The CIP Report

VOLUME 1, ISSUE 5 NOVEMBER 2002

Chemicals Sector Issue

CIP Project Staff

Kevin "Kip" Thomas
Research Associate Professor / Working Groups Project Manager

Meredith Gilchrest
CIP Law and Policy Research Archivist/ Outreach Program Manager

Rebecca Luria
CIP Project Administrator / Executive Assistant

George Baker
Interim Director JMU Institute for Infrastructure and Information Assurance

Ken Newbold
JMU Outreach Coordinator / JMU CIP Project Liaison

Contact: cipp01@gmu.edu
703-993-4840

Protecting a Nation: Homeland Defense and the Business of Chemistry

The terrorist attacks of September 11, 2001, forever changed the way Americans live and work. The chemical industry is reassessing and enhancing its security measures in the wake of these attacks – increasing levels of preparedness and solidifying partnerships with law enforcement and security agencies.

Chemistry is a critical national asset and a $450 billion business that directly employs more than one million Americans and accounts for another five million related jobs – in agriculture, pharmaceutical, automotive and other industries.

From life-saving drugs to clean drinking water and reliable energy, the chemical industry is integral to our way of life and is on the front lines of our homeland defense efforts.

Drawing upon its extensive work on safety and preparedness, the chemical industry is partnering with the EPA, Office of Homeland Security, FBI, Defense Department, Coast Guard, and other agencies to protect America from possible threats.

The American Chemistry Council (ACC) and its 180 member companies have implemented a new Responsible Care® Security Code to safeguard against potential terrorist attacks, expand relationships with law enforcement, and provide a model for chemical site protection.

At the bottom line, the business of chemistry is vital to America's economy and national security. The industry is committed to doing its part for national security and to protecting chemical facilities so that it can continue – safely – to provide essential, life-saving products and play a central role in revitalizing our nation's economy.

A Critical National Asset

Chemistry has helped build our nation, and this dynamic science continues to transform America. In 2001, the chemical industry invested $30 billion in research and development, producing innovations to make our homes safer and our environment cleaner.

Our food, safe water supply, clothing, shelter, health care, and other facets of modern life depend upon chemistry. Chemicals are vital to nearly every U.S. industry, and chemical products are key to our national defense and our quality of life:

- Health care – Polymers are used in medical devices

(Continued, Page 3)

Chemicals Sector Efforts to Address Cyber-Security Issues Underway

The number of reported IT security breeches in the United States has almost doubled with each consecutive year, with 43,136 IT security breeches already reported in the first half of 2002, according to the Department of Defense. The chemical industry is well aware of the need to balance the benefits of technology and information accessibility against safe and secure use. As our country develops its strategy to secure U.S. information systems, the chemical industry has taken a proactive approach, expanding the cyber-security efforts already underway in the industry to further safeguard information and maintain safe operations.

For the chemical industry and other critical infrastructure industries, the security of physical, information and process control systems has long been a priority. The sector manufactures and distributes more than 70,000 products, including basic and intermediate chemicals, specialty chemicals, agricultural chemicals, fertilizers, petrochemicals, plastics and fibers, paints and coatings and pharmaceuticals. In fact, the chemicals sector even benefits other critical infrastructure industries – many of which rely on the secure delivery of chemicals to serve the nation's security and defense, as well as the public's welfare. Well aware of its value and impact, the sector has maintained a focus on both safety and security, which it has demonstrated in everything from its longstanding voluntary initiatives to its vital part in military and public safety operations. Hundreds of thousands of highly trained chemists, engineers and operators are experts in the business of managing and reducing the risks associated with producing chemicals and the enabling technology.

"The business of the chemical industry relies heavily on the use of process control systems in our plants and information systems in our business units. But while we are similar in these and many other ways, we are also a diverse sector," said David Kepler, corporate vice president and chief information officer of The Dow Chemical Company. "Designing a strategy to provide secure information and process control systems within the industry while also meeting the needs of our largest and smallest chemical producers, was top priority for the industry." In April 2002, the chemical industry extended its security efforts with the creation of the Chemicals Sector Cyber-Security Information Sharing Forum. Consisting of senior-level representatives of trade associations representing more than 2,000 companies from key chemical industry segments, the Forum's first order of business was to construct an industry-wide cyber-security strategy.

Robert R. Ridout

Vice President, Information Systems and Chief Information Officer, Dupont and Program Steering Team Member

"For the chemical industry, IT plays a significant role in all of our activities, from automating transactions to providing the most strategic decision information, making the impact of technology providers an integral part of our success. With this in mind, the Forum is working with technology providers to enhance the level of security that these products and services offer. One of the best ways to achieve this goal is to leverage our influence on the IT industry's R&D organizations, encouraging them to develop solutions that meet the standards and guidelines determined by the Forum. I look forward to working with our IT partners to identify ways to improve existing commercial offerings and enable the industry to operate with an added assurance of safety."

A Program to Address Cyber-Security Needs

Reviewed and fully-endorsed by industry representatives in June 2002, the strategy defines the risk-based Chemicals Sector Cyber-Security Program (Program) which has recently begun implementation. A roadmap for developing cyber-security standards and *(Continued, Page 8)*

Overview *(Continued from Page 1)*

including stethoscopes and oxygen tents; PVC resin tubes deliver blood transfusions; polycarbonate is used in kidney dialysis filters.

- Communications – Silicon chemistry enables the microprocessor "brains" behind our nation's communications infrastructure, which in turn supports everything from computer networks to electrical grids and water systems.
- Housing – The average new house contains more than $12,000 in chemical building products, ranging from the pipes in the walls to the shingles on the roof. Chemical products are also used in siding, windows, frames, electrical wiring, paints, and insulation.
- Transportation – Every automobile contains about $2,000 worth of chemical products, including polyurethane seat cushions, neoprene hoses and belts, airbags, dashboards, seat belts and tires.

Commitment to Safety

Every day, hundreds of thousands of highly trained chemists, engineers and operators expertly manage and reduce risks associated with making chemicals, making it an industry that *puts safety first*. In fact, Labor Department data describe the industry as one of the safest in the United States. This is reflected in the industry's long-standing initiatives and programs, such as Responsible Care®.

Now in its 14th year, Responsible Care® is chemistry's comprehensive management system to continuously improve safety, communicate with neighbors, and protect employees, communities, and the environment. Since its inception, America's chemical companies have:

- Reduced emissions by 58 percent and boosted production by 18 percent.
- Achieved safety performance 4.5 times better than the average of all other U.S. manufacturing industries.
- Established about 300 Community Advisory Panels across the United States.
- Spread Responsible Care® to more than 46 countries, representing over 85 percent of the world's chemical production.

Providing 24/7 Expertise and Emergency Preparedness

Since 1971, the American Chemistry Council has operated, as a public service, the 24/7 emergency communication center known as CHEMTREC® (Chemical Transportation Emergency Center). When an emergency occurs, CHEMTREC® provides responders with technical assistance from product safety specialists, toxicologists, and other industry experts to safely handle the incident – all free of charge.

Another major initiative is TRANSCAER® (Transportation Community Awareness and Emergency Response), a program that provides information to communities through which hazardous materials are transported. TRANSCAER® offers community education, guidance in developing plans to respond to an incident, and training for local emergency responders. ACC member companies continually evaluate their security measures and work closely with local firefighters, health and community officials.

Strengthening Industry Security

Since the September 11 attacks, ACC members are emphasizing the security aspect of the industry's long-established culture of safety. The ACC has developed comprehensive Site Security Guidelines and has distributed them throughout the chemical supply chain and beyond – the Occupational Safety and Health Administration, for example, has posted them on its website.

Examples of security enhancements already implemented by ACC member companies include: additional security personnel and upgraded security policies and procedures; enhanced crisis management and/or emergency response programs and criminal background checks on new hires; access control systems, perimeter barriers and intrusion alarms.

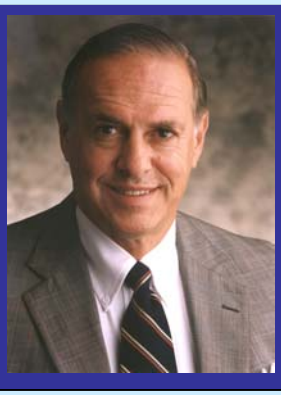
The ACC has also partnered with the EPA, FBI and others to organize regional security briefings around the nation. The CHEMTREC® (Chemical Transportation Emergency Center) team has worked with the FBI's Hazardous Materials Response Team to improve coordination between the industry and the agency.

This past June, the ACC signed an agreement with the FBI's National Infrastructure Protection Center (NIPC) to create the Chemical Sector Information Sharing and Analysis Center (ISAC) – an important public/private sector partnership operated by CHEMTREC® that shares vital security-related information among the multi-agency NIPC based at the FBI headquarters and the companies that make and use chemical products.

The ACC has also adopted a new Responsible Care® *(Continued, Page 4)*

Overview *(Continued from Page 3)* Security Code – a state-of-the-art security management system that is mandatory for ACC members. To address site, transportation and "cyber-security," all ACC members must:

1. Prioritize facilities into one of four tiers with Tier 1 being top priority.
2. Assess security to identify any gaps in physical security and security procedures.
3. Develop and implement security enhancements to fill those gaps and address risks. This includes applying security procedures to "cyber assets" as well as physical assets; documenting the key elements of their security program; and conducting training and drills of employees, contractors and service providers to enhance response capability.
4. Verify security enhancements through independent, third parties such as firefighters, law enforcement officials, insurance auditors and/or federal and state officials. In addition, ACC member firms must conduct regular audits to assess the efficacy of security programs; commit to continuous assessment and improvement of security efforts; evaluate, respond to and report all security threats to company and law enforcement personnel; respond to any security incident, investigate its cause and take corrective action to prevent a recurrence. ■



James L. Kolstad

President and COO National Association of Chemical Distributors

In April of 2002, the NACD membership adopted specific security requirements, including cyber-security, as part of our industry code, the Responsible Distribution Process (RDP). These new security enhancements are now included in the RDP codes of management practice of all NACD members, and require third party verification beginning in January of 2003.

Chemical Sector ISAC

The Chemical Sector Information Sharing and Analysis Center (ISAC) was launched in late spring of this year through an agreement between the American Chemistry Council (ACC) and the National Infrastructure Protection Center (NIPC). The ISAC will allow vital security-related information to move effectively between the NIPC and companies involved in the manufacture, storage, transportation, distribution or handling of chemical products.

The purpose of the ISAC is to provide timely and critical information concerning potential or actual threats against the chemical industry. A primary goal of the ISAC is to enable the NIPC to disseminate timely and actionable assessment, advisories and alerts to appropriate government and private sector entities when incidents are deemed to have possible serious national security, economic or social consequences.

The Chemical Sector ISAC is operated out of the sector's 24-hour Chemical Transportation Emergency Center (CHEMTREC). In addition to the dissemination of physical and cyber threat information, the ISAC maintains an electronic communication system that allows for voluntary and secure electronic reporting to the NIPC of malicious, unexplained or suspicious incidents involving chemical facilities or chemicals in commerce.

Participation in the ISAC is open to ACC members, members of other chemical trade associations and other organizations in the chemicals sector value chain, including transportation. Membership is intended to be inclusive in order to maximize the value and utility of the ISAC, and participation is free of charge. The ISAC's website can be found at http://chemicalisac.chemtrec.com. ■

CIP LEADERSHIP HIGHLIGHT

Al Wavering
Acting Division Chief
Intelligent Systems Division
National Institute of Standards and Technology

As an agency of the Commerce Department's Technology Administration, the National Institute of Standards and Technology (NIST) has promoted economic growth by working with industry to develop and apply technology, measurements and standards since its creation in 1901. Since 1972, NIST has played a vital role in protecting the security and integrity of information in computer systems in the public and private sectors.

Under the leadership of Al Wavering, the Intelligent Systems Division (ISD) performs research and development focusing on the measurement and standards associated with the development and application of intelligent systems. The ISD is currently focusing some of its efforts in the area of critical infrastructure protection under the auspices of the Process Control Security Requirements Forum (PCSRF).

The PCSRF is working with companies and industry organizations to identify existing vulnerabilities and develop security requirements for industrial control systems. The long-term goal of this program, in conjunction with other critical infrastructure protection efforts, is for process control industries to transition to a state of low cyber vulnerability while retaining reliability, flexibility, safety, and performance characteristics. Employing a staged approach, the PCSRF plans to identify and assess threats and risks to process control information and functions; make and promote the adoption of security requirements recommendations; and, promote security awareness and integration of security considerations in the life cycle of electric power and industrial process control systems. The PCSRF is using the "Common Criteria for IT Security Evaluation" as its framework.

Currently in its initial stages, the PCSRF has brought together various industry groups to develop the requirements. On a sector-by-sector basis, the PCSRF is identifying vulnerabilities and requirements within the participating industries. The chemicals sector is one of the key industries participating in this initiative.

During the summer of 2002, the PCSRF held a meeting with the Chemical Industry Data Exchange and other government and industry groups to discuss vulnerability assessment methodologies. This meeting helped to outline a general strategy for NIST to work with the chemicals sector and to identify ways in which NIST and the sector can join efforts. Mr. Wavering stated that he has "high hopes for NIST's interaction with the chemical sector. They have allocated resources and people to work on this initiative." He stated further that the chemical sector is "an important sector to include in the work of the PCSRF."

The chemicals sector plans to continue their dialogue with NIST in the context of the PCSRF in the near future. As an industry, the chemicals sector will continue their involvement with the PCSRF through the execution and implementation of the project.

Stressing the importance of industry participation, Mr. Wavering said, "The development of requirements is a relatively small but important part of a larger effort to move from the current situation, to one in which IT security is engineered into systems in terms of their overall life cycle. We are very anxious to work with industry and to have their active participation in the PCSRF's work. Industry contributions are absolutely critical, and without them, this project will not succeed."

Securing the Chemical Industry

by Ralph Bollinger and Beth Turner

September 11 was a watershed date in more ways than one. For the chemical industry, last year's terrorist attacks forever changed the way in which we--and government--view security measures at our facilities. These unprecedented actions called for decisive, swift reactions from our industry, and we rose to the occasion by developing a Responsible Care Security Code during the first half of this year. This new security code was approved in June, in addition to the recommendations for enhancing Responsible Care.

Those in the industry know that our current security measures are already significant. Why, then, did we need a specific code to make security enhancements a requirement of membership? For one thing, we are facing a security challenge like no other. The chemical industry, like utilities and other elements of America's critical infrastructure, must examine our security practices in a new, post 9/11 light. We must do our best to satisfy ourselves--and the public--that we have taken all warranted measures to reduce the risks and severity of potential attacks. This code demonstrates that we are committed to addressing security issues head-on, and to joining President Bush's and Governor Ridge's efforts in defending our homeland.

The security code represents the latest enhancement of our industry's security. Since the September attacks, the American Chemistry Council (ACC) has been working closely with the FBI, EPA, Department of Defense, the Office of Homeland Security and other government organizations in its security efforts. It has published Site Security Guidelines and Transportation Security Guidelines and made them widely available. And in April, the ACC and the FBI-based National Infrastructure Protection Center agreed to establish a Chemical Sector Information Sharing and Analysis Center. This partnership will facilitate the flow of security-related information between chemical manufacturers and those who protect our country.

The new code establishes 13 management practices for security (see sidebar) and gives members three years to fully implement these practices. These include emphasis on senior leadership commitment to enhanced security along with important systems such as documentation, training, communications with stakeholders, incident and threat response, and audits.

In summary, the code requires member companies to implement a management system including risk assessments of potential security vulnerabilities throughout the entire value chain of our operations. As these assessments are completed, companies must develop and implement (at times in conjunction with our suppliers or customers) appropriate means to eliminate or reduce identified vulnerabilities. The entire management system must be monitored to ensure appropriate activities are occurring and that the system is achieving the desired objective of improved security.

Enhancing Site Security

Implementing one key element of the code at manufacturing facilities--site security--has been the industry's first priority. First, companies were required to prioritize their facilities into four tiers based on potential risk to the communities. ACC members accomplished this step within 90 days.

Now, members and Partners are being asked to assess the security at their facilities, using a vulnerability assessment methodology developed by Sandia National Laboratories, the Center for Chemical Process Safety (CCPS), or an equivalent method approved by CCPS. The Sandia and CCPS methodologies are now available, as are CCPS-approved member company vulnerability assessments from Air Products, BASF and ExxonMobil. Companies will begin assessments with *(Continued, Page 7)*

TIMETABLE: SITE SECURITY ASSESSMENTS

	Tier 1	Tier 2	Tier 3	Tier 4
Complete facility security vulnerability assessment	12/31/02	5/30/03	12/31/03	12/31/03
Complete implementation of facility security enhancements*	12/31/03	6/30/04	12/31/04	12/31/04
Have verification of enhancement completed	3/31/04	9/30/04	3/31/05	**

*Enhancements requiring major capital enhancements / system changes may take longer, but must be implemented as soon as practical.

**Because Tier 4 facilities do not have potential offsite consequences, they are assessed using a modified methodology and do not require third-party verification.

New Management Practices

As part of the new Security Code, each ACC member company must implement a risk-based security management system for people, property, products, processes, information and information systems throughout the chemical industry value chain. The system must include the following 13 management practices:

1. Senior leadership commitment to continuous improvement through published policies, provision of sufficient and qualified resources and established accountability.
2. Prioritization and periodic analysis of potential security threats, vulnerabilities and consequences using accepted methodologies.
3. Development and implementation of security measures commensurate with risks, and taking into account inherently safer approaches to process design, engineering and administrative controls, and prevention and mitigation measures.
4. Recognition that protecting information and information systems is a critical component of a sound security management system.
5. Documentation of security management programs, processes, and procedures.
6. Training, drills and guidance for employees, contractors, service providers, value chain partners and others, as appropriate, to enhance awareness and capability.
7. Communications, dialogue and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers and government officials and agencies balanced with safeguards for sensitive information.
8. Evaluation, response, reporting and communication of security threats as appropriate.
9. Evaluation, response, investigation, reporting, communication and corrective action for security incidents.
10. Audits to assess security programs and processes and implementation of corrective actions.
11. Third-party verification that, at chemical operating facilities with potential off-site impacts, companies have implemented the physical site security measures to which they have committed.
12. Evaluation and management of security issues associated with changes involving people, property, products, processes, information or information systems.
13. Continuous performance improvement processes entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends and development and implementation of corrective actions.

Securing Industry *(Continued from Page 6)* their highest priority facilities. Tier 1 assessments are due at the end of this year, and Tier 2 assessments are due by the end of June 2003. Companies will have an additional six months to complete assessments at both Tier 3 and Tier 4 facilities.

Next, companies must implement appropriate enhancements identified by the vulnerability assessments, again, in order of highest priority. Finally, for facilities at which any incident could have an offsite consequence, companies must have an independent third party verify that the physical site security measures that they committed to have been made. Examples of potential verifiers include local first responders, security consultants and insurance auditors.

Next Steps

Site security is just one dimension of the security code. As companies are working on securing their sites, ACC is developing security guidelines for the supply chain and information technology. Tools to assist companies to prioritize their value chain needs, and to conduct a security vulnerability assessment of this business segment, will soon be released. In addition, working with Richard Clarke, President Bush's senior advisor on cyber-security, experts from member companies are implementing a strategy to help companies improve the security of their information technology and automated process control systems. Guidance for cyber-security vulnerability assessments will be provided to the industry over the next few months.

As of July 1, the implementation clock has been ticking. Members and Partners will continue to report their progress on an interim basis until the code is fully implemented in 2005. While the work ahead will be considerable and the pace swift, it is vital that our industry deliver on this most critical commitment. ■

Ralph Bollinger is the safety, health and environment advisor for chemicals at ExxonMobil. E-mail him at ralph.l.bollinger@exxon.com; *Beth Turner is director of Responsible Care at DuPont. E-mail her at* beth.turner@usa.dupont.com.

CIP LEADERSHIP HIGHLIGHT

David Kepler

Corporate Vice President and Chief Information Officer for The Dow Chemical Company

The chemicals sector realized in early 2002 the need to accelerate cyber-security efforts already underway to further protect information and process control security. In response to this need, the industry came together to create the Chemicals Sector Cyber-Security Information Sharing Forum. Extending his role as a leader in information technology and e-business within the chemical industry, David Kepler has taken on the responsibility of Forum Chairperson. Kepler is corporate vice president and chief information officer for The Dow Chemical Company.

The Forum consists of senior-level representatives from trade associations representing more than 2,000 companies from key chemical industry segments. Its mission is to implement an industry-wide cyber-security strategy focusing on cyber-security risk management and reduction. In June 2002, the strategy was endorsed by the industry, followed by the Forum's participation in the unveiling of the "for comment" version of the National Strategy to Secure Cyberspace in September.

"The chemicals sector touches so many aspects of how we live our lives and how business is conducted throughout the world. As an industry, we have a clear understanding of the chemicals sector's contribution to individuals, communities and the global economy," said Kepler. "Moving towards the implementation of our sector strategy, we will further establish industry-wide practices and standards to support overall sector cyber-security and enhance the type and amount of information shared through the Chemicals Sector ISAC."

In addition to his numerous duties at Dow, Kepler serves on the Board of Directors of the U.S. Chamber of Commerce. He is an active member of The Research Board Inc., the American Chemical Society and the American Institute of Chemical Engineers. He received a bachelor's degree in chemical engineering from the University of California at Berkley**.**

Cyber-Security *(Continued from Page 2)* practices, the Program is aligned with the American Chemistry Council's Responsible Care® Security Code of Management Practices and outlines five key initiatives for enhancing cyber-security throughout the chemicals sector value-chain.

The first of these initiatives involves fostering involvement and commitment across the sector. Success in this track will serve as the conduit for providing the resources required to accomplish the other objectives of the strategy.

Next, establishing a cyber-security public affairs program will expand on the voluntary efforts already in place within the industry. Using the Forum as its vehicle, the public affairs aspect of the Program will provide opportunities for sector participants to advocate sector practices, policies and positions to government.

The third Program component involves the development of industry-wide sector practices and standards to protect confidentiality, integrity and availability of information for members of the chemicals sector. The Forum is working with the Chemical Industry Data Exchange (CIDX) to create cyber-security practices and standards for the global chemicals sector. Recommended practices, including management practices, procedures, guidelines and standards, are risk-based and address common issues of interest to all segments and participants in the chemicals sector. Industry-wide practices and standards lead to the creation and implementation of an information-sharing network where all members of the global chemicals business can collaborate and openly communicate ideas and concerns.

In the fourth Program initiative, the Forum is working with CHEMTREC®, the American Chemistry Council's HAZMAT emergency response center, to establish and operate the proposed network for distributing *(Continued, Page 9)*

Cyber-Security *(Continued from Page 8)* warnings of cyber-security threats, vulnerabilities and incidents.

The final initiative strongly encourages accelerating the development of improved security technology and solutions. Collaborating with information technology product and service providers, government and academia pushes forward the development and implementation of improved technologies. In turn, the industry will be able to cost-effectively address defined risks.

"A key component of any security program is to identify and evaluate the risks and the consequences of those risks in terms of vulnerability. We are confident the Program we have developed will manage and reduce risks; therefore protecting our information and keeping our operations safe," said Christine Adams, Cyber-Security Program Manager and Performance Chemicals Business Information Systems Manager at Dow. "Although the scope of this strategy is focused on the United States, we realize the global nature of the chemicals sector requires us to look beyond our borders to create a program that encompasses the business we conduct throughout the world."

Christine Adams
Cyber-Security Program Manager and Performance Chemicals Business Information Systems Manager
The Dow Chemical Company

United States domestic efforts alone cannot deter or prevent cyber attacks. The chemical industry is well aware of the need to work closely with its international partners to put into place those cooperative mechanisms that can help prevent the damage resulting from infringement on cyber-security. As the industry begins to implement its Program in the United States, the Forum will consider ways to realize its wide range of initiatives to enhance cyberspace security globally.

Forum Moves Forward with Implementation

The chemicals sector's strategy, which is fully supported by the industry's culture of safety, aims to curb potential security threats and make it increasingly difficult to invade the chemical industry's cyberspace. "Because of the collaborative spirit our industry embodies, we have the ability to quickly and cooperatively respond and will once again demonstrate this teamwork as we move forward with the cyber-security program," Adams said.

In July 2002, the completed strategy was presented to the U.S. Government. Two months later, the chemicals sector participated in the official unveiling of the "for comment" version of the President's National Strategy to Secure Cyberspace, which represents the sector's interests within its "Level 3: Critical Sectors: Private Sector" section. Strategy implementation relies on the cooperation of industry leaders. In October 2002, project teams aligned with each Program component began implementing their plans. Through the remainder of the year, the teams will identify immediate opportunities to improve the base level of cyber-security within the industry. They will also begin leveraging existing industry capabilities to improve security processes and establish better cyber-security practices for the future.

Some of the immediate opportunities being pursued within the Cyber-Security Program include:

- Comments from the chemicals sector on the draft National Strategy to Secure Cyberspace were recently submitted to the President's Critical Infrastructure Protection Board.
- A Plan of Engagement with each trade association for their respective member companies is in development. Effective engagement is critical to raising awareness across the sector and increasing the rate of adoption of practices and standards as they are rolled out to the industry.
- Plans for a recommendation on the adoption of the ISO 17799 standard for guidance on management practices are being put in place to facilitate "self assessment" against the ISO standard.
- Cyber-security assessment guidelines are being integrated with the vulnerability assessment methodologies being used to comply with the new Responsible Care® Security Code.
- The sector is collaborating with organizations like NIST and ISA to establish cyber-security standards appropriate for the chemical industry.
- The CHEMTREC ISAC is expanding its current capabilities to provide a broader audience across the sector with incident reporting, virus alerts, threat warnings and vulnerability reporting.

The next few years will show a continual improvement of capabilities within the chemical industry to manage risks, as different degrees of implementation are reached. ■

Chemical Industry Data Exchange

The chemical industry must work together to create standards that will promote inter-company productivity. Standards will enable every company to apply Information Technology to ensure the security of manufacturing and supply, increase productivity

Pat Simmons

Executive Director CIDX

and improve the sustainability of the industry. As the chemical industry becomes more integrated through e-business, issues such as security, transaction reliability, business processes and standardization become increasingly important.

CIDX provides a neutral industry forum for industry participants, in an appropriate manner, to enlist each other's assistance in creating data and business

Brian Harmon

Chairman of the Board of Directors CIDX

process alignment standards - which could be leveraged to help address cyber-security as well. Because of the nature of e-business, industry standards are critical to maintaining industry unity and safety. Together, the chemical industry can create a truly vibrant, efficient and high-impact e-business environment, free of cyber-security fear--but only if as an industry, we understand that we are best served by continuing to work together to improve our capabilities.

Chemicals Sector Responds to National Strategy

In September 2002, the Chemicals Sector Cyber-Security Information Sharing Forum participated in the unveiling of the "for comment" version of the President's National Strategy to Secure Cyberspace. For the National Strategy to be effective, it must be a plan to which a broad cross-section of the country is committed. To achieve this nation-wide agreement, the government requested input from various industry sectors as well as the general public.

The Forum was among the critical infrastructures to contribute to the national cyber-security strategy. The Forum recognizes the thorough job the Critical Infrastructure Protection Board has done addressing cyber-security issues in the Strategy and has also taken the opportunity to review and offer comments on the sector's perspective of the National Strategy.

"The chemicals sector commends the government for developing a strong and proactive plan that addresses the nation's cyber-security concerns," said David Kepler, corporate vice president and chief information officer for The Dow Chemical Company. "We are pleased to work with the government to be part of such a vital and expansive effort to secure information and protect our country's interests and future involvement in cyberspace."

In its response to the National Strategy, the Forum recommended that the National Strategy designate the Department of Homeland Security as the lead agency partner for the chemical industry. The National Homeland Security Strategy shows a commitment to serious critical infrastructure cyber-security. The Department of Homeland Security is designed with the expertise and structure to manage cyber-security under partnership. For these two reasons, the chemicals sector is proposing its alignment with the Department of Homeland Security.

Additionally, the Forum suggests the National Strategy more forcefully reflect the Administration's position on information-sharing legislation. Currently, the Strategy addresses basic cyber-security concerns, but real information sharing among businesses and between businesses and government has been limited by concerns that such information may still be disclosed under the Freedom of Information Act. The Forum *(Continued, Page 14)*

Chemical Security in an Age of Terrorism

America's war on organized terror, unlike past conflicts, involves an enemy that directly threatens citizens and institutions within our borders. It is in great part a defensive war, requiring substantial public and private investment in homeland security measures. The challenge, however, is to reduce the threat of terrorist attacks while simultaneously preserving our way of life and protecting critical national assets.

Through grim experience, the American public has learned that anyone or any place is a potential target. High on the list of security concerns is the nation's industrial infrastructure, which encompasses not just productive capacity but also utilities, transportation hubs, health centers and information technology.

The chemical industry is a vital part of this infrastructure – a $450 billion business that directly employs more than one million Americans and sustains five million additional jobs in related industries. Chemical products pervade nearly every sector of society and contribute enormously to the public's health and economic welfare.

Moreover, chemicals are essential to national defense. Chlorine chemistry, for example, aside from ensuring the safety of drinking water and contributing to the production of thousands of beneficial products, is a crucial weapon against the threat of anthrax. It is used both in decontamination and in manufacturing antibiotics such as Cipro® and doxycycline. The impact of a crippling attack on a chlor-alkali plant would extend far beyond the surrounding community, potentially affecting downstream industries such as food processing, water disinfection, health care – even construction and communications.

Thus, the overriding challenge is to achieve plant security without impeding the production of chemicals that are vital to national defense and public health. Recent public opinion polls indicate that most Americans favor this approach to chemical security. According to data obtained by California-based Charlton Research Company (CRC) through focus groups and a national telephone survey[1], more than 90% of respondents supported the view that security measures at chemical facilities should not impede the production of important chemicals. A majority (54%) also agreed that the best way to keep plants secure is to reduce terrorists' access to them, not to require changes in production methods.

Yet despite increased apprehension and concern in the aftermath of September 11, more Americans today recognize the complexities involved in ensuring our national security and favor responses that address immediate defense needs, as well as long-term strategic and economic interests.

In fact, Charlton's research findings signal what may be an important change in public attitudes toward risk. While 56% of current respondents support "prudent, workable plans" for preventing terrorist attacks on chemical facilities, only 37% favor taking every possible measure to eliminate risks, including curtailing production. Interestingly, this contrasts with 1999 research that revealed a strong preference for the "precautionary principle[2]," an approach that calls for avoiding or eliminating all real or even potential risks (59% in favor, 29% opposed).

Most Americans appear to recognize that achieving "zero risk" is impossible. A significant majority (73%) believe that some degree of risk is necessary for society to go forward and make progress. The question is how can this best be done in the area of chemical security.

Protecting our country means protecting it on all fronts: our people, our businesses and our way of life. To do this government and industry must work together. The government should provide information, assistance and oversight, while industry has the experience and ability to undertake efforts to ensure the safe production, distribution, and storage of the chemicals it produces. Once again, Charlton's research reveals that the American public wants a balance between industry and government in addressing security concerns.

Fortunately, both groups appear to be moving in the right direction. With Congressional approval of the new Department of Homeland Security virtually assured, the government will be better able to develop and coordinate a comprehensive national plan to protect America's infrastructure from terrorist attack. Likewise, members of the American Chemistry Council, which together comprise more than 90% of the nation's chemical production, are now implementing new security measures as part of the association's required Responsible Care® program. Using methodologies developed by the U.S. Department of Justice, the program emphasizes preventing an attack as opposed to managing the consequences of a terrorist incident. It draws upon the industry's widespread risk management expertise to address site, transportation, *(Continued, Page 12)*

JMU Professor to Use a Graphical Programming Environment to Model Probabilistic Risk Assessment

Dr. Joe Blandino of the Department of Integrated Science and Technology at James Madison University will be conducting a feasibility study that will develop a Probabilistic Risk Assessment Model using the LabVIEW Graphical Programming Environment. The deliverable for this project will be a probabilistic risk model of a communications center developed using LabVIEW. Using a graphical programming language, the LabView software offers advantages in developing user interfaces. Dr. Blandino and two JMU undergraduate students will be conducting the study.

The current state of world affairs necessitates that infrastructure providers in each identified critical sector evaluate where their systems are vulnerable and the costs associated with system down time. Even in a world free of extremist activities this information is useful to predict damages and costs resulting from natural disasters, human error and Murphy's Law. Current modeling techniques to predict system vulnerabilities and failure are effective, but model development requires specific programming expertise.

LabVIEW is a graphical programming language that is optimized for data acquisition and process monitoring. LabVIEW allows the development of visually appealing and intuitive user interfaces. These interfaces can be developed with minimal programming experience. For probabilistic modeling, each system component will be a separate subroutine. Developing these subroutines is the primary objective necessary for achieving the goal of this project. Once developed, these subroutines can be easily connected or "wired" together through logic icons. All that will be required to develop a probabilistic risk assessment model is connecting the system components in the appropriate fault tree. The component subroutines will become the building blocks for any infrastructure system. Since there will be minimal programming other than graphically connecting components in a fault tree, anyone with knowledge of how the system components interact will be able to build an accurate model.

If the goal of this project is achieved, the resulting software tools will benefit a wide range of users from insurance companies to large corporations to local health care facilities. Current technology, although effective, is not suitable for use by non-programmers. Unique problems are faced by each sector of critical infrastructure; this is why it is important that we demonstrate an easy to use decision identification tool that can be used by non-programmers in a variety of industries to address a broad range of vulnerabilities.

Chemical Security *(Continued from Page 11)* and cyber-security vulnerabilities. It also employs independent, third-party verification process to ensure compliance.

There have been a number of legislative and regulatory attempts to address chemical plant security. However, none has emerged that address the inherent complexities of this issue, mainly because it has been dealt with as an environmental, rather than a homeland security concern. Activist groups, such as Greenpeace, have promoted this environmental approach, using security as a platform for advancing an anti-chemical agenda. The goal appears to be an attempt to cast industry, rather than terrorists, as the enemy.

One way activists have done this is by publicly promoting the availability of "worst case scenario" information for individual chemical facilities, even after the Federal Bureau of Investigation, Environmental Protection Agency, and other federal organizations determined it was potentially helpful to terrorists and pulled the material from government web sites and reading rooms.

The Charlton research also addressed this question and found that eight out of ten Americans agreed that posting data about industrial sites and "worst-case" accident scenarios on private web pages could pose a threat to national security. Further, more than two-thirds of the respondents were in favor of actually removing information from government web sites that could be useful to terrorists, even if it limited their own "right-to-know" about activities in their community. This view was supported by similar research conducted by the Pew Center on Internet Life. Clearly, sensitive information about chemical plant vulnerabilities and security plans should be restricted to government officials, first responders, *(Continued, Page 15)*

Value Chain Guidance Systems Are A Go

by Heather Rhoderick, Manager, Responsible Care Team, ACC

2002 will be remembered in the chemical industry as the year that launched Responsible Care® to the next level and introduced the new Security Code. Both will have a profound impact on the industry--both its operations and how it is viewed by the public.

The value chain is an integral part of the chemical industry. In addition to chemical manufacturers, many other players are responsible for delivering products and getting them to the ultimate end user. All involved players share responsibility relating to security, and all should work together on the security of products once they leave plant gates.

Toward that end, a guidance document to aid members in implementing the code throughout the value chain is scheduled to go online in the near future. This document will address off-site--such as transportation, distribution, storage and customers--as well as more traditional product stewardship issues.

As with any good guidance system, this resource will give *approaches* on how to implement the Security Code from a value chain perspective rather than trying to provide all the answers. This is not a one-size-fits-all approach. Developed with input from American Chemistry Council member and partner companies, as well as other organizations outside of ACC's membership, the guidance materials will provide assistance in implementing all aspects of the Security Code from a value chain perspective, including prioritizing value chain activities and conducting security risk assessments, which include analysis of threats, vulnerabilities and consequences.

Many Responsible Care companies will find similarities between the approaches outlined in this guidance and their current distribution and product stewardship processes put in place through Responsible Care. To help users see the connections and overlaps between value chain aspects of the new Security Code and their current Responsible Care activities, a matrix comparing distribution and product stewardship activities with the new Security Code is provided in the guidance documents.

CHEMICALS SECTOR CYBER-SECURITY INFORMATION SHARING FORUM

American Chemistry Council	http://www.americanchemistry.com
The Chlorine Institute	http://www.cl2.com
Compressed Gas Association	http://www.cganet.com
Consumer Specialty Products Association	http://www.cspa.org
CropLife America and Agricultural	http://www.croplifeamerica.org
Dangerous Goods Advisory Council	http://www.hmac.org
The Fertilizer Institute	http://www.tfi.org
Institute of Makers of Explosives	http://www.ime.org
National Association of Chemical Distributors	http://www.nacd.com/index.cfm
National Paint and Coatings Association	http://www.paint.org/
Synthetic Organic Chemical Manufacturers Association	http://www.socma.com

Synthetic Organic Chemical Manufacturers Association (SOCMA)

As SOCMA Vice President Kathleen Shaver explained, SOCMA worked this year with the American Chemistry Council (ACC) to develop the new security code. “We are currently engaged in an aggressive outreach campaign to educate our member firms on the requirements of the new code including assessment of cyber systems.”

SOCMA's board approved the new security code in September, and the membership will be voting on it on December 10. "I predict that on December 10th SOCMA member firms will vote in favor of adopting the 7th code of Responsible Care," says SOCMA President Ed Fording.

Ed Fording
President
SOCMA

Looking to the year ahead, Fording notes that a challenge for both SOCMA and ACC is the need to address those firms that are not members of either association. "Regulators and others often express concerns about the part of the industry that does not participate in Responsible Care," he says. "SOCMA has increased its outreach to these companies to educate them about Responsible Care as well as encourage them to become members."

To help all chemical facilities assess security vulnerabilities, SOCMA has developed an asset-based security vulnerability assessment (SVA) methodology for analyzing the existing security measures at a facility and identifying areas in need of improvement. Fording notes that other available methodologies don’t take into account many of the issues faced by batch and custom manufacturers. "SOCMA has provided the industry with an additional tool that reflects the unique circumstances of batch processing," Fording says. "I am happy to say that the SVA model has been approved by the Center for Chemical Process Safety (CCPS) and can be used to help meet the requirements of the industry's new Responsible Care Security Code." According to project manager Jim Cooper, the SOCMA SVA model will be available free of charge at www.socma.com.

Strategy *(Continued from Page 10)* urges the prompt and vigorous implementation of the Critical Infrastructure Information Act of 2002, which exempts voluntarily submitted critical infrastructure information from FOIA, when the protection is requested.

The Forum is also concerned that the National Infrastructure Protection Center (NIPC) continue to serve as the central point of contact for supplying threat information from the federal government to the chemicals sector. Since many of its members participate in the Chemicals Sector Information Sharing and Analysis Center (ISAC), the Forum wants to ensure that sector companies do not start receiving varying and potentially confusing threat information from multiple government agencies. In accordance, the Forum urges the National Strategy to reflect the role that the NIPC is intended to serve.

Finally, the Forum is uneasy with the Strategy grouping all process automation and control systems under the heading of Supervisory Control and Data Acquisition (SCADA). The distributed control and SCADA systems have very distinct differences, and must be treated separately from a security perspective. The Forum encourages the Strategy to specify expected principles and outcomes, rather than suggesting technology solutions.

The National Strategy was created to address cyber-security concerns. By weaving the Forum’s suggestions along with input from other sectors and the American public into the current formula, the National Strategy will be made that much stronger. With continuing refinement to reflect the ever-changing technological landscape, the Strategy will reach the ultimate goal of achieving a safe and secure cyberspace. ■

Chemical Security *(Continued from Page 12)* and other public health and safety officials who have a legitimate and pressing need for it.

As the United States moves forward in addressing chemical plant security, it is clear that while it is a difficult and significant challenge, it is also a manageable one. It is paramount that care be taken to ensure that efforts, while well-intentioned, do not inadvertently compromise the very security we seek. The full cooperation of government and industry will be key. The American public expects – and deserves – no less. ■

[1] Charlton Research Company, "National Issues Survey", 2002. Funding provided by the Chlorine Chemistry Council®.

[2] The Precautionary Principle, as defined in the 1999 survey, "generally means that a product or material should be banned from the market if there is any doubt about its safety - regardless of the benefits of the product or scientific evidence that could prove it safe. It also states that new technologies or products should not be permitted until we know with certainty that they won't endanger people's health and safety or the environment. Finally, it states that government policies should be based on what might cause harm - even if there is no scientific evidence that a hazard exists." (Charlton Research Company for ACC, November 1999)

TFI Establishes Security Code for Fertilizer Industry

The Fertilizer Institute (TFI) recently announced the adoption of its "Security Code of Management Practices for the Fertilizer Industry" to help the industry protect people, property, products, processes, information and information systems by enhancing security, including the security against a potential terrorist attack.

"This code provides formal recognition of the increased security measures the fertilizer industry has adopted over the past year, and demonstrates our industry's expanded awareness of and commitment to security in the wake of the Sept. 11, 2001 terrorist events," said TFI President Kraig R. Naasz.

Kraig Naasz

President
TFI

The code is designed to help the fertilizer industry achieve continuous security performance. It also addresses the issue of cyber-security and the potential of an attack on information systems, a critical component of a sound security management system. Using a risk-based approach the code helps identify, assess and address vulnerabilities, prevent or mitigate incidents, enhance training and response capabilities, and maintain and improve relationships with key state, local and federal government partners.

Implemented with the understanding that security is a shared responsibility requires action by all stakeholders including carriers, customers, suppliers, service providers, government officials and agencies. It establishes a timeline for completion of site security vulnerability assessments, implementation of security measures to address identified vulnerabilities as well as a timeline for verification of those measures by a third party.

"This new security code embodies the industry's vigilant approach to the safekeeping of its products," said Naasz. "The tiered approach in establishing a timeline for implementation of security measures recognizes the site-specific nature of fertilizer industry security and ensures that the most vulnerable facilities are placed at the top of the priority list."

Under the code, manufacturers, agribusiness retailers and distributors are encouraged to use a vulnerability assessment method developed by the Agribusiness Security Working Group (whose members include TFI, the Agricultural Retailers Association (ARA) and CropLife America), the Council for Chemical Process Safety (CCPS) or the Synthetic Organic Chemical Manufacturers Association (SOCMA). Results of the vulnerability assessment will provide facility management with a means of ranking the facility's risk level and help establish a corresponding timeframe for completion of security measures.

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

If you would like to be added to the distribution list for *The CIP Report,* please send an e-mail to cipp01@gmu.edu.