
# THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 8 NUMBER 5

NOVEMBER 2009
CHEMICAL SECTOR





Contact: CIPP02@gmu.edu
703.993.4840



In this issue of *The CIP Report*, we highlight the Chemical Sector. The Chemical Sector employs approximately 863,000 people and generates billions of dollars in annual revenue, therefore vital to the competitive economic market. At present, the Chemical Sector is experiencing tremendous legislative changes. This month's issue reflects upon these changes as well as other relevant topics.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

First, the Department of Homeland Security's Chemical Branch Chief provides a general overview of the Chemical Sector and describes the current efforts being undertaken to improve collaboration between the public and private sectors. Next, chemical experts from AcuTech Group, Incorporated discuss the emergence of Inherent Safety, an approach to security risk management in the Chemical Sector. This article is followed by a discussion on the enhancement of emergency preparedness in the Chemical Sector by a specialist in critical infrastructure protection and risk management at IEM Incorporated. A professor from the University of Texas at Dallas examines the potential threat to homeland security and emergency management due to the availability of hazardous materials at higher education institusions. Next, we include an article by James Madison University, the Center for Infrastructure Protection's partner, who discusses chemical hazards and local emergency planning.

We also include an article that provides an overview of the Ninth Control Systems Cyber Security Conference, which was held in October. This month's *Legal Insights* examines the "citizen suit" provisions in the Chemical Facility Anti-Terrorism Act of 2009. We are also delighted to include a brief statement about the formation of the new partnership between the Center for Infrastructure Protection and the Poste Italiane Group. Poste Italiane, located in Rome, Italy, is the leading postal services operator in Italy.

We would like to take this opportunity to thank the contributors to this month's issue. We truly appreciate your valuable insights.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

# Chemical Sector Security: Success through Collaboration

by Amy Graydon, Chemical Branch Chief
Sector Specific Agency Executive Management Office
Office of Infrastructure Protection

Partnerships represent the foundation of the national Critical Infrastructure Key Resources (CIKR) protection effort. The U.S. Department of Homeland Security (DHS), as the Chemical Sector-Specific Agency (SSA), leads the voluntary efforts to collaborate with private and public stakeholders to increase the protection and resilience of the Chemical Sector in the physical, cyber, and insider realms. Through these relationships, the Chemical Sector is working to reduce the Nation's chemical manufacturing and distribution infrastructure's vulnerability to all hazards to an acceptable level based upon sound risk-based methodologies using risk-based assessments, industry best practices, and a comprehensive information-sharing environment between industry and government.

The private sector owns the majority of chemical facilities, a fact that requires DHS to work closely with the private sector owners and operators and industry associations to identify and prioritize assets, assess risks, develop and implement protective programs, and measure program effectiveness. The Chemical Sector has overlaps and interdependencies with a wide range of other sectors, including Communications, Oil and Natural Gas, Food and Agriculture, Information Technology, Transportation, and Water.

Today, as we prepare for the second wave of the 2009-2010 H1N1 influenza season, the effective utilization of these partnerships is critical to minimizing the impact of the flu on the Sector. In coordination with the U.S. Department of Health and Human Services, the Chemical SSA is working with both the government and the private sector to ensure Chemical Sector stakeholders have access to the appropriate planning resources and guides for distribution to their employees. In addition, the same partners who are on the frontlines in the fight against the H1N1 virus will assist the SSA by providing pandemic-related situational awareness to the SSA and DHS. These real-time reports from the field will help inform Leadership about the flu's impact on the Chemical Sector, which will allow the Federal Government to better gauge its response.

Clearly, strong partnerships are central to an effective homeland security effort such as the Department's preparations for a pandemic outbreak. These public and private sector partners organize themselves via Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC), respectively. GCCs and SCCs create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing approaches to CIKR protection and work together to advance capabilities. The success of these councils is based on active engagement in effective, multi-directional information sharing. When owners and operators have a comprehensive picture of threats or hazards, their ability to assess risks, make security investments, and take protective actions is enhanced. Similarly, when equipped with an understanding of private sector information needs, the government can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The benefits of a strong public-private partnership were evident at the third annual Chemical Sector Security Summit held this summer in Baltimore. The three-day event attracted approximately 350 participants, including a diverse array of chemical stakeholder partners, such as industry owners and operators; Federal, State, and local officials; Congressional staff members; and representatives from the international community. Seven out of every 10 participants at this year's summit were from the private sector, while the remainder of the participants represented Federal,

*(Continued on Page 3)*

**Chemical Sector** *(Cont. from 2)*

State, and local government.

The summit provides an open forum for the public and private sector to work together to share information within the confines of the National Infrastructure Protection Plan Partnership (NIPP) framework. Plenary sessions and breakout workshops included presentations and discussions on Chemical Facility Anti-Terrorism Standards (CFATS); threats to the homeland and the Chemical Sector; State and local issues; industry practices; incident management; and cybersecurity, among others.

While the Chemical Sector is focused on implementing CFATS at high risk facilities, the Sector also recognizes the value of voluntary efforts. An important aspect of the summit included a discussion of a suite of voluntary tools, programs, and support activities the Chemical SSA offers to chemical facilities nationwide, including the following:

**Web-Based Chemical Security Awareness Training**
The Chemical Security Awareness Training Program is an online interactive program that enables chemical facilities to increase the security awareness of their employees. The SSA designed the free voluntary training for employees not typically involved in facility security.

**Voluntary Chemical Assessment Tool**
The Voluntary Chemical Assessment Tool (VCAT) is a free, Web-based application intended for non-regulated facilities. VCAT is designed to help owners and operators identify security gaps, determine a facility's current risk level, and conduct cost-benefit analysis of options for enhancing a facility's security posture.

**Security Outreach and Awareness Program**
The Security Outreach and Awareness Program (SOAP) provides critical information to facility managers, control engineers, and IT administrators working in cybersecurity management. Participating companies receive a free voluntary review of their security system networks and a summary of their cybersecurity policies and processes.

**Homeland Security Information Network – Critical Sectors**
The Homeland Security Information Network – Critical Sectors (HSIN-CS) is the sector's primary information-sharing platform especially during significant incidents. HSIN connects users to TRIPwire, a secure online portal that provides unclassified information about terrorist tactics, techniques, and procedures. Additionally, HISN links members with the U.S. Computer Emergency Readiness Team (US-CERT), the principal Federal cyber watch and warning center.

**Vehicle Borne Improvised Explosive Device Training**
The Vehicle Borne Improvised Explosive Device (VBIED) Training was developed in coordination with DHS' Office of Bombing Prevention and is a series of one day training sessions for chemical facility security officers. The free program increases the Chemical Sector's awareness of the threat of improvised explosive devices, provides safety precautions for security professionals dealing with explosive incidents, and enables Chemical Sector professionals to deter, prevent, detect, protect against, and respond to terrorist use of VBIEDs. This course will be offered at six locations nationwide in 2010.

In addition, the Chemical SSA's public and private sector partners maintain many of their own tools to address the many threats they face, both manmade and natural. DHS leverages these tools to provide stakeholders from across the sector with the opportunity to take advantage of best practices in an effort to enhance resilience. One example of this type of partnership is the Security Seminar and Exercise Series with State Chemical Industry Councils. This collaborative effort between the Chemical SSA and various State Chemical Industry Councils fosters communication between facilities and their local emergency response teams. The events cover a wide variety of topics and are relevant to the specific interests of the local chemical facilities. Professional facilitators lead an interactive tabletop exercise to help participants learn to respond to real world situations in real time. A recent exercise scenario involved an active shooter at a manufacturing facility. To date,

*(Continued on Page 23)*

# Inherent Safety: An Approach to Security Risk Management in the Chemical Sector

by David Moore, President & CEO
Lee Salamone, Senior Consultant
AcuTech Group, Inc.

**Introduction**

Inherent Safety (IS) (or Inherently Safer Technology – IST – as it is commonly referred to) has emerged as a key chemical process risk management issue. Process safety professionals have embraced IS concepts voluntarily for years and it is an established approach for addressing process safety risks. IS is a general philosophy rather than a science or particular technology, and it is imbedded in the thought process of chemical and safety engineers as they design and operate safe plants.

The IS concept is based on the belief that if one can eliminate, lessen, or moderate the hazard, not only is the risk reduced, it may be possible to remove the risk altogether from consideration. Alternatively, an inherently safer system would make the hazard less likely to be realized and less intense if there is an accident or intentional release. The goal of inherently safer systems is to reduce or eliminate hazards to reduce risk, and it should be a first priority for managing risk.

There is currently considerable debate on Capitol Hill about imbedding IS into Chemical Sector regulations for chemical security. The relationship of IS to chemical security is clear, but the practicality of mandating its use is debatable since the use of IS to reduce hazard (and consequence or attractiveness) may be limited by technological or business concerns. The discussion on IS and chemical security has been ongoing since the terrorist attacks of September 11, 2001. Since the promulgation of the landmark Chemical Facility Anti-Terrorism Standards (CFATS) (6 CFR 27) in April, 2007, which implemented the Congressional mandate to secure "high risk" chemical facilities (P.L. 109-295), the merit of regulating IS has been at the forefront of the ongoing discussions about securing the Chemical Sector, and has recently been a key topic in the reauthorization of CFATS.

**How the Chemical Sector is Secured**

Among the 18 critical infrastructure/key resource (CI/KR) sectors named by DHS, the chemical industry is one that is largely privately owned. It is a highly diversified industry with interdependencies throughout its vast value chain. Securing the sector as a whole has necessarily become an effort that is divided among federal and state authorities with some activities required by law or regulation and some activities being undertaken voluntarily by the sector. Many of these efforts have focused on securing facilities, transportation of hazardous materials, sales, and cyber security aspects of manufacturing (such as computerized process or manufacturing controls) using the traditional principles of deter, detect, delay and respond. The idea of making fixed chemical facilities less attractive targets by removing or significantly reducing the potential off-site consequence of a release has certainly occurred to practitioners of chemical security and to the advocates and critics of the industry, but the principles behind IS do not lend themselves to quick and easy solutions.

The CFATS regulation is targeted specifically at the Chemical Sector and requires facilities that possess any of the more than 320 materials listed in the regulation, at or above a screening threshold quantity, to be screened and evaluated and, if covered, to secure the facility against

*(Continued on Page 5)*

Inherent Safety *(Cont. from 4)*

intentional acts that would cause a release of a toxic, flammable or explosive material with offsite consequences, or theft/diversion of a material that could be used in an intentional act off site in an improvised explosive device or by itself as a weapon, or sabotage of a material on-site that would result in a release once the material leaves the facility. It is the possession of certain materials that initiates a facility's compliance activity and the regulation includes all manner of facilities that manufacture, use, store, and distribute chemicals: chemical manufacturers, formulators, and distributors, petroleum refineries, aboveground fuel storage terminals, food manufacturers, pharmaceutical manufacturers, paper mills, laboratories, paint makers, and warehouses, among others.

**Inherent Safety Principles**

IS includes four basic strategies to apply for risk management of chemical facilities:

- Substitution - to replace a material with a less hazardous substance
- Minimization - to use smaller quantities of hazardous substances
- Moderation - to use less hazardous conditions, a less hazardous form of a material, or facilities that minimize the impact of a release of hazardous material or energy
- Simplification - to design facilities or processes which eliminate unnecessary complexity and make operating errors less likely or which are forgiving of errors that are made.

These four strategies could be independent ideas or they may relate to one another, depending on the situation. There is no defined and agreed upon way to consider them in a formal analysis methodology. Engineers are encouraged to consider them to the extent possible, but given the innumerable situations where they may be applied there is still no agreed-upon rule regarding what is an adequate consideration of IS.

**The Practice of Inherent Safety**

Inherent Safety is not new, but regulation of it is cutting edge. Most of industry is already practicing it, but not formally documenting how they use inherent safety as a strategy for safety or security risk management. Engineers tend to make orderly, inherently safer decisions by nature. This has been expected of industry as a matter of principle, and there is evidence it is being practiced, but measurement of the actions or the benefits is not being measured. The lack of published evidence may be a symptom of the lack of formal and agreed upon IS analysis approaches; another reason may be that the requirement to consider IS approaches simply has not existed until recently to drive documentation of the considerations.

It is precisely because IS is ill-defined and involves considerable judgment that it is very difficult to define and implement with any uniformity and objectivity. This is particularly true in the Chemical Sector where the diversity of chemical uses and processes and site specific situations prevents clear characterization of the industry or a one-sized-fits-all solution.[1]

IS can also be very subjective — how 'safe or secure' is 'safe or secure enough' is a decision of those conducting the study or making risk management investments. There are no clear and objective guidelines to make these decisions as it is considered a concept to apply as one sees fit and as opportunities arise.

**The Regulation of Inherent Safety**

In actual practice, IS implementation has proven to be problematic largely because, at this time, it is more of a theoretic concept rather than a codified procedure with a well-established and understood framework for evaluation and implementation. Furthermore, it cannot be regarded as the sole design criteria as it must be integrated with other considerations.

Today, there are only a few examples of regulatory requirements for process safety or security related to IS. For example, IS requirements are part of the Contra Costa County, California, local Industrial Safety Ordinance (ISO), enacted in 1998, which affects only eight

*(Continued on Page 6)*

[1] Testimony of David A. Moore, "Inherently Safer Technology in the Context of Chemical Site Security," before the Senate Environment and Public Works Committee Dirksen Senate Office Building, June 21, 2006.

Inherent Safety *(Cont. from 5)*

chemical sites. As for security, the only requirement that exists is in New Jersey where the Governor enacted a Prescriptive Order which includes the need to consider IS for chemical security for certain sites in the state. Neither regulation goes so far as to require a change in technology due to the enormous challenges and liabilities associated with that move.

The enabling legislation for CFATS prohibits the Department from disapproving a site security plan "based on the presence or absence of a particular security measure," including inherently safer technologies. Even so, covered chemical facilities are certainly free to consider IST options, and their use may reduce risk and regulatory burdens. But DHS has recently said that it also believes that IST is often not appropriate in the security arena, because many IST solutions do not eliminate or reduce risk, but only move risk to another location.

**Conflict between Safety and Security**

The need to introduce inherent safety as a strategy at all facilities subject to a security regulation is questionable. It would potentially cause a great deal of analysis to consider a single strategy, thereby demanding a large effort and creating issues about documentation with many technical and legal dilemmas. The preferred approach to industry is more autonomous: allow industry to set security objectives to determine the relevant issues and vulnerabilities and make appropriate risk management decisions. IS should be considered as a potential strategy rather than the first priority and allow the most effective homeland security strategies to be applied rather than force a particular one or a change in every technology. In fact, *what is inherently safer is not necessarily what is inherently more secure*. For example:

Moderation - A process that successfully applied an inherently safer technology may have changed a catalyst to end with a 'moderated' process — one that is operated at a lower pressure and temperature. This is commendable for safety, but may have little to do with security. The process may be disabled by an adversary just the same, which is an issue of economic security, or it may release a flammable or toxic cloud which is just as significant.

Minimization - In another case, an owner may have reduced the inventory of a feedstock in a tank to reduce the consequences of an attack. The feedstock is a toxic substance, so this appears sensible, but the material is also a 'dual purpose' chemical that could be used to make an improvised chemical weapon. In that case, simply reducing the volume may not matter for the threat of theft of the materials — in fact, smaller quantities may be more man-portable thereby accommodating theft. The plant may need more frequent deliveries of the material, which also increases the chance of theft.

Simplification - An owner may invest considerable sums of capital to improve the simplicity of the control system, thereby lessening the chance of human error as a cause of an accident. This may result in a control system that is easier for an adversary to compromise.

Substitution - A petroleum refiner may substitute hydrogen fluoride catalyst with sulfuric acid for alkylation (along with substantial process changes). While the individual offsite impacts of a release from storage may be reduced, the opportunities for disruption of the transportation chain are increased due to the additional deliveries of acid that are required. Besides the number of additional volumes of materials transited throughout the community, the site has increased vulnerability each time a vehicle has to enter the perimeter. Generally speaking, security professionals try to find ways to reduce penetrations through a secured perimeter.

**CFATS and Inherent Safety**

The lengthy debate that led to the legislative authority to regulate chemical security thoroughly examined the benefits and difficulties of mandating IS concepts as part of security. The Chemical Sector, as diversified in size, type, material, and businesses as possible, was largely united against a mandatory consideration of IS to reduce risk. In the end, Congress specified that the regulation of "high risk" chemical facilities must be performance-based

*(Continued on Page 7)*

Inherent Safety *(Cont. from 6)*

and that DHS was prohibited from approving or disapproving any security plan based on the presence or absence of any particular security measure or practice — including IS.

But is the current version of CFATS naturally causing the desired effect? While DHS is currently prohibited from forcing companies to consider altering their processes, materials, or practices, it is interesting that among the nearly 7,000 facilities that were screened into the program based on an analysis of the materials and activities on site, many are now considering just the kind of changes described by IS principles to either exit the CFATS program or lower the potential offsite consequences of an intentional act and thus lower their compliance burden. Facilities are busily substituting materials, lowering concentrations, reducing inventories and simplifying (or simply eliminating) processes and business lines rather than investing time and resources in compliance. As these companies are making rational business decisions that suit their needs, the principles of IS are, in fact, helping them to reduce risk.

**The Future of IS and Chemical Security**

As new legislation is debated to extend the authority of DHS over these facilities (the CFATS law was written to sunset within three years), these discussions about the feasibility of IS recur. The Obama Administration has recently announced its support for the consideration of IS for facilities covered under CFATS[2] and various process industry lobby groups are bracing themselves for a return of the debate. In recent testimony before the House Subcommittee on Energy and Commerce, DHS representatives outlined policy principles with regard to IS at high-risk facilities:

- Support for consistency of IST approaches for facilities regardless of sector;

- Support for all high-risk chemical facilities, Tiers 1-4, to assess IST methods and report the assessment in the facilities' site security plans. Further, the appropriate regulatory entity should have the authority to require facilities posing the highest degree of risk (Tiers 1 and 2) to implement IST method(s) if such methods enhance overall security, are feasible and meet other public safety objectives;

- For Tier 3 and 4 facilities, the appropriate regulatory entit should review the IST assessment contained in the site security plan. The entity should be authorized to provide recommendations on implementing IST, but it would not

*(Continued on Page 24)*

## DHS' Chemical Facility Anti-Terrorism Standards

Section 550 of the Homeland Security Appropriations Act of 2007 ("Section 550"), enacted on October 4, 2006, provided the Department of Homeland Security (DHS) with authority to regulate security at certain high risk chemical facilities in the United States. The Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 CFR Part 27) is risk-based and performance-based, which makes it both particularly progressive and flexible, and yet challenging at the same time. CFATS compliance must now be included as a part of an overall security management strategy to develop a comprehensive, integrated, and cost-effective approach to site security that incorporates the risk posed by terrorism but meet overall corporate security management objectives.

Significant company and public sector resources may be required to comply with CFATS. This is especially true for the compliance step where a Site Security Plan (SSP) is developed based on the Risk-Based Performance Standards (RBPS). The eighteen RBPS cover aspects of facility security including perimeter security, asset level security, access control, cyber security, response capabilities, measures to address theft and diversion and sabotage, among other.

[2] Testimony of Rand Beers, Undersecretary, National Protection and Programs Directorate, US Department of Homeland Security, October 1, 2009, before the House Subcommittee on Energy and Commerce.

# How Federal Chemical Security Regulations Can Enhance Emergency Preparedness

by Mark A. Scott*, IEM Inc.

Security has always been a concern for the commercial chemical industry. Since the events of September 11, however, chemical security has come to signify much more: more attention from government, customers, suppliers, and the public; more regulatory obligations; and, ultimately, more costs. For many companies in this Sector, regulatory requirements such as the Chemical Facility Anti-Terrorism Standards (CFATS) impose new responsibilities that make operating a chemical plant even more challenging.

Under CFATS, a facility considered to present a high security risk must satisfy a series of mandatory requirements, including preparing a Site Security Plan and submitting to regular inspections by the Department of Homeland Security (DHS). Failure to satisfactorily meet these requirements can lead to civil penalties and other actions up to and including shutdown of operations. Compliance with CFATS is thus the first and most important responsibility of covered facilities.

Developing a plan to prepare for malicious acts against a chemical plant makes good business sense. However, if we step back and look not just at the physical security requirements but also at the broader range of impacts resulting from CFATS, we can begin to better understand the enhanced value offered by this program. With this understanding, the Chemical Sector can leverage CFATS for greater protection and resilience.

**CFATS Is Emergency Management**

Underlying the entire CFATS process is a basic set of emergency management principles that are used routinely by governmental jurisdictions and private organizations to manage risk. Taken together, the principles provide a framework for preparing for major events that can disrupt operations at a chemical facility and have dangerous consequences. The essential components include:

*Understanding Threats*: The emergency management process begins with identification of the types of threats that exist, the likelihood they will occur, and their potential consequences. Under CFATS, understanding threats and vulnerabilities begins with the requirement for a Security Vulnerability Assessment (SVA). Based on evaluation of the SVA, DHS determines whether a facility presents a high enough risk to fall under the CFATS requirements.

*Assessing Capabilities and Identifying Gaps:* Once key threats have been identified, organizations and jurisdictions can assess their existing preparedness and response capabilities and identify where improvements are needed. Under CFATS, this occurs during the SVA development process as each of the 18 risk-based performance standards (RBPS) are addressed during preparation of the Site Security Plan. The Plan also includes planned and proposed improvements to existing capabilities.

*Developing Plans and Procedures:* The heart of emergency management is the plan: the actions an organization or jurisdiction intends to take to mitigate risks and respond to and recover from emergency situations. Under CFATS, the mandated Site Security Plan serves this purpose. Using the RBPS as a guide, covered chemical facilities identify how they will prepare for and respond to terrorist and other malicious acts.

*Identifying Roles and Responsibilities:* Because a plan is only as good as its execution, emer-

*(Continued on Page 9)*

**Security Regulations** *(Cont. from 8)*

gency plans always include a focus on key staff roles and responsibilities for effective implementation of the plan. Under CFATS, roles and responsibilities are addressed throughout the Site Security Plan but especially under Standard 17-Officials and Organization, which requires all covered facilities to provide evidence that they have one or more officials and an organization responsible for security and for compliance with the RBPS. Specific metrics include defined owner/operator responsibilities; corporate security officer and facility security officer responsibilities; cyber security officer; and facility management roles.

**Training Employees and Testing Plans**: Successful execution of an emergency plan requires that everyone with a stake in the outcome understands the plan and their role. Plant employees play a particularly important role in recognizing threats and providing appropriate response. Under CFATS, Standard 11-Training requires all covered facilities to consider a Security Awareness and Training Program to ensure their personnel are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. Training on the plan and practicing through exercises and drills is therefore essential to ensure the readiness of all facility personnel.

**CFATS Is More Than Just Compliance**

Seen within this broader context of emergency management, CFATS offers value beyond just "checking the box" with DHS. The process of developing a Site Security Plan, and the resultant security measures that are employed, offers three major benefits to the chemical industry and its bottom line:

1. **Better Preparation for All Threats**
CFATS addresses the risk posed by acts of terrorism; however, chemical plant managers well understand that risks to plant operations can come from many sources: natural disasters, such as hurricanes, tornadoes, flooding, and other severe weather events; accidents, such as unintentional releases or spills of hazardous materials, power outages, and transportation mishaps; and intentional acts, such as terrorism and sabotage. Each source can attribute to economic loss, environmental and safety impacts, and business interruption. Developing a robust emergency preparedness capability helps ensure resiliency in the face of these threats. CFATS supports this effort by requiring a systematic review of a facility's security posture and by emphasizing the essential emergency management elements of planning, training, and exercising. The result is a plant that is better able to prepare for and respond to any threat.

2. **Stronger Relationships with Local Emergency Responders**
CFATS brings local emergency responders into the security planning process by requiring that facility plans be coordinated and exercised with surrounding jurisdictions. This is important because, in an emergency, plants will need to rely on the quick and effective response of local fire, police, emergency management, and other emergency services functions. Establishing relationships with responders before a crisis occurs, and ensuring that a facility's plans and the community emergency plans are in sync, will help make that happen. Through CFATS, those relationships can be built where they do not yet exist and strengthened where they do. The result is a better prepared chemical plant and community.

3. **Enhanced Business Continuity**
All businesses seek to minimize interruption to their operations. For chemical plants, even a temporary shutdown can pose significant costs, as well as risks during startup following the shutdown. The goal of business continuity is to ensure that critical facility management functions are not significantly damaged following a disaster or crisis of any nature. CFATS helps ensure continuity of operations by focusing on mitigating risks from malicious acts and by pushing for more effective emergency response plans. This process helps reduce the likelihood that crisis events will occur and ensures a faster response and recovery if they do. The result is a facility that is much better positioned for continuous operation without interruption.

*(Continued on Page 22)*

# New Homeland Security Concerns Regarding Higher Education Institutions and Chemical Hazardous Materials

by Dr. Nicolas A. Valcik
Associate Director, Office of Strategic Planning and Analysis/Clinical Assistant Professor
Program of Public Affairs – The University of Texas at Dallas

**Introduction**

With the advent of new technologies, universities and colleges have increased the amounts and variety of hazardous materials (HAZMAT) used in instruction and for research purposes. With those new technological fields comes an increase in potential risk in either homeland security or emergency management. Since 2001, there have been a host of new federal and state mandates regarding Homeland Security and Emergency Management operational issues that dictate compliance guidelines upon higher education institutions. The Patriot Act of 2001 was the forerunner of two more mandates: the Bioterrorism Preparedness and Response Act of 2002 and Homeland Security Chemical Facility Anti-Terrorism Standards of 2007. These mandates have affected reporting, security, and operational business processes at higher education institutions (Valcik, 2006 and Valcik, 2010). How do legislative acts and federal agency mandates such as these impact higher education institutions? These two acts expect colleges and universities (along with any other organization that have extensive research or storage capacities) to track and report biological and chemical agents (HAZMAT) to the federal government for homeland security and emergency management reasons. For the purposes of this article, the focus will be on the Department of Homeland Security Appropriations Act of 2007: Section 550, DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27 – Chemical Facility Anti-Terrorism Standards (Department of Homeland Security, 2007).

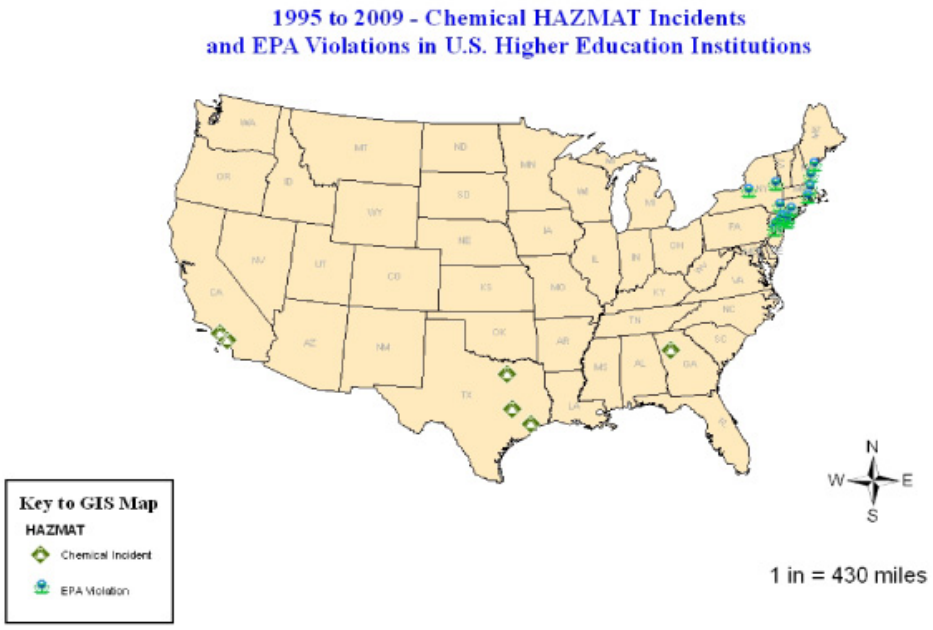



Figure I.

What are the concerns that universities and colleges have for securing, inventorying, and reporting chemical HAZMAT? Most higher education institutions have a surprisingly large and varied array of chemicals on their campuses for instruction, research, and even maintenance. Universities and colleges have the additional concern of being open to the local community. This openness increases the difficulties in securing facilities with HAZMAT storage for ongoing research projects and creates an ongoing tension between security concerns and the need for faculty and students to collaborate on research projects. Many universities function much like a small city in size, function, operational requirements as well as complexity. As can be seen in Figure 1 and Figure 2 (on page 11), there have been several higher education institutions involved with chemical HAZMAT incidents or EPA violations.

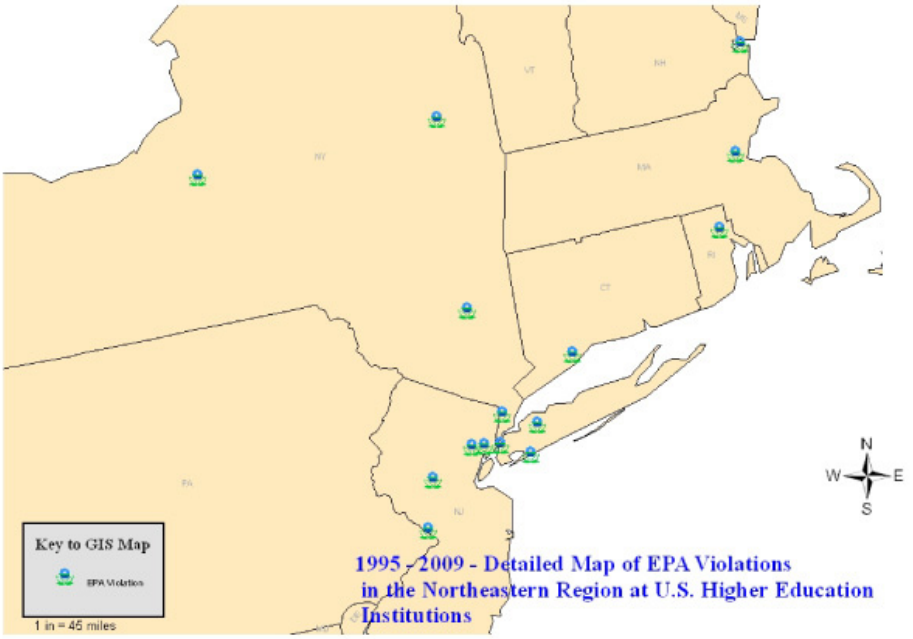
*(Continued on Page 11)*

**Higher Education** *(Cont. from 10)*

### Chemical HAZMAT used for Maintenance

A seemingly innocuous activity at a university or college can in fact use a large amount of hazardous chemicals. How many higher education institutions have a swimming pool on their premises? Some universities such as The University of Texas at Arlington have two pools, an outdoor and an indoor pool (The University of Texas at Arlington, 2009). Both pools require numerous chemicals to maintain the proper sanitary conditions for the water (i.e. pH Factor etc.). The main chemical of concern in the case of swimming pools is chlorine. Chlorine is corrosive and reactive with fire, which turns chlorine into a gaseous state (OSHA, 2009). In addition, not only is chlorine capable of causing a dangerous accident, but it can also be the major component of a weapon. Chlorine gas was used during World War I as a chemical warfare agent and in Iraq by insurgents which killed two and wounded 356 in 2007 (OSHA, 2009 and CNN, 2007). Therefore chlorine should be a chemical of concern if kept on hand by higher education institutions since that chemical could potentially be used for criminal or terroristic acts. Chemicals similar to chlorine must be reported to the United States Environmental Protection Agency as well as the Department of Homeland Security for emergency management purposes (OSHA, 2009). Besides athletic areas, chlorine in liquid or granular state might also be stored and used in research.

Figure 2.




The issue of chemicals used and stored in various places across campus is a typical situation at most colleges and universities and has existed since research programs began at higher education institutions. There should be an operational mechanism located centrally within a higher education institution to track all types of chemicals that are potentially dangerous or are above certain threshold limits for storage or use. In addition, information on those chemicals should be accessible to first responders and security forces in emergency situations. An organization should also track the rate of consumption of certain types of chemicals in an effort to prevent abuse or theft of chemicals that may be used in terroristic or criminal activities (i.e. controlled substances such as morphine).

Even the landscaping departments at higher education institutions must properly itemize and store the chemicals that they use. As seen in the bombing of the Alfred P. Murrah federal building in Oklahoma City by Timothy McVeigh, fertilizer can be used to make bomb materials (Rita Cosby, Clay Rawson and Peter Russo, 2005). Even a modest-sized campus can store and use enough fertilizer in a given year to provide a terrorist with enough material to bomb a building.

### Chemicals Used for Research

Institutions with sizable chemistry, biology, neuroscience, and engineering programs, for example, require a large amount of chemicals for both instruction and research. Chemicals such as chloroform, liquid nitrogen, hydrogen, and hydrochloric acid are now staples in modern university and college laboratories. Even basic instructional laboratories have a variety of

*(Continued on Page 12)*

**Higher Education** *(Cont. from 11)*

chemical stores used by students in basic experiments in core chemistry and biology courses. Securing and maintaining information on these types of chemicals can be a daunting task. In some laboratories and chemical storerooms, there can be hundreds of different chemicals that need to be catalogued for inventory control and emergency management purposes.

**Chemicals Used for Instruction**

One example of an area that uses many different types of flammable or volatile chemicals is art instruction. Sculpting, print making, and photography are taught at many community colleges, private colleges, and universities; these disciplines regularly use chemicals that require storage in locked, fireproof cabinets. If the sculpture studio keeps a gas welder, then the art program will also have to contend with compressed gases that could pose a hazard. If a gas welder were stolen, it could potentially be used by perpetrators to break into other secure areas of the campus.

**Recommendations to Protect Infrastructure and Assets**

To comply with Homeland Security directives, an institution should establish and maintain an inventory of chemical HAZMAT within a secure electronic database. At The University of Texas at Dallas, the Logistical Tracking System (LTS©) was developed to track biological, radiological, chemical, and waste HAZMAT to the Geospatial Information Systems (GIS) floor plans of the university. Additionally, LTS has the capability for police,security, and other first responders to view security camera feeds as well as extract a list of HAZMAT in a particular building if an emergency situation requires additional information. An organization should also keep a list of personnel and research assistance that have access to specific types of HAZMAT they are authorized to use or store.

**Picture 1.**

A security camera strategy should be placed around all critical areas where chemical HAZMAT is stored and used extensively. Security cameras should also be maintained and serviced on a regular basis. As shown in Picture 1, a security camera is useless if it is not maintained properly.

It is preferable for research facilities to be set apart from open access areas. By doing so, security personnel can reduce foot traffic through sensitive research areas, effectively deploy security devices throughout an entire building instead of room by room or floor by floor, and maximize the effectiveness of a smaller security force over a large area.

All higher education institutions, whether they are a large public research university, a community college or a small private college, should have a safety manual for chemicals. In addition, written policies and procedures should be widely available to departments and academic areas on how to handle chemical HAZMAT. The policies and procedures should address how chemical HAZMAT is to be delivered, properly stored, secured, inventoried, and establish proper access procedures. Proper labeling of chemical HAZMAT is crucial. The Material Safety Data Sheets (MSDS) should accompany any chemicals that are in a laboratory or storage area for safety reasons. MSDS information can also be found online at websites such as http://www.sciencelab.com/ (Science Lab, 2009). Researchers that are the principle investigators of ongoing research or are supervising teaching laboratories where chemicals are present should always know and understand the nature of chemicals that are under their purview. This is especially important at larger, higher education institutions as these institutions conduct many research projects and activities. The size of an institution can make it extremely difficult for a central organization (i.e. Environmental Health and

*(Continued on Page 13)*

**Higher Education** *(Cont. from 12)*

Safety (EHS) department) to have a grasp of everything that is on campus in regard to chemical HAZMAT and the characteristics of very specialized chemicals. Therefore it is imperative that EHS departments work closely with security forces as well as the researchers.

**Conclusion**

Ever since the late 1890's, when atomic research was in its infancy, the presence of chemical HAZMAT in laboratories have necessitated new policies and procedures to ensure the safety of not only the laboratory itself but also the researchers, students, and staff (Rhodes, 1986). Since the dawn of nuclear science, concerns have shifted from simple safety issues toward more pressing security issues. Campus security forces need to focus on protecting millions of dollars of facilities, infrastructure, and assets instead of the more common place aspects of municipal policing (i.e. speeding for example). An occasional drunk student is minor compared to new threats posed by criminals and terrorists in today's world. If the higher education community is to be successful in accomplishing their missions in research and instruction, issues of safety and security with regard to chemical HAZMAT will require diligence, innovative techniques, and cooperation between faculty and administrators to ensure a safe and secure educational environment.

**References**


Barrera, Zeke, 2008. The University of Texas at Dallas - Director of Environmental Health and Safety. *

Campus Consortium for Environmental Excellence, 2000. "EPA Launches Compliance Initiative Aimed at 258 New England Universities – Fines University of New Hampshire for Hazardous Waste Violations", January 7, 2000, http://www.c2e2.org/labxl/RCRA/region1_enforcement/region1enforcement.htm (Retrieved on April 20, 2009).*

Christensen, Kim, 2009. "Deadly UCLA lab fire leaves haunting questions", Los Angeles Times, March 1, 2009, http://www.latimes.com/news/local/la-me-uclaburn1-2009mar01,0,3624028.story?page=1 (Retrieved on April 17, 2009).*

CNN, 2007. "Iraq Gas Attack Makes Hundreds Ill", March 18, 2007, http://www.cnn.com/2007/WORLD/meast/03/17/iraq.main/index.html (Retrieved on September 14, 2009).

Cosby, Rita, Rawson, Clay and Russo, Peter, 2005. "G-Men Recall Hunting Down McVeigh, Nichols," Fox News, April 15, 2005, http://www.foxnews.com/story/0,2933,153729,00.html (Retrieved on September 14, 2009).

Department of Homeland Security, 2007. Department of Homeland Security Appropriations Act 2007: Section 550, DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27 Chlo – Chemical Facility Anti Terrorism Standards, http://www.dhs.gov/xlibrary/assets/IP_ChemicalFacilitySecurity.pdf (Retrieved on September 14, 2009).

EPA, 2002. "EPA Files Complaints Against Three Universities for Hazardous Waste Violations: Columbia University, Long Island University, and New Jersey City University; Fines Total More than $1.1 Million", News by State. 11/07/2002, http://yosemite.epa.gov/opa/admpress.nsf/8b770facf5edf6f185257359003fb69e/37477b63d1bf5c0b852571640065172b!OpenDocument (Retrieved on April 20, 2009).*

EPA, 2008. "Major Enforcement Actions Against Colleges and Universities in New York, New Jersey, and the Caribbean", Region 2 Enforcement, http://www.epa.gov/region02/p2/college/enforcement.htm (Retrieved on April 20, 2009).*

Oklahoma Higher Education, 2000. "Universities, Colleges Not Receiving Top Marks for Environmental Compliance – EPA Holding Educational Institutions to Same Standards as Industry", System Safety Health Resource Center, http://www.okhighered.org/training-center/newsletters/osrhe/university-college-epa-compliance.html (Retrieved on April 20, 2009).*

OSHA, 2009. "Occupational Health and Safety Guideline for


*(Continued on Page 21)*

# By Committee: Chemical Hazards and Local Emergency Planning

by Dr. Gary Kirk, James Madison University*
Assistant Professor of Political Science
Director, Master of Public Administration Program

The 1986 Emergency Planning and Community Right-to-Know Act (EPCRA), also known as the Superfund Amendment and Reauthorization Act (SARA), required states to develop emergency response committees (SERCs) to designate and oversee local emergency planning committees (LEPCs). Local committees were tasked with planning for accidental chemical releases and making available to the public information about chemical stores in their communities. Additionally, the language of EPCRA dictated that LEPCs develop a membership profile inclusive of numerous stakeholder groups, including elected officials, first responders, facility owners, media representatives, and leaders from community organizations. The unique structure of LEPCs promised unprecedented availability of information about chemical infrastructure and the possibility of high quality planning efforts backed by expertise and interests located in each community. As LEPCs approach their 25th anniversary, it is important to reflect on their effectiveness and to reevaluate their roles in light of an increasingly complex chemical infrastructure.

In 2007, a survey of LEPCs in Virginia[1] provided insight into these topics. The results provided information about the current status, the perceptions, and the potential future of LEPCs. Of the 110 LEPCs identified in Virginia, responses were received from 73 (66%). In short, the survey results indicated a wide range of activity-levels. Only 40% of LEPCs in Virginia were deemed compliant with EPCRA requirements; this corresponded to levels observed in a 1999 Environmental Protection Agency[2] study which found that 41% of LEPCs were compliant nationwide. The Virginia study found that LEPCs with jurisdiction over more chemical facilities were more likely to be in compliance with EPCRA. Amongst LEPCs in the quartile with the highest number of chemical facilities (>35), there was 80% compliance, while the quartile with the fewest facilities (<8) had 80% noncompliance. If the number of chemical facilities is an indicator of risk, then LEPCs dealing with higher risk seem to be more prepared in terms of meeting the legislative requirements.

In contrast to these active, compliant LEPCs, a substantial number of communities had inactive committees. The Virginia survey tried to identify potential causes of inactivity. Overwhelmingly, the lack of financial (50%) and human resources (65%) were cited as the reason for inactivity. Clearly there are implications for implementing EPCRA as an unfunded federal mandate; Virginia, like many other states, has not implemented facility filing fees or other revenue streams as funding sources for LEPC expenses. Expenses specifically mentioned as priorities by LEPCs frequently included software to assist facility filing and integration with emergency response and GIS systems; staff to coordinate meetings and publication of disclosure documents; and costs associated with emergency response training exercises. LEPCs that received staffing and financial support primarily got it through local government emergency services budgets (i.e., fire and rescue), but even those budgets were seen as mostly inadequate to effectively complete the work of the unit. Other funding and staff support reportedly came as in-kind

*(Continued on Page 23)*

[1] Templeton, Jill & Gary Kirk. 2008. The Status of Local Emergency Planning Committees (LEPCs) in Virginia. Retrieved September 20, 2009 from http://www.jmu.edu/iiia/webdocs/Reports/Templeton%20Kirk%20LEPC%20Final%20Report.pdf.
[2] Starik, Mark, William C. Adams, Polly A. Berman, and Krishnan Sudharsan. 2000. 1999 Nationwide LEPC Survey. Retrieved December 14, 2007 from http://www.epa.gov/emergencies/publications.htm.

# The Ninth Control Systems Cyber Security Conference: An Overview

by Joe Weiss, PE, CISM
Applied Control Solutions, LLC

The Ninth Control Systems Cyber Security Conference, hosted by Applied Control Solutions, was held from October 19 to October 22 in Bethesda, MD. The festivities commenced Monday morning with parallel activities. On Monday morning, a tour of the Washington Suburban Sanitary Commission's Rock Creek Water treatment facility was arranged. In parallel, the initial meeting of the ISA Nuclear Plant Cyber Security Joint Working Group was held. The ACS Conference started Monday afternoon with two introductory sessions: Control Systems for the non-Control System Engineer and IT for the Control Systems Engineer.

The ties between the chemical sector and the cyber sector are complex and the conference was not able to explore them in as much depth as they deserve, but the process of learning, discussing, and highlighting important issues is an ongoing one. The discussion of industrial control systems necessarily encompasses many in the chemical industry. Discussion was also focused on the water and nuclear sectors.

Cyber security is extremely important to the chemical industry for a variety of reasons. There has been a proliferation of threats such as hacking, viruses, and the Sector's increasing use of cyber systems. Like every other sector of the economy, the Chemical Sector has seen its processes change through contact with information technology. These changes allow businesses to streamline their processes and automate formerly paper-driven processes, but this opens up entire new systems to attack or failure. As the American Chemistry Council's Cyber Security Strategy states, the interdependencies between the Chemical Sector and the Cyber Sector "demonstrate the importance of having proactive risk management and reduction strategies in place to help protect chemical industry companies, communities, and the nation as a whole."

The Conference began in earnest Tuesday with approximately 110 attendees. They represented United States and international electric and water utilities, chemical and oil/gas companies, IT and control system suppliers and consultants, universities, and United States and international government agencies. The purpose behind titling the conference "Control Systems Cyber Security" is due to the fact that industrial control systems are common across multiple industries. The agenda can be found at www.realtimeacs.com.

On Tuesday, there were two hacking demonstrations of control systems and several discussions on control system cyber vulnerabilities. There was also a discussion on the need for technical control system cyber security curriculum (policy programs exist). There were two keynote speakers: the Honorable Yvette Clarke, Chairwoman of the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology and member of the Intelligence, Information Sharing, and Terrorism Risk Assessment Subcommittee provided the lunch keynote while Whitfield Diffie gave the evening keynote and discussed control system cyber security issues from the Tuesday's session. On Wednesday, there were four different sessions on actual control system cyber incidents — none of which was public. In one session, two control system engineers from two different utilities that have control systems from every major supplier discussed their recent control system cyber incidents — one had his plant shutdown. A couple interesting side notes were that existing control system logging are adequate to identify control system incidents and their control system suppliers were not of much help when it came to providing control system cyber security support. Both engineers felt it was so important to share information they attended the Conference on their own nickel. This is in marked

*(Continued on Page 22)*

Legal Insights

# Citizen Enforcement of Security Laws

by James W. Conrad, Jr.[1]

Legislation to regulate the security of chemical facilities has been introduced in every Congress since October 2001. The bills introduced in any given Congress have usually picked up wherever the last Congress had left off, and thus have tended to resemble one another, with only minor differences. The dramatic exception to this trend was this June, when House Homeland Security Committee Chairman Bennie Thompson (D-MS) introduced a bill (H.R. 2868) containing a "citizen suit" provision.[2] These provisions are a feature of almost every federal environmental statute, and citizen enforcement of federal law dates back to the Civil War. However, the concept is singularly inappropriate in the security context. Mr. Thompson's provision has already been modified by the House Energy and Commerce Committee, but Congress should ensure that it does not reappear in any chemical security legislation that Congress finally enacts.

**Background**

Authorizing private citizens to be "private Attorneys General" to sue on the United States' behalf has a long but somewhat inconsistent history. The False Claims Act, a "qui tam" statute enacted in 1863 and directed against Civil War profiteers, authorized "any person" to sue in the name of the United States to recover payments made by the federal government on the basis of a fraudulent claim.[3] (The citizen plaintiff got to keep half the claim amount and half of any damages.[4]) The Sherman Act, dating to 1890, enables anyone injured by a violator of the antitrust laws to sue for treble damages.[5] In addition, beginning with the Clean Air Act Amendments of 1970, virtually every federal environmental or natural resources law enacted since that date has contained a provision empowering any person to file suit against either (i) anyone, including the United States, alleged to be in violation of the statute; or (ii) the Environmental Protection Agency (EPA) (or other relevant agency), if it has allegedly failed to take some nondiscretionary action required by the law.

These provisions generally require prior notice to the violator and the relevant agencies, and typically cannot be maintained if the United States or an authorized state is "diligently prosecuting" an action against the violation. The federal government can intervene by right in one of these actions.[6]

While these provisions have become boilerplate in environmental and natural resource statutes, curiously, they are not common in statutes regulating food and drugs, aviation safety, consumer product safety, bank safety and soundness, transportation safety, or any of the

*(Continued on Page 17)*

[1] Principal, Conrad Law & Policy Counsel, Washington, DC (www.conradcounsel.com). J.D. 1985, GW Law School. Conrad has worked on chemical facility security issues continuously since 2001, first as in-house counsel at the American Chemistry Council and currently as outside counsel to the Society of Chemical Manufacturers & Affiliates.

[2] H.R. 2868, the "Chemical Facility Anti-Terrorism Act of 2009" (introduced June 15, 2009). The citizen suit provision, contained in Section 3(a) of the bill, is proposed new 6 U.S.C. § 2116.

[3] Ch. 67, 12 Stat. 696, § 4 (March 2, 1863). The current version of this statute is found at 31 U.S.C. § 3730.

[4] *Id.* § 6.

[5] 15 U.S.C. § 15.

[6] *See*, e.g., 42 U.S.C. § 7604 (Clean Air Act). A comprehensive list of these similar provisions is contained in H. R. Rep. No. 111-205 (July 13, 2009), at 49.

**Legal Insights** *(Cont. from 16)*

other myriad substantive areas that the federal government regulates. Why this is the case is not obvious, and might make a good law review article. (In the meantime, my best guess is that they have been added by Congressional subcommittees that are used to adding them in similar cases, and not added by subcommittees that are not so accustomed — such reflexive behavior is remarkably common on Capitol Hill.)

Although chemical facility security is nominally "security" legislation, there has never been any question that many of its strongest supporters view it as means to accomplish a goal they have not previously been able to attain: a federal mandate to reduce or eliminate the use of chemicals, like chlorine and hydrogen fluoride, that the legislation's proponents feel are simply too hazardous.[7] The Department of Homeland Security's current "Chemical Facility Anti-Terrorism Standards" (CFATS), which pending legislation would partially codify, is premised on an "Appendix A" list of chemicals that pose hazards in chemical terrorism scenarios.[8] Thus, it probably should not be too surprising that the drafters of Mr. Thompson's bill finally tumbled toward the idea of an "environmental" citizen suit provision in that bill. As introduced and reported by the Homeland Security Committee, Section 2116 of the new statute, to be created by the bill (H.R. 2868), would authorize any person to file suit:

(1) against any governmental entity (including the United States, any other governmental instrumentality or agency, and any federally owned-contractor operated facility, to the extent permitted by the eleventh amendment to the Constitution) alleged to be in violation of any order that has become effective pursuant to [the new legislation]; or

(2) against the Secretary [of DHS], for an alleged failure to perform any act or duty under [that legislation] that is not discretionary for the Secretary.[9]

Lawsuits could be brought in specified federal district courts; 120 days prior notice would be required to be given to DHS and any other alleged violator. Actions under Paragraph (1) above would be barred by DHS's diligent prosecution of the alleged violator and DHS could intervene in a citizen suit.[10]

Despite the superficial similarity between chemical facility security and environmental laws, this proposed provision would be ill-advised policy. As explained below, (i) it is particularly unwise to allow citizens to sue facilities; (ii) it is less problematic, but still unhelpful, to allow them to sue DHS; and (iii) the House Energy and Commerce Committee's replacement "petition" process is a preferable alternative, although still unnecessary.

**Facilities Should Not be Subject to Suit Under Chemical Security Laws**

As noted above, Section 2116 is very closely modeled on the citizen suit provisions of environmental and natural resource statutes. One of the main reasons that these provisions are found in many such laws is because the obligations — and the compliance status — of regulated entities under them is a matter of public record. It is relatively easy to get access to facilities' permits, and their compliance data is normally also made public as a matter of law.[11] In many cases, facility compliance information is comprehensively released via websites like EPA's "Enforcement and Compliance History Online (ECHO)."[12] Also, citizen enforcement is generally thought to promote the purposes of these laws. By supplementing EPA and state enforcement with citizen oversight, Congress has crafted a mechanism that allows the law to

*(Continued on Page 18)*

[7] *See, e.g.*, Greenpeace, "Chronology of Legislation on Chemical Security" (beginning before 9/11), available at http://www.greenpeace.org/raw/content/usa/press-center/reports4/chronology-of-bush-inaction-an.pdf.
[8] *See* 6 C.F.R. Part 27, Appendix.
[9] H.R. 2868, supra note 2, § 3(a) (proposed new 6 U.S.C. § 2116(a)).
[10] *Id.* (new 6 U.S.C. § 2116(a) – (e)).
[11] For example, "effluent data" and "emission data" are required to be made public by the Clean Water and Clean Air Acts, respectively. *See* 33 U.S.C. § 1318(b); 42 U.S.C. 7414(c).
[12] www.epa.gov/echo.

**Legal Insights** *(Cont. from 17)*

be enforced even if the responsible agencies are unable or unwilling to act. Neighbors of polluting plants can give notice that they intend to sue to eliminate or reduce emissions, discharges, etc.; agencies can preempt that action, join in the lawsuit, or do nothing. In any event, pollution is challenged.

Citizen oversight of enforcement of security laws, by contrast, would actually be counterproductive to the purposes of those laws. In contrast to environmental laws' bias toward disclosure, security laws exhibit a severe bias toward nondisclosure. Most appositely, under the current CFATS program, the only fact about a facility's regulation that a citizen might be able to obtain legally is that fact that the facility is regulated. Every other item of information that the facility or DHS has developed under the law — the facility's risk-based "tier level," vulnerability assessment, security plan, list of security measures, etc. — is protected from being released to the general public under the Freedom of Information Act, equivalent state laws, or in litigation.[13] H.R. 2868 would generally perpetuate these protections.[14] And for good reason: if this information were publicly available, terrorists could use it to target facilities and their surrounding communities. Because this information is protected (currently as "Chemical-terrorism Vulnerability Information" or "CVI"),[15] there is no way that "any person" could evaluate the compliance status of a facility. Indeed, it is questionable whether such a person, relying on publicly-available information, could even form the reasonable belief regarding noncompliance that would be required to file a lawsuit in federal court under Rule 11(b) of the Federal Rules of Civil Procedure.

Since H.R. 2868 also limits routine public availability of compliance-related information, it would appear that the drafters of the bill expect that plaintiffs under Section 2116 would have to attempt to obtain information regarding noncompliance from DHS or regulated facilities through the process of pretrial discovery, presumably under protective orders.[16] To create an expectation that this could occur routinely would be misleading. Even under the more relaxed standard that the bill would create for access to "protected information" in litigation — equivalent to that now applicable to "sensitive security information" or "SSI" — the bill would still make it fairly difficult to obtain such information. The plaintiff would have to show a need equivalent to that required currently to obtain fact work product, the plaintiff's counsel would have to complete a background check, and the court would have to issue a protective order after concluding that access to the information did not present a risk of harm.[17] Courts have rarely, if ever, approved the release of SSI under this regime. It would be highly irregular for Congress to establish a presumptive right of action that could not, in many cases, ever be exercised.[18]

On the other hand, if the drafters of the bill expect that it *will* lead to wide access to protected information in citizen suits, or if that is what will in fact occur, that is even greater cause for concern. It is hard to believe that the information protection regime established under the bill would operate successfully if it routinely allowed security-sensitive information to be released under protective orders. Citizen enforcement cases against unpopular and scary chemical

*(Continued on Page 19)*

[13] *See* 6 C.F.R. § 27.400.

[14] *See* H.R. 2868, § 3(a) (proposed new 6 U.S.C. § 2110).

[15] *See* footnote 13 *supra.*

[16] *See* the Homeland Security Committee's report on H.R. 2868 (H. Rep. No. 111-205, pt. 1, July 13, 2009), at 49 (referring to the Committee's expectations regarding "information provided during such proceedings").

[17] *See* Pub. L. No. 109-295, § 525(d), referenced in proposed new 6 U.S.C. § 2110(c).

[18] Indeed, the Homeland Security Committee's report seems to promise greater protection of information than the bill itself provides, as the report says "[t]he Committee expects that information provided during [citizen suit] proceedings should be maintained in accordance with existing protections for classified and sensitive materials including but not limited to the protections set forth in Section 2110 of this title." Report at 49. It is unclear to what other protections the bill might be referring.

**Legal Insights** *(Cont. from 18)*

facilities are likely to be so politicized, and so high-profile, that sensitive information is bound to leak out. It is for this reason that DHS Deputy Under Secretary Reitinger — a former senior Justice Department official — expressed "concern" about the citizen suit provision in the Homeland Security Committee's hearing on June 16 of this year. In response to a question, he stated that, "no matter what the protections are," protected information "inevitably" would be disclosed over time.[19] Accordingly, Congress should not create weak spots in the web of applicable legal protections that could allow CVI to be disclosed in random citizen suits. Unlike the environmental laws, chemical facility security is one area where citizen enforcement could actually work against, not support, the protective purpose of the law.

Some proponents of applying the citizen suit model to CFATS argue that regulated facilities have large amounts of dangerous chemicals onsite — the same hazard that might make them regulated under environmental laws — and thus that H.R. 2868 should have the same citizen suit feature as those laws. H.R. 2868 confirms,[20] however, that it would not displace any environmental laws, and any information that a facility has to make public under those laws would remain publicly available under the bill — as it is under the current CFATS program. Citizens who want access to that information can get it, and those who think that environmental laws are not being followed at a facility can attempt to enforce those laws. But the bill should not create a litigation tool to go beyond those authorities to obtain security-related information.

As noted earlier, citizen suit provisions are not common outside the environment and natural resources field. Nor has the Supreme Court inferred a private right of action in ages.[21] Of greatest relevance, citizen suit provisions are uniformly absent from federal statutes regulating the security of ports, port facilities, vessels, aircraft, railroads, or motor vehicles. Citizen suit provisions can reduce risks in the environmental/natural resources context. They will only increase risks, however, in the security context.

**DHS Should Not be Subject to Suit Either**

DHS has been working diligently since October 2006 to implement the current CFATS legislation, and has developed a credible program under very tight deadlines. There is no reason to believe that DHS would have done a better job if it were acting under judicial supervision — indeed, having to defend itself in court would only distract from its ability to get the CFATS program up and running. Deputy Under Secretary Reitinger alluded to this potential for "diversion from existing labors" in his responses to questions during the hearing on June 16. Again, as noted above, there is no way that average citizens practically could determine whether DHS has acted correctly or incorrectly in approving a facility's site security plan or otherwise complying with a CFATS obligation — that information is protected from release under DHS's CVI rules. And again, environmental laws are a bad model for a law that deals so extensively with protected, rather than public, information.

The Homeland Security Committee's report on H.R. 2868 (the "Report") defends subjecting DHS to suit by claiming that "the Nuclear Regulatory Commission (NRC), which, like the Department [of Homeland Security] is a security agency, and is subject to suits

*(Continued on Page 20)*

[19] Deputy Under Secretary Reitinger emphasized at this hearing that he was not expressing a formal position of the Obama Administration, which at that point had not formed any official views on H.R. 2868. Remarkably, the Administration later adopted a formal position of "no opinion" regarding the inclusion of a citizen suit provision in the bill. *See* Statement for the Record of Rand Beers, DHS Under Secretary for National Protection & Programs, before the Subcommittee on Energy & Environment of the House Committee on Energy & Commerce (Oct. 1, 2009), available at http://energycommerce.house.gov/Press_111/20091001/beers_testimony.pdf (saying nothing about the topic).

[20] See new Section 2110(d).

[21] The Homeland Security Committee's report is thus misleading in describing the citizen suit provision as "remov[ing] the current restrictions on citizen suits" from a statute that is silent on the topic. H.R. Rep. No. 111-205, supra note 16, at 21.

**Legal Insights** *(Cont. from 19)*

brought by citizens."[22] In fact, the NRC is subject to citizen suits under environmental laws in the same way as any other federal agency that operates facilities that are regulated under such laws. But the Atomic Energy Act (AEA) does not authorize citizen suits against the NRC for violating or failing to take required action under the AEA. If DHS operated hazardous waste treatment plants, it would be subject to citizen suits under the federal hazardous waste law for its operation of those plants. But that is no basis for saying it should be subject to suit under its own organic statute.

**The Energy and Commerce Committee's "Petition" Process is an Improvement but Still Unnecessary**

The House Energy and Commerce Committee took up H.R. 2868 after the Homeland Security Committee, and recently reported its own version of the bill.[23] To its credit, the Committee revised Section 2116 so that it no longer allows citizens to sue private facilities. Instead, suits are permitted only against (i) facilities owned by the federal government that are allegedly in violation of a compliance order issued by DHS; and (ii) DHS, for failing to take a nondiscretionary act required by the statute.[24] Citizens who believe that a privately-owned facility is violating some requirement under CFATS are provided a process by which they could petition DHS.[25] Under this process, DHS would be required to respond to the petitioner regarding the steps it took to investigate and its final determination, to the extent permitted by the bill's information protection requirement. The DHS Inspector General could review these determinations de novo. If DHS chose not to take enforcement action, that decision would constitute final agency action reviewable in federal district court under the Administrative Procedure Act (APA). Thus, the dispute could end up in court, but (i) the defendant would be DHS, not the facility, and (ii) whether any relevant information could be included in the agency's administrative record on review would be determined by DHS in the first instance, and governed by the SSI rules discussed above.[26]

In explaining why it dropped the most objectionable feature of Section 2116, the Energy and Commerce Committee explained:

*The Committee decided to exclude private rights of action against chemical facilities in this section for two reasons. First, the Department raised concerns about the risk of disclosure of sensitive security information in a judicial proceeding. Second, the standards created under this bill are risk-based and performance-based and therefore are more subjective and less susceptible to judicial review than standards in other statutes with citizen suit provisions. Since compliance data is protected from public disclosure and compliance is subjective, it would be difficult for a citizen to identify and allege a violation in this context. The Committee does not intend for this to serve as precedent for citizen suit provisions in any existing or future laws.*[27]

The Committee is plainly headed in the right direction, although it would be preferable, for the reasons stated above, for the citizen suit provision to be removed altogether. Moreover, the petition process is redundant. The bill contains a "whistleblower protections" provision,[28] and it is difficult to see why it would not suffice to accomplish the purposes of the petition section. If deemed necessary, the whistleblower section could be amended to clarify that a failure by DHS to take enforcement action in response to a report submitted under it would be reviewable under the APA.

*(Continued on Page 21)*

[22] H.R. Rep. No. 111-205, *supra* note 16, at 49.
[23] H.R. Rep. No. 111-205, pt. 2 (Oct. 23, 2009).
[24] *Id.* at 16. Oddly, diligent enforcement by DHS is not a bar to filing of a citizen suit under this version of the section.
[25] *Id.* at 19-20 (proposed new 6 U.S.C. § 2117).
[26] See text accompanying footnote 17 *supra*.
[27] H.R. Rep. No. 111-205, pt. 2, at 53. It is also possible that the Committee was influenced by the House Judiciary Committee, to which the bill was also concurrently referred, but which chose to work behind the scenes rather than issue its own report.
[28] *Id.* at 11 (proposed new § 2108).

**Legal Insights** *(Cont. from 20)*

**Conclusion**

Citizen suit provisions are common and useful features of environmental and natural resources legislation. They are likely to be counterproductive, and potentially dangerous, in the security field. The House Energy and Commerce Committee has wisely dropped the most problematic aspect of H.R. 2868's citizen suit provision. It is fervently to be hoped that this approach, and not the Homeland Security Committee's, is contained in the version of the bill that ultimately is taken up on the House floor. Ideally, before Congress enacts new legislation to permanently reauthorize the CFATS program, it will delete the concept altogether. ❖

---

**Higher Education** *(Cont. from 13)*

Chlorine", United States Department of Labor, Occupational Safety and Health Administration, http://www.osha.gov/SLTC/healthguidelines/chlorine/recognition.html (Retrieved on September 14, 2009).

Rhodes, Richard, 1986. The Making of the Atomic Bomb, ISBN-0-671-44133-7, Simon and Schuster, New York, New York.

Science Lab, 2009. "Chemicals and Laboratory Equipment," ScienceLab.com, http://www.sciencelab.com/ (Retrieved on September 15, 2009).

Simpson, David, 2009. "Accident at Mercer lab causes explosion, hospital trip". The Atlanta Journal-Constitution. Tuesday, February 17, 2009, http://www.ajc.com/services/content/metro/dekalb/stories/2009/02/17/mercer_lab_explosion.html?cxtype=rss&cxsvc=7&cxcat=13 (Retrieved on April 17, 2009).*

The University of Texas at Arlington, 2009. "Campus Recreation," http://www.uta.edu/campusrec/index.php?option=com_content&task=view&id=14&Itemid=51 (Retrieved on September 14, 2009).

Valcik, Nicolas A., 2006. Regulating the Use of Biological Hazardous Materials in Universities: Complying with the New Federal Guidelines, ISBN-13:978-0-7734-5572-6, Edwin Mellen Press, Lewiston, New York.*

Valcik, Nicolas, 2010. (Forthcoming March 2010) "Chapter 7 - New Hazardous Materials (HAZMAT) Federal Regulations for Higher Education Institutions", In N. Valcik (Ed.), "Institutional Research: Homeland Security". New Directions for Institutional Research, Hoboken, NJ, John Wiley and Sons, Inc., San Francisco, California.*

* These references were used to make Figure 1 and Figure 2.

**Security Regulations** *(Cont. from 9)*

**Making the Most of CFATS**

Working through the CFATS process puts chemical facilities in a stronger position to prepare for all threat situations, to strengthen relationships with local responders, and to enhance business continuity. Here are three ways to make that happen:

**1. Leverage the Plan**
Whether using an existing Alternative Security Plan or developing a new Site Security Plan, facility owners and operators should look for opportunities to connect security considerations with environmental management and process safety procedures. Doing so will strengthen performance in each of these areas. Similarly, linking facility plans to those of the surrounding community and to the supply chain ensures quicker response and reduced downtime resulting from crisis events.

**2. Test the Plan**
The best way to know that a Site Security Plan will achieve the benefits outlined above is to test it out through exercises and drills. CFATS Standard 11 requires this, so facility owners and operators should take it to heart and put the plan through its paces. Facility owners and operators must honestly evaluate successes and areas needing improvement, and make adjustments where necessary. Doing this regularly will provide greater assurance that the enterprise will be ready when the unexpected happens.

**3. Engage with Stakeholders**
A company's employees, customers, supply chain, local responders, and community members all have a stake in the safety of the enterprise and a role to play in making that happen. Involving them appropriately throughout the security planning process will build trust and help make them partners in the effort to build a safer and more secure facility. Chemical Sector members should seek ways to collaborate with affected parties without divulging sensitive information or otherwise compromising security. Stakeholder engagement takes effort, but the payoff is worth it. ❖

*__Mark Scott__ *is Manager of Critical Infrastructure Protection for IEM Inc. He may be reached at mark.scott@iem.com. IEM, based in Baton Rouge, Louisiana, is a professional services firm offering risk management solutions in the homeland security and defense markets. More information is available at www.iem.com.*

**Conference** *(Cont. from 15)*

contrast to the utility and industry leadership who did not think this conference was important enough to attend even though many were based in Washington. On Wednesday evening, the Honorable James Langevin gave the evening keynote. Congressman Langevin felt the topic of the conference was so important that he spent 30-45 minutes after his presentation answering questions and talking to the attendees.

On Thursday, we received a summary of government activities including legislative efforts on cyber security, a cyber security activities by the Nuclear Regulatory Commission, efforts on-going at the Bonneville Power Administration using the NIST Framework, and non-governmental activities in certification and cyber incident collection. Another very interesting presentation included a discussion on the legal issues with cyber security and a discussion the Russian cyber attack on Estonia.

On Friday, NIST held a training session on NIST SP800-53 and SP800-82. I met with a number of congressional staff late morning and gave a presentation at the Pentagon's "cyber-hour."

The next ACS Conference tentatively will be next October in the Washington DC area. ❖

**Emergency Planning** *(Cont. from 14)*

support from local hospitals and chemical facilities. A host of other factors seemed to contribute to LEPC inactivity too; among the most commonly cited were a lack of interest from members in maintaining compliance (42%) and a lack of required expertise on the committee (23%).

Despite these challenges to effective operations, many LEPCs in Virginia appeared ready to take on responsibilities outside the original scope of EPCRA. Nearly 79% of active LEPCs indicated that they were involved in planning for accidents involving transportation of chemicals, and nearly 60% have responded to a 1999 EPA goal of including counterterrorism planning for chemical facilities. Natural and man-made disasters also have been incorporated into plans for 57% of active LEPCs, with coverage ranging from hurricanes and floods to illegal drug manufacturing and the flu pandemic. Of all LEPCs surveyed in Virginia, 80% felt that they should be approaching disaster planning from an all-hazards perspective.

When working properly, LEPCs have the advantage of bringing multiple perspectives, interests, and resources to the emergency planning dialogue. The diversity of LEPC membership has the potential to encourage development of high-quality solutions to complex problems. In the Virginia survey, 92% of respondents indicated that they believe the LEPC structure fosters collaborations amongst diverse stakeholders and almost 90% felt LEPCs were working in the public interest. As LEPCs broaden their scope and are called on to absorb other emergency planning functions, localities must address the struggles that many committees face in terms of administrative support and funding, the expertise of committee members, and the legitimacy of the committee in terms of a both decision-making authority and participation by diverse stakeholders. LEPCs struggling to exist or find appropriate members run an increased risk of violating the principles of transparency and balanced community involvement that were the innovative aspects of EPCRA. ❖

*Jill Templeton, a Graduate Fellow with the Institute for Infrastructure and Information Assurance (IIIA), assisted Dr. Kirk with the LEPC research project. This project was funded through the Center for Infrastructure Protection.

**Chemical Sector** *(Cont. from 3)*

the SSA has worked with Industry Council's in California, Pennsylvania, and New Jersey.

Science and technology offer considerable promise in helping to develop efficient and cost-effective ways of mapping potential consequences, identifying potential threats, assessing risk and vulnerabilities, and enhancing the protective posture of Chemical Sector infrastructure. The Chemical SSA is working with the Sector to identify gaps as well as with DHS' Science and Technology Directorate to ensure identified R&D projects benefit facility owners and operators.

Additionally, the Chemical SSA provides strategic and operational support in the event of an incident. During an incident, SSAs and infrastructure owners and operators use the National Infrastructure Coordinating Center (NICC) as the focal point for incident and status reporting. The Chemical SSA in coordination with the SCC hosts sector specific teleconferences to facilitate information sharing during an event. The SSA aggregates the information and shares concerns and issues with the NICC which collates the situational assessments and consolidates a cross-sector report for the Federal inter-agency Common Operating Picture.

The responsibilities are vast, but so are the efforts of the Chemical Sector's stakeholders to enhance the resiliency of one of the Nation's

*(Continued on Page 24)*

**Chemical Sector** *(Cont. from 23)*

most critical sectors. Through a unified public-private sector approach, the sector's CIKR will be better prepared for, more secured from, and more resilient to terrorist attacks and natural disasters. The prosperity of the United States is, and always has been, based on collaboration of the Nation's citizens. That same sense of cooperation will provide our homeland security community with the tools necessary for success. ❖

For more information, e-mail chemicalsector@hq.dhs.gov.

---

**Inherent Safety** *(Cont. from 7)*

require facilities to implement the IST methods; and

- Support for flexibility and staggered implementation to implementing a new IST policy.

Among the issues that highlight the debate are the difficulty of judging whether IS has been considered, the difficulty of measuring performance or compliance, the need to consider risk and not just hazard, and who or what agency will be the judge of what is inherently safer and therefore more secure.

Inherent safety should not be seen as the most important strategy to implement. Risk should be the measure of security preparedness given consequence, vulnerability, and threat considerations. Despite this practical opinion, the Chemical Sector should be prepared for a future where IS is regulated, as the momentum is clearly gathering. ❖

**About the authors:**

David Moore is President and CEO of AcuTech Group, Inc. a process safety and security consulting firm with nationwide offices. He is an expert in the issues surrounding chemical facility security and is a leading national authority on Inherent Safety. He was a key author of the Center for Chemical Process Safety book, *Inherently Safer Chemical Processes, A Life Cycle Approach*, 2nd Edition.

Lee Salamone is a Senior Consultant with AcuTech. Her practice area includes security in the chemical and petrochemical areas and she served as technical editor and a contributor to *Inherently Safer Chemical Processes, A Life Cycle Approach*, 2nd Edition.

For more information about AcuTech Group, Inc., please visit www.acutech-consulting.com.

# Poste Italiane Group

The Center for Infrastructure Protection is pleased to announce a new international partnership with Poste Italiane, the leading postal services operator in Italy. On October 29, the Center for Infrastructure Protection signed a research agreement with Poste Italiane, which operates in Rome, Italy, to collaborate on cyber security research. This represents a leap forward for the Center's international and cyber security research programs. The agreement was formally signed by the Center's Director, General Claude "Mick" Kicklighter, and Poste Italiano CEO and Managing Director, Massimo Sarmi, in a ceremony at the Center's offices in the Truland Building on Mason's Arlington campus. The two men signed the agreement underneath the Italian and American flags, symbolizing the international nature of their collaboration.

Poste Italiane not only manages Italy's postal service but also provides a group of related products, such as communications, logistics, and financial services. They are currently in the process of establishing a Cyber Security Center of Excellence in Rome, Italy. This Center of Excellence will have a global focus and partner with other international and national organizations to further the field of cyber security research and create a community of stakeholders around the world to pursue these issues. It will also include training and education programs to help identify threats and prepare the international community for solutions.

Mason, working through the Center for Infrastructure Protection, will have the opportunity to collaborate on joint cyber security research and development, advise on cyber initiatives and policy developments, assist in developing international cyber cooperation, develop and conduct training or other cyber security educational efforts, and exchange academic materials and other information.

The Center for Infrastructure Protection is proud to be implementing this international relationship and advancing its mission of studying and solving infrastructure protection related issues across all sectors, especially the Cyber Sector, one of the fastest-growing. This is the beginning of a fruitful collaboration.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1