Making Strides to Improve Cyber Security in the Chemical Sector

2009 Update

ChemITC Executive Board Companies

Albemarle
Arch Chemicals
Bayer Material Sciences
The Dow Chemical Company
Dow Corning
Eastman Chemical Company
PPG Industries
Rohm and Haas
Shell Chemicals

This document is intended to update the White House Office of Cybersecurity on the chemical sector's efforts to enhance cyber security.

Recognizing the importance of working together to enhance the security of business and manufacturing control systems, the chemical sector launched a sector-wide initiative in 2002. Stemming from a long history of organizing to address issues as a sector, ten chemical trade associations came together to address the cyber security challenge. A taskforce of industry experts from a variety of disciplines was chartered to create a sector-wide strategy. The Chemical Sector Cyber Security Strategy was published in June 2002 and was later referenced by the National Strategy to Secure Cyberspace when it was released in February 2003.

The Chemical Sector Cyber Security Program was established specifically to implement the sector's strategy. The Cyber Security Program originally leveraged existing organizations – the ten chemical industry trade associations, the Chemical Industry Data Exchange (CIDX) and the Chemical Information Sharing and Analysis Center (ISAC) – to accomplish work in five strategic areas.

- Foster involvement and commitment across the sector
- Develop a robust cyber security public advocacy program
- Encourage the adoption of responsible sector practices and standards
- Strengthen the industry's information sharing network
- Encourage the acceleration of improved technology and solutions development

In 2006, the chemical sector examined its progress against the original strategy and redefined the path forward. An updated strategy was published in September 2006, outlining the sector's plans to continue facilitating improvements to IT and industrial automation and control systems security. It also built on the chemical sector's many achievements in enhancing cyber security since the original strategy published in 2002.

Today, the Chemical Sector Cyber Security Program is managed by the Chemical Information Technology Center (ChemITC®) of the American Chemistry Council (ACC). A forum for companies in and associated with the ACC to address common IT issues and support the industry's ability to safely and efficiently deliver products essential to society, ChemITC is taking a lead on cyber security activities in the chemical industry. ChemITC's focus enables the Cyber Security Program to address maturing cyber security needs and serve as the industry's focal point for cyber security information, guidance and tools.

The Cyber Security Program is once again undergoing a strategic review of its vision and progress against stated goals and revitalizing its plans for the years ahead. An updated strategy is scheduled for release in the third quarter of 2009.

What Are the Potential Impacts of a Cyber Security Attack?

In 2004, an industry-level vulnerability assessment was conducted to better understand approaches to both prevent and reduce potential impacts of cyber security threats. The available information suggested that a cascading impact was unlikely. However, unless adequate safeguards are in place, cyber attacks could result in risks to plant employees and communities, business interruption, lost capital and more. The potential of a combined physical and cyber attack and the criminal use of illegally obtained information represented possible threat scenarios that could impact industries such as the chemical sector. In addition, without the use of protective measures, there was an increased risk of threats such as:

- Using shipment, product inventory or site information to construct a physical attack
- Stealing personal identity information to acquire chemicals for improper use
- Gaining inappropriate access to systems to cause isolated disruptions

Having a set of policies, practices and technologies in place to protect the linkage of critical plant systems with corporate networks, and to pre-identify and verify customers before conducting business electronically, helps address these scenarios. Additionally, frequently upgrading operating practices and authentication technology to restrict what people can access based on roles and clearances reduces opportunities for improper actions and associated hazards.

What is the Chemical Sector Doing to Enhance Cyber Security?

Driving Adoption of Sector Practices: The Chemical Sector Cyber Security Program has developed a set of guidance documents and white papers designed to help chemical companies evaluate, assess and improve the security of their business and manufacturing systems. These documents are offered free of charge to the broader chemical sector on the Cyber Security Program's Web site – www.chemicalcybersecurity.com. Increasing the implementation of cyber security guidance and tools continues to be a primary focus of the Cyber Security Program. Working with the Chemical Sector Coordinating Council's sixteen chemical industry trade associations, the Cyber Security Program strives to integrate cyber security into the trade associations' security or product stewardship initiatives and encourage their member companies to implement cyber security guidance.

Supporting Industrial Automation and Control Systems Security Efforts: A variety of outside industry organizations are working to develop practices and standards for industrial automation and control systems. Representatives from the Cyber Security Program are participating in the efforts of these organizations, including the ISA-99 committee working groups, the Department of Homeland Security (DHS)-sponsored Industrial Control Systems Joint Working Group (ICSJWG), the DHS-funded Idaho National Laboratory (INL) Control Systems Security Center, the National Institute of Standards and Technology (NIST) Process Control Security Requirements Forum (PCSRF), the Institute for Information Protection (I3P) and others. The Cyber Security Program is also working diligently so that manufacturing and control systems perspectives are integrated into the work of its various project teams.

Accelerating the Development of Improved Technology: Improving existing and yet-to-be-developed technology solutions is a fundamental aspect of enhanced cyber security. The Cyber Security Program continues to work with technology providers to help ensure they are aware of, and can appropriately respond to, the technology issues and positions advocated by the Cyber Security Program and ChemITC. The Cyber Security Program is also examining and reporting on a number of key issues affecting the industry, and is working to establish relationships with other sector organizations and infrastructure sectors in order to promote chemical industry issues to government and research communities.

Enhancing Sector Information Sharing: The Cyber Security Program helps provide a trusted environment for information sharing within the chemical sector. The Cyber Security Program also continues to explore available information sharing processes and tools to determine how they could best serve the sector's needs. A variety of tools – including the Business Roundtable's CEO ComLink, the Homeland Security Information Network – Critical Sectors (HSIN-CS), the United States Computer Emergency Readiness Team (US-CERT), the Government Emergency Telecommunications Service (GETS) and others – enable chemical companies to respond to emerging threats, reduce the impact of cyber security incidents and be better positioned to maintain safe and secure operations. The Cyber Security Program is also actively working with the Department of Homeland Security (DHS) to improve the availability, reliability and accessibility of threat information for the sector. Current information sharing initiatives underway include establishing a chemical sector cyber crisis communications capability and an information sharing pilot with DHS intended to facilitate the exchange of information between the chemical sector and DHS on the impact of cyber vulnerabilities and cyber incidents.

The Chemical Sector and DHS – Working Together on Cyber Security

The Chemical Sector Cyber Security Program continues to align its priorities with those of the Department of Homeland Security. The Cyber Security Program works closely with DHS on a number of initiatives positioned to advance the cyber security agendas of both organizations. Listed below are the current priority initiatives underway with DHS.

National Cyber Security Division (NCSD)

- **US-CERT Chemical Compartment** – The Cyber Security Program promotes the use of the chemical sector compartment within US-CERT, designed to provide a secure environment for sharing information between DHS and the chemical sector.

- **Cyber Security Vulnerability Assessment (CSVA)** – The Chemical Sector Cyber Security Program continues to increase awareness in the sector of the availability of the CSVA tool for use in companies that currently do not use a cyber security vulnerability assessment tool.

- **Roadmap to Control Systems Security** – A robust initiative is currently underway to define the chemical sector roadmap, as well as to find commonalities with the roadmaps from other sectors that utilize industrial automation and control systems. The results of this effort will feed the National Coordinating Strategy for Control Systems.

Cross-Sector Cyber Security Working Group (CSCSWG)

The director of the Chemical Sector Cyber Security Program regularly participates in this cross-sector working group sponsored by DHS/NCSD. The following initiatives are currently underway:

- **Project 12** – The Cyber Security Program contributed to DHS's response to a request for private sector input on Project 12. Project 12, an initiative commissioned by the White House under the Comprehensive National Cybersecurity Initiative (CNCI), published a report detailing the policy and resource requirements for improving the protection of privately owned U.S. critical infrastructure networks. The report detailed how the federal government can partner with the private sector to leverage investment in intrusion protection capabilities and technology, increase awareness about the extent and severity of cyber threats facing critical infrastructure, enhance real-time cyber situational awareness and encourage specified levels of intrusion protection for critical information technology infrastructure.

- **Information Sharing Pilot** – Monthly conference calls intended to provide a forum for dialogue about security sensitive, but unclassified information on potential cyber threats and vulnerabilities.

- **Metrics Sub-Group** – The chemical sector is providing input on the development of sector-level cyber security metrics.

Industrial Control Systems Joint Working Group (ICSJWG)

- This working group is in the process of being established. Representatives from the Chemical Sector Cyber Security Program are committed to active involvement in this important DHS/NCSD-sponsored cross-sector working group.

National Exercises

- **Cyber Storm II** - The Chemical Sector Cyber Security Program facilitated the participation of 10 chemical companies in the Cyber Storm II exercise conducted in March 2008. In addition to the learnings of the individual companies participating, the exercise revealed the value of a sector-level crisis communication process. An initiative is currently underway in the chemical sector to develop a crisis communication capability that includes participation by cyber security, physical security and transportation security professionals.

- **Cyber Storm III** – The Chemical Sector Cyber Security Program plans to participate in the Cyber Storm III exercise in 2010 to test the new crisis communication process that is currently under development.

Infrastructure Compliance Standards Division (ICSD)

The Chemical Sector Cyber Security Program provided input to DHS, and has helped increase industry awareness and compliance, regarding governmental security standards for the chemical sector.

- **Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS)** - During the development of the regulations, the Chemical Sector Cyber Security Program made its guidance documents available to DHS to share its knowledge on the use of cyber systems in the chemical industry, as well as the steps many chemical companies have taken to implement risk-based measures to help enhance the security of these systems. In addition, the Cyber Security Program offered comments on the cyber components of the CFATS-RBPS. The Program continues to work with DHS ICSD in communicating the RBPS to the sector and facilitating understanding of how to apply the standards and comply with the cyber components of CFATS.

Chemical Sector-Specific Agency (SSA)

The Chemical Sector Cyber Security Program works closely with the Chemical SSA to help ensure that cyber security is integrated into the sector's overall security plans and initiatives.

- **Chemical Sector Monthly Unclassified Suspicious Activity Call** – Cyber security professionals from across the sector are invited each month to participate in this information sharing call. These calls include updates from the US-CERT.

- **Sector-Specific Plan** – The Cyber Security Program provides cyber security input to the overall Chemical Sector-Specific Plan (SSP)

- **Sector Annual Report** – The Cyber Security Program provides cyber security input to the Chemical Sector Annual Report (SAR)

- **Sector Outreach and Awareness Program (SOAP)** – The Cyber Security Program continues to raise awareness across the sector about the availability of this voluntary DHS program.

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

- **Strategic Homeland Infrastructure Risk Assessment (SHIRA)** – The Cyber Security Program participates in the annual development of potential cyber threat scenarios that are deemed to pose the highest threat to the chemical sector.

How Can Technology Providers Support the Chemical Sector's Cyber Security Efforts?

Suppliers of IT products and services are best positioned to address issues within the solutions they create and have a responsibility to test and enhance product security before releasing items into the marketplace. The Cyber Security Program is calling on information technology suppliers to design their solutions to maintain highly-available systems, support future versions of these long-lived assets and make a more formal commitment to product reliability, integrity and security. Hence, technology providers should more fully embrace the philosophy of **secure by design**.

Technology providers should deliver cost-effective solutions with capabilities that enhance their customers' ability to secure them. Key functionalities important to all solutions include:

- **User Accounts and Passwords** – Delivery of solutions that give customers the option to change the passwords on all built-in accounts and store passwords in a secure manner, offer password configuration flexibility to accommodate strong passwords and integrate with common authentication solutions to offer single sign-on.

- **Access and Authorization Controls** – Delivery of solutions that have well-documented granular access control and authorization capabilities. Do not expect customers to grant high-level/broad access to system accounts within the solution delivered.

- **Vulnerabilities and Patching** – Delivery of solutions that have well-documented operating system (OS) service dependencies to allow customers to disable functionality that is not needed. Certify technology solutions against OS patches quickly to give customers confidence in applying the patches.

- **Audit, Logging and Reporting** – Delivery of solutions that have well-documented logging and reporting capabilities to allow for customer auditing.

The chemical sector's cyber security efforts rely on increased coordination between technology providers and the industry to foster an understanding of the common and unique needs of the sector, begin enhancing the security of products scheduled for release and enable technology providers to become better stewards of their IT products and services. Information technology providers are invited to join the Cyber Security Program as affiliate members so that working directly with ChemITC, they can strive to better understand and address the chemical sector's security and technology needs. Affiliate membership is available to organizations engaged in the provision of hardware, software and IT services to the chemical industry.

How Can Government Support the Chemical Sector's Cyber Security Efforts?

The scope of the cyber security challenge is beyond any one company or sector's control. Government involvement is crucial to addressing the issue. The Cyber Security Program supports the findings and recommendations that the National Infrastructure Advisory Council (NIAC) published in its Critical Infrastructure Protection Strategic Assessment on October 14, 2008. A link to that report is included here:

http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf

The chemical industry and government must work hand-in-hand to develop useful, sensible and cost-effective measures that address potential threats in a manner that is operationally viable for both companies and the government. It is through cooperation and participation that sound legislation can be established. Such cooperation will help ensure that legislative initiatives for chemical sector security are aligned with, and flexible enough to address, the evolving cyber security challenges.

The government should continue to invest in research initiatives underway in organizations like Idaho National Labs (INL), the National Institute of Standards and Technology (NIST) and the Institute for Information Infrastructure Protection (I3P). For example, in addition to its role in protecting national infrastructure, DHS needs to make resources and research funds available to assist and augment the chemical sector's efforts. This includes developing models for optimizing information sharing, enhancing the reliability of operational systems, creating methods of containing cyber security problems where they strike to limit the broader effect and improving investigative techniques to allow for proactive mitigation of and rapid response to security risks.

Groups like NIST can assist the chemical industry in creating and implementing practices that will help the chemical sector, as well as other industrial sectors, address the ever-evolving issue of cyber security in a coordinated manner.

The chemical sector's interaction with the DHS-funded Control Systems Security Center, which is operated by INL, enables the Cyber Security Program to see that the chemical sector's perspective is represented and addressed as the Center identifies and develops solutions to protect the nation's vital infrastructures from cyber attacks. Control system vulnerability and risk assessments, tool development and incident response are among the areas the chemical sector can leverage as it seeks opportunities to enhance its systems.

In addition, the government could help by providing the incentive for technology providers to deliver cost-effective technology solutions that move from a philosophy of "security is the responsibility of the user" to one of accepting the responsibility to design security into the solution in such a manner that provides the customer with the ability to manage and maintain the product securely (please refer to the capabilities listed in the previous section on technology providers support).

For More Information

The Chemical Sector Cyber Security Program is available to assist chemical companies as they work toward enhanced information technology and industrial automation and control system security. Please visit our Web site – www.chemicalcybersecurity.com – or e-mail us at cybersecurity@chemitc.com for more information about the Cyber Security Program.

You can also contact the following people for more information about ChemITC and the Chemical Sector Cyber Security Program.

- Bridgette Bourge, Panel Manager, ACC ChemITC
  Email: bridgette_bourge@americanchemistry.com
  Phone: (703) 741-5630

- Christine Adams, IT Public Policy, The Dow Chemical Company
  Director, Chemical Sector Cyber Security Program
  Email: cmadams@dow.com
  Phone: (202) 429-3417