

With decades of experience in applying IST, Dow has learned that IST can be misapplied and result in higher risk if the “big picture” is not properly considered. A mistaken approach merely shifts the risk from one area to another, and may create new and greater hazards or amplify the magnitude of an existing hazard. Consider these examples:

1. Minimizing the size of raw material storage tanks has been proposed as an IST that will reduce potential impact in the process area; however, other risks may increase. If the tank is smaller than the shipping container, there is a higher risk of overflowing the tank. A smaller tank will require more frequent loading or unloading, increasing the opportunity for spills. Further, a smaller tank size may require more shipments meaning more trucks carrying hazardous materials up and down the highway and increasing transportation risks.
2. Substituting bleach for chlorine in water treatment reduces risk at the site of the water treatment plant but increases the amount of chlorine required at the bleach manufacturing site. The irony of this high profile issue is that chlorine is still the active ingredient in the bleach. Someone somewhere has to use chlorine to produce the bleach in the first place so the water treatment unit can handle the safer form of chlorine. If the bleach manufacturer who now has to use more chlorine is located in

an area that is highly populated, chlorine must be shipped through that community. This scenario merely shifts, not eliminates, the risk. Also, because bleach requires more product volume to get the equivalent amount of active ingredient, shipments are actually increased. This fact results in additional transportation risks from the increased shipments, not to mention increased energy consumption and associated air emissions.

3. Substituting Freon refrigerants with “inherently safer” ammonia-based refrigerant systems were recommended for many years. This resulted in shifting hazards associated with ozone-depleting chlorofluorocarbons (CFCs) to greater health risks and injuries, and even fatalities, from fire, explosions and toxicity associated with the alternatives such as ammonia.

Based upon the risks of misapplying IST, mandating it in legislation is illogical and unsound. The complexity of process plants essentially prevents any prescriptive rules that would be widely applicable and runs contrary to the “one-size fits all” governmental approach which focuses on a single process or site. IST is best applied by technical experts who are very familiar with the process technology and that understand the need for a holistic approach and the domino effects that can be created by a change—site by site and product by product or molecule by molecule.

This begs the question as to why IST continues to resurface as a component recommended by some for inclusion in security regulations. The most likely culprit is perpetuation by the media and the uninformed of exaggerated risks associated with potential chemical releases. There is also a misperception that chemical sources are not secure and that companies will not adequately assess risks if left to their own devices. Further, criticism tends to be premature without accurate knowledge or facts about what chemical companies are doing or what risks are at play when IST is discussed. To dissuade lack of public confidence, it is important that companies publicly demonstrate their commitment to securing their sites.

They must also share knowledge and efforts on alternative processes and chemicals, and show how industry is continuously striving to improve security and safety. At the same time, it is critical that federal action be taken setting stringent compliance risk-based performance standards for all covered companies to meet.

Hope in the Current Legislative Climate

Safety and security are achieved by applying layers of protection including adding safety devices, stronger containment, impenetrable seals and well trained personnel as well as eliminating risk by reducing quantities, changing the material so that it is safer and assessing the viability of replacements. However, it is not a simple evaluation or application and it is neither appropriate nor practical for government to prescriptively regulate the specific measures, technologies or processes that companies must implement to address overall risk. National legislation is needed but one that encourages evaluation and implementation of performance based measures based upon risks and not one that mandates the implementation of any one security or risk reduction tool.

Sen. Susan Collins (R-Maine), the chair of the Senate Homeland Security and Governmental Affairs Committee, and ranking member Sen. Joseph Lieberman (D-Conn.) authored a comprehensive and balanced piece of legislation last year, the Chemical Facility Anti-Terrorism Act of 2005 (S. 2145). The legislation focuses on assessing and effectively managing risks at chemical plants by requiring vulnerability assessments, development of security plans and emergency response plans, and implementation of performance-based security measures. The bill also incorporates the requirements found in other federal legislation, such as the Maritime Transportation Security Act of 2002, and builds upon the proven strengths of the industry. The most serious concern with the bill is it does not preempt state action and jeopardizes the national interest in having a uniform anti-terrorist strategy for chemical plant security. State and local governments cannot be allowed to promulgate different or piecemeal regulations that frustrate the need for uniformity when national security

and the national economy are at issue. Sen. Voinovich (R-Ohio) reportedly is proposing to amend the bill to address this concern as well as others. With the amendments, this Bill has promise to be the most effective, stringent and comprehensive security initiative for industry. In a parallel track, a similar bill has been introduced in the House by Rep. Vito Fossella (R-N.Y.).

Four Senate Democrats, Illinois Sens. Barack Obama and Dick Durbin, and New Jersey Sens. Frank Lautenberg and Bob Menendez, have also introduced chemical plant legislation; however, it is based upon mandating prescriptive IST which, as shown above, is potentially detrimental and stagnating. In addition, the bill heavily and unnecessarily overlaps with already effective safety and environmental laws and is unfortunately confusing the debate on real security measures and policies.

Conclusion

Chemicals are what allow companies to reach the breakthrough products that consumers demand for building materials that protect our homes and cars, medicine and disinfectants that protect our health, pesticides and biocides that protect our food, and filtering membranes that clean our water. However, to the extent the chemical manufacturing sector is about innovation and enhancing the way we live, it also is about dealing safely and responsibly with hazardous materials. With elevated homeland security concerns, the use of hazardous materials requires heightened security at chemical plants, and we in the chemical industry are calling upon Congress to act now to bring all companies up to the same stringent standards. Being in the business of chemistry requires being a responsible corporate citizen and uncompromising when it comes to safety, security and pollution prevention. As a result, the chemical manufacturing sector is one of the safest in industry, and with sensible regulations, promises to be one of the most secure.

Ava A. Harter is a senior attorney at The Dow Chemical Company in Midland, Michigan. She counsels the company on environmental, emergency services and security matters.

ACHIEVING BOTH PRIVACY AND SECURITY— IMPROVING THE DHS APPROACH

Lisa E. Funk
American Airlines, Inc.

Privacy as an abstract concept has been important to Americans as long as the United States has existed. Americans have sought to keep their personal lives private, whether in the exercise of religion, the pursuit of happiness or in the spirit of “freedom” in general.

Recent years have brought increased national security concerns as the development of the Internet and advances in the ability to store and sort huge volumes of data has skyrocketed. This has opened up new opportunities to use personal information for marketing, meeting consumer demands, improving government services and promoting national security. At the same time, ease of access to electronically held personal information has increased the incidence of identity theft and concerns for the privacy of individual personal data. In modern terms, personal privacy has now expanded to include not only physical privacy but also protection of personally-identifiable information.

The dual—and sometimes dueling—goals of national security and individual privacy have become a frequent focus of debate among security and privacy law experts. One of the biggest areas of debate is whether any privacy rights should be given up in order to promote national security. In air travel, for example, passengers’ information is compared with government watch lists in an effort to prevent terrorists from getting access to planes. Transportation Security Administration and Customs and Border Protection officials regularly review travelers’ identification before allowing them access to planes or to the United States. On the physical privacy side, new backscatter x-ray technology also allows airport screeners in some locations to see what, if anything, may be hidden under travelers’ clothing. Frequently, discussion centers on how much privacy should be relinquished in order to increase security.

However, those who talk about reaching a “balance” between privacy and security miss the fact that each

can be achieved without diluting the other. *See generally*, Jennifer Granick, *Security vs. Privacy: the Rematch*, WIRED NEWS, May 23, 2006, available at www.wired.com/news/columns/0,709710.html?tw=wn_technology_2. Privacy and security do not have to be mutually exclusive. In fact, the public and members of Congress have increasingly demanded that privacy not be diluted in the name of security. *See, e.g., In Testimony, Hayden Defends Domestic Spying*, COX NEWS SERVICE, May 19, 2006, available at www.kansascity.com/mld/kansascity/news/politics/14614902.htm.

The Department of Homeland Security (DHS) has a framework designed to both protect privacy of individual citizens' personal information and to enhance national security. In practice however, these two efforts do not always succeed.

The DHS Approach

DHS was the first federal department or agency to establish and fully staff a Privacy Office mandated "to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity" of DHS security measures. www.dhs.gov/dhspublic/interapp/editorial/editorial_0338.xml. Even with this active office in place and led by strong chief privacy officers, DHS has still faltered publicly on data security matters. The department recently earned its second "F" in a row on the annual computer security practices report card released by the House Committee on Government Reform. Computer Security Report Card, Mar. 16, 2006, prepared by the Government Reform Committee of the U.S. House of Representatives.

The DHS Privacy Office serves multiple roles within the department, including ensuring that Privacy Impact Assessments are performed prior to implementation of new projects that involve information gathering or data storage. The Privacy Office also takes responsibility for monitoring and assisting various DHS projects with establishing and maintaining compliance with the public notification and disclosure requirements of the Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, codified as amended, 5 U.S.C. § 552a. *See* www.dhs.gov/dhspublic/interapp/editorial/

editorial_0338.xml. In the past, the DHS has canceled programs due in part to privacy concerns raised by the Department's Privacy Office. *See* GOV'T ACCOUNTABILITY OFF., AVIATION SECURITY: TRANSPORTATION SECURITY ADMINISTRATION DID NOT FULLY DISCLOSE USES OF PERSONAL INFORMATION DURING SECURE FLIGHT PROGRAM TESTING IN INITIAL PRIVACY NOTICES, BUT HAS RECENTLY TAKEN STEPS TO MORE FULLY INFORM THE PUBLIC (July 22, 2005) at 3 (hereinafter "Aviation Security").

Despite best efforts of the Privacy Office staff, this laudable oversight program has suffered a number of setbacks. For example, the Government Accountability Office (GAO) revealed last year that the Transportation Security Agency (TSA) had exceeded the scope of published Federal Register notices to collect personal information on nearly 200,000 people from commercial data brokers. *See* GAO: TSA data collection violated Privacy Act, ASSOCIATED PRESS, July 22, 2005, available at www.msnbc.msn.com/id/8672258/. According to the GAO's letter submission to a group of Congressional Committees, TSA violated the Privacy Act by the failure to fully disclose to the public its use of personal information in fall 2004 notices. "Aviation Security," at 1. The GAO stated that TSA only filed a corrective Federal Register notice after collecting the initially undisclosed information and after GAO briefed TSA on its privacy protections concerns. *Id.* at 1-2.

The increasing reliance of DHS agencies on unverified data gathered by commercial data brokers to develop various data pools aimed at tracking trends that may pose threats to national security has particularly raised privacy concerns as it has come to light. Certain of the data brokers at issue, including ChoicePoint and LexisNexis, suffered their own data breaches in 2005 when personal information on more than 100,000 individuals was unwittingly sold to fraud rings. *See generally*, Robert O'Harrow Jr., *Agencies Not Protecting Privacy Rights*, GAO Says, WASH. POST, Apr. 5, 2006, at A-9. The GAO reported in April 2006 that DHS, the Justice Department and two other agencies together spent about \$30 million in 2005 for information gathered from such data brokers. GOV'T ACCOUNTABILITY OFF., PERSONAL INFORMATION:

AGENCY AND RESELLER ADHERENCE TO PRIVACY PRINCIPLES (Apr. 2006).

Soon after its inception, the DHS Privacy Office identified as one of its top three issues “the use of private sector information for homeland security purposes.” Letter from Steven J. Pecinovsky, Director, DHS Departmental GAO/OIG Liaison Office, to Linda Koontz, Director, Information Management, Government Accountability Office (Mar. 17, 2006), incorporated as Appendix IV, “Comments from the Department of Homeland Security” to GOV’T ACCOUNTABILITY OFF., PERSONAL INFORMATION: AGENCY AND RESELLER ADHERENCE TO KEY PRIVACY PRINCIPLES. The Privacy Office has published guidance to DHS on Privacy Impact Assessments that include directions relevant to the collection and use of commercial data. *Id.* In addition, the Privacy Office published an updated version of this guidance in 2006 both internally at DHS and on the Department’s external web site. *Id.* Yet, DHS performance still is deemed inadequate in GAO reports and on the annual computer security practices report card.

Changing for the Better

The key to improving DHS performance in addressing privacy concerns is to raise privacy protection in the collective consciousness of DHS personnel beyond just a laudable goal. Privacy protection must be an equal primary duty of each DHS employee along with ensuring the nation’s security. Advisories and recommendations of the DHS Privacy Office must be considered and incorporated into DHS decisions at every development in both new and ongoing projects. Security can be achieved without collecting and retaining personal data on a large swath of innocent civilians. Moreover, unverified personal data available in the marketplace is unlikely to provide much value even if it can be reviewed.

A great many security initiatives indeed require no personally-identifiable data whatsoever. Motion-detecting scanners, security keys and other high-tech tools can be used successfully without incorporating any personal information into their operating chips. When personal information must be collected or reviewed

against terrorist watch lists or other security tools, DHS must clearly and publicly state how such information will be handled and comply with every other requirement of the Privacy Act. In addition, DHS must ensure that such collected personal information is safely returned or destroyed as soon as possible after review determines that the subject person poses no threat.

DHS recently has been considering using radio-frequency identification chips and biometric tools for a number of border and other security projects. Great care must be used to ensure that any biometric data collected or used for DHS purposes be secured, encoded and protected by institutional measures that limit access to such information to a select few DHS employees with a true “need to know.” In DHS programs where biometric data such as eye scans and fingerprints are already in use, a regular recurring review process must ensure not only that each program provides a cost-efficient security value but also that each program responsibly respects and protects the privacy of participants. As DHS continues to grow, this will require commensurate expansions of the staff and influence of the DHS Privacy Office and standing advisory committees under its auspices to perform initial reviews and necessary recurrent auditing. *See, e.g.,* Renee Boucher Ferguson, *DHS Subcommittee Questions RFID Security*, EWEEK, May 24, 2006, available at www.eweek.com/print_article2/0,1217,a=179223,00.asp.

As a key element of the federal government, DHS must remain ardently attuned to the fact that protecting the security of this nation necessarily includes protecting the core values of liberty and freedom on which the country has been built. Throughout our history, liberty and freedom has included the rights of law-abiding individuals to be secure in reasonable expectations of personal privacy. This must be paramount.

Lisa E. Funk is an attorney for American Airlines, Inc. who handles a broad range of data privacy issues. The opinions expressed in this article are solely her own and do not necessarily reflect opinions or positions of American Airlines, Inc. or its affiliates.

NRC REQUIRED TO CONSIDER TERRORIST ATTACK IN NEPA ANALYSIS

Joan Krajewski
Microsoft Corporation

On June 2, 2006, the United States Court of Appeals for the Ninth Circuit Court ruled in *San Luis Obispo Mothers for Peace v. Nuclear Regulatory Commission* (NRC), No. 03-74628, that the NRC is required to consider the possibility of a terrorist attack in its review under the National Environmental Policy Act of 1969 (NEPA). This decision has potential consequences for a wide range of facilities requesting federal and state actions (under state NEPA legislation) regarding siting and other issues. In addition, it likely will inspire additional NEPA litigation as the NRC withholds from public disclosure, its consideration of Safeguards Information—a category of unclassified and sensitive information that is germane to terrorism, but required to be protected from unauthorized disclosure under the Atomic Energy Act.

Background

In the case reviewed by the court, Pacific Gas & Electric Company (PG&E) sought an NRC license in 2001 to construct and operate an interim storage facility for spent radioactive fuel rods from its Diablo Canyon nuclear power plant. PG&E anticipates that its existing storage capacity would be exhausted this year.

The San Luis Obispo Mothers for Peace, a non-profit, intervened along with the Sierra Club and a private citizen. Among the contentions they raised was “the failure to address environmental impacts of terrorist or other acts of malice or insanity” during the NEPA review.

The NRC declined to review potential acts of terrorism. It relied on rulings in four post-September 11 NRC proceedings as follows:

- The possibility of a terrorist attack is far too removed from the natural or expected consequences of the agency licensing decision.

- The risk of terrorist attack could not be quantified, and thus, the analysis would be meaningless.
- Consideration of a terrorist attack would entail a “worst case” analysis, which NEPA does not require.
- Consideration of sensitive security issues is not appropriate in the public forum NEPA provides.

Ninth Circuit Court of Appeals Analysis

The court found the NRC’s justifications to be unreasonable. Addressing each point, the court reasoned:

- The NRC’s position that attacks are too remote for consideration was unreasonable when it stressed its own efforts against terrorism, including a “top to bottom” security review.
- The NRC had already shown in different contexts that it is capable of conducting a low probability-high consequence analysis, and precise quantification was not a requirement for triggering consideration under NEPA.
- Consideration of the environmental impact of a terrorist attack is not a “worst case” analysis where the petitioners asked the NRC to consider a range of potential environmental impacts.
- NEPA did not excuse sensitive issues from its scope, and the NRC had the option of shielding NEPA results involving protected information from public scrutiny while considering information provided by the public.

The court remanded the case for further proceedings.

Potential Impacts

While the decision is too recent to fully appreciate how it will be applied, potential impacts include enlargement of the scope of pending and future agency NEPA or state-equivalent proceedings involving critical infrastructure or other potentially vulnerable targets.

The decision also leaves unresolved the scope of the clash between NEPA's public process and the requirement to protect unclassified Safeguards Information of nuclear facilities described in 10 C.F.R. Part 73 such as:

- Physical security plan for the nuclear facility or site
- Drawings or maps representing the physical protection system
- Details of alarm system layouts
- Written physical security orders and procedures
- Details of the on-site and off-site security communications systems
- Lists or locations of certain safety-related equipment identified in the documents as vital for purposes of physical protection
- Composite safeguards contingency plan for the facility or site
- Portions of the facility guard qualification and training plan, which disclose features of the physical security system or response procedures
- Response plans to specific threats detailing size, disposition, response times and armament of on and off-site responding forces
- Details of vehicle immobilization features
- Arrangements with local police response forces and locations of safe havens
- Details regarding limitations of radio-telephone communications
- Procedures for response to safeguards emergencies
- Portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses or vulnerabilities in the system

The existing definition of Safeguards Information is subject to significant proposed expansion in a pending NRC rulemaking—Protection of Safeguards Information (RIN 3150-AH57) and may be modified on a case-by-case basis through other NRC action. Despite the impact of the court's opinion in *San Luis*

Obispo Mothers, broadening the definition of sensitive information may limit the ability of the public to fully participate in the NEPA process by shielding much of the NRC's consideration of potential terrorist attack from disclosure.

Joan Krajewski is the chief environmental and product safety counsel of Microsoft Corporation located in Redmond, Washington.

LIKE TO WRITE?

The Special Committee on Homeland Security welcomes the participation of members who are interested in preparing this newsletter. If you would like to lend a hand by writing, editing, identifying authors, or identifying issues please contact the editor Joan Krajewski at 425/706-4539 or joankr@microsoft.com.

VISIT US ON THE WEB!

To learn more about the ABA, Section and Committee, please visit:

American Bar Association:

www.abanet.org

Section of Environment, Energy, and Resources:

www.abanet.org/environ

Special Committee on Homeland Security:

www.abanet.org/environ/committees/homelandsecurity/

Books from the Section and ABA Publishing:

www.ababooks.org