U.S. Chemicals Sector Cyber-Security Strategy

Reducing the Risks to Our Society and Economy by Leveraging Technology, Processes and People to Protect Chemicals Sector Cyber-Security

Prepared By:

The Chemicals Sector Cyber-Security Information Sharing Forum
Cyber-Security Strategy Task Team

June 2002

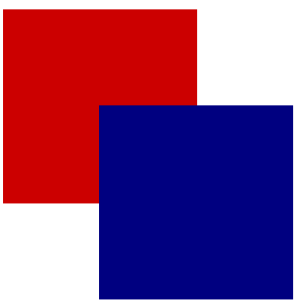

Table of Contents

1. Executive Summary

The chemicals sector provides the essentials of modern life. Because the sector touches so many aspects of how we live our lives and how business is conducted throughout the world, communications technology, connectivity and information exchange are essential aspects of all company operations and processes in the sector. However, the same technologies that make business operations and manufacturing processes more efficient can introduce new vulnerabilities. As the world faces increased threats, the chemicals sector needs to increase its capability to manage exposure to information security risk and protect against the threat of unauthorized access to information being used to facilitate or cause a physical attack. Cyber-security is an integral part of overall security, and the industry will address the risk as a sector-wide initiative, to minimize the potential impact to both public safety and the economy.

Reducing current and future information security risks will require a combination of leading-edge technology, accepted sector practices and timely information sharing throughout the sector. Fortunately, the type of sector-wide cooperation called for to address cyber-security issues has many precedents in the chemicals sector. Established, proven programs are in place to help the sector confront the current threat – from an emergency communications network to global industry associations and standards bodies that provide the groundwork for improving current security processes and establishing better cyber-security practices for the future. The sector's culture of safety gives the industry an added advantage – from its longstanding voluntary initiatives to its adherence to governmental standards, support for research and effective partnerships with local, state and federal government agencies.

The recently formed Chemicals Sector Cyber-Security Information Sharing Forum, which consists of global chemicals sector trade associations and individual companies representing key industry segments, has developed a sector cyber-security strategy to guide the industry's efforts. Recommendations in the strategy include developing a Chemicals Sector Cyber-Security Program that focuses on cyber-security risk management and reduction to provide open, secure information and process control systems that help protect communities and enable collaborative business operations. The risk-based program meets both the common and unique cyber-security needs of each segment and company type in the sector.

The program includes fostering involvement and commitment across the sector; establishing a cyber-security public affairs program; establishing voluntary sector practices and standards; establishing an information sharing network; and encouraging acceleration of improved security technology and solutions development. The program calls for leveraging collective knowledge, shared technology and practices development to establish industry-wide voluntary practices and standards. The proposed Cyber-Security Information Sharing Network will distribute advance warnings of cyber-security threats, vulnerabilities and incidents. The program will also foster collaboration with information technology product and service providers, government and academia to accelerate development and implementation of improved technologies and methodologies to cost-effectively address defined vulnerabilities.

When approaching cyber-security, the chemicals sector will leverage technology, processes and people to implement the same proactive, collaborative approach that it has taken on previous issues of global importance. The sector is committed to developing the standards, products and practices necessary to shield proprietary information, facilitate safe operations and protect our way of life by playing an essential role in the nation's first line of defense against terrorism.

2. Chemicals Sector Background[1]

The chemicals sector is an essential element of the nation's economic security, our homeland defense and the public's health and welfare. As a critical infrastructure sector, the chemicals sector has a rich history of providing products that are essential to the U.S. economy and way of life. The sector includes manufacturers and distributors of more than 70,000 products, including basic and intermediate chemicals, specialty chemicals, agricultural chemicals, fertilizers, petrochemicals, plastics and fibers, paints and coatings and pharmaceuticals. As a $450 billion business, the chemicals sector directly employs more than one million Americans and accounts for another five million related jobs in the U.S. economy. The nation's food, safe water supply, clothing, shelter, health care, computer technology, transportation and many other facets of modern life depend upon the business of chemistry.

An analysis by the National Research Council found that 20 percent of the U.S. economy is generated with the help of catalysis, which is just one of many processes of chemistry. More than $97 billion of the sector's products go to health care alone. Modern chemistry enables other mainstays of the economy, such as the agricultural, communications, construction and automotive industries. The chemicals sector is the nation's top exporter, at $80 billion in shipments, accounting for 10 cents out of every dollar in exports. The sector pays one-third higher wages than any other manufacturing sector, invests $30 billion in research and development activities and accounts for one of every seven patents issued by the U.S. Patent and Trademark Office.

The security and reliability of the chemicals sector benefits all other critical infrastructure communities – communities that rely on the secure delivery of chemicals to serve the nation's security and defense as well as the public's welfare. Silicon chemistry and fiber optics have enabled the nation's vast communications infrastructure, from computer networks and the Internet to the electrical grids and water supply in American cities. The products of chemistry are also key to how we live our lives – from enabling modern health care to improving the safety and performance of the products used to build our homes and cars, to providing plant nutrients to grow the crops that feed the world. Chemistry innovations also lead to drug innovations that eliminate a wide range of diseases and decrease time spent in hospital care.

2.1. History of Security and Risk Management

The chemicals sector has a clear understanding of its value and its impact on individual communities and the economy. The sector also possesses a sharp awareness of the risk factors and how to responsibly manage risk. Hundreds of thousands of highly trained chemists, engineers and operators are experts in the business of managing and reducing risks associated with making chemicals.

The chemicals sector's commitment to both safety and security is demonstrated through the sector's long-standing voluntary initiatives and programs; its adherence to and support for government standards and research; and its longstanding and effective partnerships with local, state and federal government agencies. Chemistry is a vital part of our military and public safety operations – from the disinfectants and antibiotics used to protect against biological warfare agents, to the bulletproof and flame-resistant fibers used to make helmets and flak jackets, to the microprocessors that give a

1 Sources for the Chemicals Sector Background section include information provided by the American Chemistry Council (ACC), Chemical Industry Data eXchange (CIDX) and The Fertilizer Institute (TFI).

technological intelligence edge to our security forces.

Risk encompasses the combination of vulnerability, threat and consequence. Information and communications infrastructures have become a critical part of chemicals sector operations. Communications technology and controlled sharing of business information are essential aspects of all company operations and processes in the sector. However, the same technologies that make business faster and more efficient can introduce new vulnerabilities. Now, as the world faces increased threats, the chemicals sector needs to increase its capability to manage exposure to information security risk. The industry will address the risk as a sector-wide initiative, in order to minimize the consequences to both public safety and the economy.

Mitigating information security risks will require a combination of leading edge technology, accepted sector practices and timely information sharing throughout the sector. The unified sector cooperation needed to address the current threat has many precedents in the chemicals sector, and the sector has a long history of addressing important issues proactively. The sector has demonstrated commitment to issues-management and the ability to respond quickly, in a sector-wide cooperative manner, to effectively address key issues – from Y2K to emergency response and standards for e-commerce transactions.

While the events of 9/11 redefined the scope of the threat, cyber-security was on the chemicals sector's radar screen long before 9/11. The chemicals sector is fortunate to draw upon established and proven programs that provide the groundwork for improving today's security processes and establishing better safety practices for tomorrow.

2.1.1. Responsible Care®

The Responsible Care initiative is an example of the chemicals sector's history of cooperation, and how sharing best practices can drive performance improvements across the chemicals sector. In its 14th year, the Responsible Care initiative is a comprehensive management system developed by experts for use throughout the chemicals sector to continuously improve safety performance and communications and to protect employees, communities and the environment. Members of sector associations, such as American Chemistry Council and the Synthetic Organic Chemical Manufacturers Association, along with other companies and associations involved in the sector's supply chain, participate in Responsible Care as partners. As a result, hundreds of companies are working together to further improve safety and performance throughout commerce and communities. Since the initiative was launched, America's chemistry companies have:

- Reduced emissions by 58 percent since 1988, while boosting production by 18 percent.
- Achieved safety performance 4.5 times safer than the average of all other U.S. manufacturing industries combined.
- Established about 300 Community Advisory Panels across the United States.
- Spread Responsible Care internationally to more than 46 countries, representing more than 85 percent of the world's chemical production.
- Established 80 partner companies and 30 partner associations that work to extend Responsible Care throughout the supply chain.

2.1.2. Be Aware and Be Secure Programs

Since the bombing in Oklahoma City in 1995, The Fertilizer Institute (TFI) and the Bureau of Alcohol, Tobacco and Firearms (ATF) have worked closely together to secure ammonium nitrate fertilizer and, from a TFI standpoint, all fertilizer materials. In 1996, TFI entered into a joint partnership with ATF to develop a public awareness campaign entitled "Be Aware for America." The industry-based voluntary program is designed to draw retailers, distributors, the public and law enforcement into a partnership aimed at heightening awareness and providing a network for reporting suspicious

activity relative to purchasing or using ammonium nitrate fertilizer. The National Research Council (NRC) assessed the program and recommended that it be expanded. In 2000, TFI and ATF began expanding the program to emphasize security measures in receiving, storage and transportation. In July 2001, a "Be Secure for America" campaign was launched to encourage manufacturers, distributors and retailers to take voluntary measures to ensure the security of ammonium nitrate. In addition to printed information, the program offers a 1-800 number that goes directly to ATF for reporting suspicious activity.

2.1.3. Chem eStandards™

In 2000, the sector identified a critical need to develop standards for XML-based e-commerce transactions and rapidly built consensus on what was required and how to approach the issue. Guided by the Chemical Industry Data eXchange (CIDX™), a collaborative global sector effort was launched to develop standards that were open, neutral and freely available. More than 60 companies and 130 sector subject matter experts worked cooperatively to develop Chem eStandards. The effort required strong participation from large and small companies in all segments of the sector, as well as service suppliers, software vendors and others. Chem eStandards are now well established within the chemicals sector and are being adopted by key trading industries. The CIDX organization also provides an ongoing forum for information sharing, leveraged learnings and future standards development.

2.1.4. TRANSCAER®

A major initiative sponsored by 10 trade associations, TRANSCAER (Transportation Community Awareness and Emergency Response) is designed to provide information directly to communities through which hazardous materials are transported. This program educates the community on the products that flow through the community, provides guidance and expertise on how to develop contingency plans in the unlikely event that an incident does occur, provides guidance on how to test the plan, and provides training to local emergency responders on how to deal with incidents and where to obtain information to assist in planning and preparedness.

2.1.5. CHEMTREC®

Since 1971, the American Chemistry Council has operated, as a public service, the 24-hour-a-day, seven-day-a-week emergency communication center known as CHEMTREC, which stands for Chemical Transportation Emergency Center. When a distribution emergency occurs, CHEMTREC provides emergency responders with technical assistance, such as product safety specialists, emergency response coordinators, toxicologists, physicians and other experts, to safely mitigate the incident. All calls are free of charge to emergency responders. CHEMTREC also has agreements in force with the U.S. Department of Transportation, the U.S. Army, and the Department of Defense to provide information and assistance to those organizations whenever and wherever it is needed.

2.1.6. Industry-Government Cooperation

The sector has a long history of working with the government to improve its knowledge and understanding of how chemicals interact with human health and the environment. The chemicals sector works closely with the Department of Defense, the Federal Bureau of Investigation, the Environmental Protection Agency, the Department of Transportation, the Federal Emergency Management Agency, the Department of Energy, the Coast Guard and many others, to bring the federal government's security expertise together with industry innovation.

2.2. Chemicals Sector Cyber-Security Information Sharing Forum

Given the chemicals sector's history as a performance industry, the sector has set and consistently delivered against self-imposed goals and standards. The chemicals sector has aligned itself through a strong family of cooperative trade associations around the world. These organizations enabled the sector to quickly deploy the proactive, collaborative approach taken on previous issues addressed by the sector. In this same spirit of cooperation, the sector has

aligned trade organizations representing more than 2,000 companies to address the issue of cyber-security through the Chemicals Sector Cyber-Security Information Sharing Forum.

To adequately represent the concerns and interests of the entire sector, the Forum consists of a number of trade associations and individual companies representing key industry segments within the sector. The Chemicals Sector Cyber-Security Information Sharing Forum is made up of senior-level company officials and/or staff representatives of these trade associations:

- American Chemistry Council
- The Chlorine Institute
- Compressed Gas Association
- Consumer Specialty Products Association
- CropLife America and Agricultural
- Dangerous Goods Advisory Council
- The Fertilizer Institute
- Institute of Makers of Explosives
- National Association of Chemical Distributors
- National Paint and Coatings Association
- Soap and Detergents Association
- Synthetic Organic Chemical Manufacturers Association

2.2.1. U.S. Chemicals Sector Cyber-Security Strategy Task Team

The recently formed Chemicals Sector Cyber-Security Information Sharing Forum chartered a task team to develop a sector cyber-security strategy. This group was comprised of 16 individuals representing information security, process control security, physical security, supply chain/logistics, information technology (IT) strategy development, industry collaborations, standards development, legal and telecommunications. This diverse group of subject matter experts from within the chemicals sector came together to draft the U.S. Chemicals Sector Cyber-Security Strategy.

3. Situation Analysis

Cyber-security, which encompasses both information and process control security, is an integral part of overall chemicals sector security. When evaluating the chemicals sector cyber-security landscape, it is critical to analyze the current and desired state of cyber-security as it applies to both information security and process control security. As process control systems become more powerful and integrated with engineering design and maintenance systems, information security becomes even more important to process control. In the past, information systems and process control systems within an organization were rarely integrated. While integration of these systems can be secure with proper controls, the trend toward increasing integration, automation and connectivity throughout the chemicals sector exposes the sector to the threat of unauthorized access to information, which could be used to facilitate or cause a physical attack or disaster from anywhere in the world.

The following assessment of the current and desired states of information systems security and process control systems security, and a careful analysis of the security trends and gaps that apply to each, provide the framework for the recommended sector cyber-security strategy. The following situation analysis is a generalized, rather than comprehensive, analysis of the characteristics of the sector as a whole.

3.1. Current State of Cyber-Security

Cyber-security is not a new issue for the chemicals sector, and many steps have been taken to protect our information and keep our operations safe. The sector has significant expertise on process safety and standards development and use – expertise that will be leveraged to address new cyber-security concerns.

3.1.1. Sector Practices and Standards

The chemicals sector has high recognition of the value of standards as an effective means of aligning business practices, reducing complexity and bringing overall industry performance to a base level of practice. Many industry standards for information security exist. However, broad agreement on which practices should be adopted on a sector-wide basis, or agreement and awareness of what type of information should be protected, has not yet been achieved. Many companies in the sector follow common practices in process control because safety of the process is the first and primary consideration in design. The varying degrees of automation, security practices and technological sophistication among sector participants introduces vulnerability into the supply chain. Risk levels vary based on the mix of chemicals manufactured or distributed, the associated hazard and the potential information security risks. More external value chain partners and contractors are gaining access to networking capabilities or sensitive information, and the scope of information systems is becoming more global. These factors increase our vulnerability to cyber-terrorism.

3.1.2. Technology and Process

Information technology plays a key role in the operations of both large and small chemical companies, from procurement to manufacturing, logistics, sales, customer service and accounting. Currently, the chemicals sector uses available technology-based tools to provide security safeguards for overall network operations, but most focus on protection from the Internet. Clearly the risks are broader than this. Moreover, security is not just a tool one buys; it depends upon the management policies, operating procedures and user behaviors within an organization. It also depends upon the incident response capabilities of individual companies.

Given the increasing connectivity both within and among companies, the long lifecycle of the sectors' computer systems, the increasing

connections between older and newer systems, and the sector's increasing use of commercial off-the-shelf technologies creates potential vulnerabilities at system gaps and interface points. In addition, current software industry practices condone the commercialization of application, infrastructure and security programs that have not been vigorously tested for cyber-security vulnerabilities or may contain new cyber-security vulnerabilities.

Some of the current practices in corporate offices and in process control require review, including password-protected screensavers and the lack of usernames and passwords on computers with limited physical access. Currently, these issues are addressed on a company-by-company basis**.** While some major chemical companies are reducing their vulnerability to cyber-attacks by adopting new network architecture designs with improved access controls, security is still the responsibility of the companies using the equipment, and individual users can potentially impact the effectiveness of security practices.

To date, no information sharing initiative across the sector has been established to address cyber-security intrusions. Concern about the risk of potential civil and criminal liability and the concern that information disclosed to the government would be accessible by inappropriate parties could be a barrier.

3.1.3. Verification

In the chemicals sector, verifying adherence to policy and standards is typically a joint responsibility of internal and/or external audit functions. Some organizations within the sector conduct assessments of their service providers and other third parties prior to connecting with internal environments, but this type of auditing is not practiced sector-wide. While there are no sector-wide standards or audits, several cross-industry standards organizations and industry groups are beginning to address certain aspects of cyber-security.

3.2. Cyber-Security Trends

Companies within the sector are dependent on leveraging information technology to remain competitive. With increased automation and external threats, the sector has continually increased its use of technology and improved practices to address security. Business and technology trends are driving changes in operations, technology and business practices, leading to an even higher degree of use and integration of information technology, which changes vulnerabilities and risks. Some of the trends affecting information systems and process control systems security include: business process re-engineering; competitive pressures; increased electronic trading and supply chain integration; increased outsourcing, alliances and joint ventures; increased use of commodity technologies; quickly evolving technology; and connectivity of multi-sites and global operations.

3.3. Desired State of Cyber-Security

The objective of sector cyber-security practices is to protect the confidentiality, integrity and availability of information and the safety and operational effectiveness of process control, as well as to prevent information from being used to compromise the physical security practices of companies in the chemicals sector. To be effective, these controls need to include not only technology, but also processes and people.

In the ideal state, cyber-security has the support of the executive management of individual companies, viewing its importance as commensurate with safety. Ideally, because of this support, these issues are addressed on an inter-company basis in the chemicals sector. Standard language and methodologies are used to protect the security of electronic interactions among companies. Close coordination is demonstrated among organizations within an enterprise, including information security, physical security, health and environmental services, purchasing and sales organizations.

3.3.1. Sector Practices and Standards

In the future state, chemicals sector members will proactively cooperate and collaborate via sector information sharing networks to drive voluntary practices and standards throughout the sector and verify that technology providers are meeting sector cyber-security needs. Voluntary practices and standards will exist for at least the following: automated product stewardship; expected security practices; information classification guidelines; improved awareness; identity management; risk management methodology; and incident response and management methodology.

In process control, security in the chemicals sector will include proper process control security design and management for safe, secure, integrated operations. The sector will have the tools, processes and methodologies to process and respond to increasing volumes of information for chemical facility operations in a more integrated enterprise.

Cyber-security enterprises will protect information and process control security by setting organizational security goals, establishing security policies and putting in place risk remediation processes to identify and implement needed corrective measures. Risk management will be based on the nature of the process and the materials used, and guided by firm safety and loss prevention principles.

3.3.2. Technology and Process

The sector's technology will have more secure interfaces and higher quality IT products. In the event of a cyber-attack, critical systems will be isolated from the rest of the network and still function. In addition to a company's information security perimeter, high-risk systems will be more compartmentalized according to sensitivity. The chemicals sector will have secure, open cyber-systems that are free from defects or vulnerabilities that can be exploited. Proactive collaboration between sector members and their information technology colleagues will help protect the security of information and process control systems, while meeting business needs for flexible, cost-effective process operations and for integration with other business supply chain processes. Seamless cooperation between the control engineering and information technology disciplines will be evident, and standard risk assessment methodologies will be available and used.

3.3.3. Verification

Standard process and technology-based tools are available to verify voluntary sector practices and standards by means of self-audit programs, certification and/or affordable third party audits. A standard certification process and self-assessment checklists are available and used to identify and correct vulnerabilities and mitigate risk.

3.4. Cyber-Security Gaps

Differences between the current state of the industry and the desired state represent specific gaps that must be addressed. Many of these gaps can be addressed by the chemicals sector, but others will need to be addressed through cooperation among all industries that use process control systems, including pulp and paper, food processing, power, oil and gas and other process industries.

3.4.1. Voluntary Sector Practices and Standards

While the sector has demonstrated its commitment to issues management and its ability to cooperate and respond quickly to effectively address key issues, the sector lacks agreement on voluntary standards and common practices for cyber-security. The industry needs to develop common security practices across the sector, including voluntary standard practices for, but not limited to, effective electronic customer qualification, benchmarking tools and a common risk management methodology.

3.4.2. Technology and Process

Current commercial offerings need improved security. However, technology providers have little incentive to upgrade the security performance of their offerings for the chemicals sector alone. Interdisciplinary, sector-wide cooperation is needed to address the current technology gaps to achieve improved security in the following key areas: open systems, software quality, identity authentication, remote access, network management, wireless communications, enterprise systems and access to process control systems.

3.4.3. Verification

As more companies become interconnected in the chemicals sector, there is a growing need for assurance that all sector trading partners, including extended supply chain partners, are following accepted voluntary practices and standards for cyber-security. Currently, the chemicals sector lacks certification processes and services for cyber-security, as well as self-assessment tools and a cost-effective methodology to qualify supply chain partners.

4. Recommended U.S. Chemicals Sector Cyber-Security Strategy

The global chemicals sector has a long history of proactively addressing issues of concern. Past collaborative efforts have demonstrated the chemicals sector's inclusive approach to building consensus, as well as its ability to bring leaders and subject matter experts together to understand issues, to develop the best strategic approach to address challenges and to raise the funding to staff and resource initiatives that benefit society, the environment and the economy. When approaching cyber-security, the chemicals sector will deploy the same proactive, collaborative approach that it has taken on previous issues.

The purpose of the U.S. Chemicals Sector Cyber-Security Strategy is to enhance cyber-security throughout the chemicals sector value chain to help protect people, property, products, processes, information and information systems. Although the scope of this strategy is focused on the U.S., the chemicals sector is global, and thus any recommendations need to be addressed within the context of the global nature of the chemicals sector.

The recommended program (Program) is based on an integrated set of elements that are intended to elevate the priority of security to that of safety for companies in the sector and encourage enterprise decision-makers to take the lead in developing or augmenting security policies and programs. To the extent permitted by applicable law, the chemicals sector will work together to augment information and process control security design and management to achieve continuous improvement in cyber-security performance broadly across the sector. The voluntary practices and standards developed will be commensurate with the level of risk, threats and vulnerabilities.

4.1. Guiding Principles

To be successful and fully meet the cyber-security needs of both large and small companies in all segments of the chemicals sector, the sector will use the following principles to guide its cyber-security program:

- Recognize that cyber-security is an integral part of overall security, and operate in a manner consistent with the principles and practices of the chemicals sector security programs such as the Responsible Care Security Code.
- Recognize the high degree of integration of the chemicals sector with other critical infrastructure sectors, as well as the global economy.
- Recognize that effective cyber-risk management starts at the top with the board of directors and active executive management direction.
- Develop principle- and process-based solutions that are appropriate for the diversity of membership and risk/consequence profiles within the chemicals sector.
- Consider both enterprise-specific and inter-enterprise cyber-security vulnerabilities.
- Address the U.S. national needs consistent with the needs and practices of the global chemicals sector.
- Leverage and augment cyber-security expertise within the sector, and leverage from other sectors.
- Maintain and evolve the Chemicals Sector Cyber-Security Strategy and Program to keep pace with change.
- Encourage inclusive participation from all qualified chemicals sector supply chain participants, including customers, carriers, suppliers, distributors, technology and service providers and contractors.

4.2. Strategic Intent

The sector will implement a Chemicals Sector Cyber-Security Program that focuses on cyber-security risk management and reduction to provide open but secure information and process control systems that help protect our community and enable collaborative business operations. The comprehensive cyber-security program will provide a means to improve the security of chemicals sector information and information infrastructure and allocate resources to effectively establish the following key program elements:

- Fostering involvement and commitment across the sector;
- Establishing a cyber-security public affairs program;
- Establishing voluntary sector practices and standards;
- Establishing an information sharing network; and
- Encouraging acceleration of improved security technology and solutions development.

4.3. Fostering Involvement and Commitment Across the Sector

Broad support and participation from all segments of the sector are critical for success of the proposed program. A Leadership Forum will be established to foster involvement and commitment across the sector, and will be open to all qualified sector participants. This forum will have responsibility for overall program implementation and sustainability. The Leadership Forum will sponsor and arrange funding for program development and promote adoption of the key elements of the chemicals sector cyber-security initiatives outlined in this strategy.

The objectives of the Leadership Forum will be to:

- Significantly raise awareness and understanding of cyber-security issues through education and communication programs across the sector and with our communities, shareholders and employees.
- Define the potential business, economic and social impacts, consequences and implications of potential cyber-security incidents.
- Promote executive management attention and governance to cyber-security.
- Generate commitment for the Chemicals Sector Cyber-Security Program.
- Gain endorsement, adoption and implementation support of trade associations and standards bodies.
- Establish a cyber-security public affairs program.

The Leadership Forum will leverage the network of existing trade associations, standards bodies and professional organizations to establish and implement the needed elements of the program.

To address development of voluntary sector practices and standards, and to encourage acceleration of improved technology and solutions development, a "Community of Interest" (see section 4.5.1.) will be established to leverage collective knowledge, shared technology and practices development among chemicals sector professionals, as well as with experts from other sectors, technology providers and other supply chain partners. Participation and support from existing information technology and process control standards bodies and professional organizations will be sought.

Similarly, the Leadership Forum will work with existing organizations and sector experts to develop and implement an information sharing network and provide leadership for a cyber-security public affairs program.

Building on this network of resources and the Community of Interest, the Leadership Forum will sponsor active awareness, education and training activities to foster broad understanding of the issues, potential implications and importance of proactively addressing cyber-security in the chemicals sector. Activities may include training, drills and guidance for qualified

sector participants, supply chain partners, contractors, and service and technology providers, to enhance cyber-security understanding and capabilities.

The existing Chemicals Sector Cyber-Security Information Sharing Forum could be transformed and leveraged to serve as the Leadership Forum.

4.4. Establishing Cyber-Security Public Affairs Program

Open information sharing is required to achieve the full benefits of the Chemicals Sector Cyber-Security Program. The Leadership Forum will provide opportunities for qualified sector participants to work together to advocate establishment of sector practices and policies that foster information sharing to mitigate cyber-security risks.

Government assistance may be sought to encourage public policies and regulations that foster necessary and appropriate sector interaction and information sharing to mitigate cyber-security risks and to favor tax credits for investment in cyber-security. Potential issues to be addressed may include:

- Relief from any restrictive antitrust laws that may prohibit or result in disincentives to industry cooperation.
- Mitigation from additional liability exposure.
- Exemption of certain types of shared information from discovery or access under the Freedom of Information Act.
- Resolution of tension between cyber-security and privacy.
- Economic incentives to drive cyber-security technology development and investments.

4.5. Establishing Voluntary Sector Practices and Standards

Qualified chemicals sector participants should be deliberate in establishing industry-wide, voluntary management practices, procedures, guidelines and standards to support the overall sector cyber-security expectations and to demonstrate the support and commitment of company management.

Although risks to business and information systems may vary across different segments of the sector, or even between different types of companies within a segment, a number of common principles, processes and practices can be used by all to identify and address the appropriate cyber-security approach for each specific situation. Voluntary sector practices and standards are needed to protect confidentiality, integrity and availability of information. To be successful, the voluntary sector practices and standards should be open, neutral and freely available.

Subject to appropriate legal requirements, the Leadership Forum will charter an organization to:

- Establish a Community of Interest to bring together cyber-security experts and other subject matter experts to guide sector practices and leverage expertise.
- Gather and assess available practices, from within the sector and leveraging knowledge and expertise from other sectors, standards bodies and professional organizations, to address chemicals sector vulnerabilities.
- Build, publish and maintain a knowledge base of potential vulnerabilities and possible known solutions.
- Recommend (and develop, if needed) voluntary sector practices and standards to address the needs of the chemicals sector.
- Establish a process for assessing needs for suggested performance levels, as well as appropriate processes and support for auditing and verification.
- Serve as the “voice of the industry” with technology providers and researchers to develop solutions that meet the chemicals sector’s requirements.

4.5.1. Community of Interest

The Cyber-Security Community of Interest will work together to assess the common and unique cyber-security vulnerabilities, threats and risks of the segments of the chemicals sector. The assessment will be conducted under the umbrella of the designated standards body established by the Leadership Forum.

The Community of Interest will provide a forum for companies to share cyber-security knowledge and experience. Companies will have the opportunity to discuss cyber-security issues with other chemicals sector professionals and experts from technology providers, supply chain partners and other sectors. Issues addressed will include:

- Ongoing identification and analysis of potential chemicals sector cyber-security vulnerabilities, risks and consequences.
- Identification, analysis and recommendations on options to address high priority risks and to mitigate consequences.
- Development and maintenance of a repository of available solutions for consideration by chemicals sector companies and their supply chain partners.

The organization will seek broad sector input, support and participation in the selection and/or development of voluntary practices, guidelines and standards, as well as the promotion and support of appropriate risk assessment methodologies and management practices to address sector needs.

4.5.2. Development of Voluntary Sector Practices, Guidelines and Standards

The designated standards body will lead the development and adoption of sector practices, guidelines and appropriate support materials and services for use in conjunction with the Program. Where appropriate, the organization may also recommend appropriate risk-based, voluntary standards of security and reliability performance for implementation across the sector.

Recommended voluntary sector practices and standards should be risk-based and address common issues of interest to all segments and qualified participants in the chemicals sector. Any methodologies and systems recommended must be affordable and scalable, so solutions can be effectively implemented by all companies. A portfolio of available services and options to support implementation should be identified and published in a reference guide.

Identification and selection of specific areas to address cannot be attempted until the appropriate standards body is operational. Based on the preliminary work in support of this strategy, areas that might be explored are:

- Methodologies for corporate cyber-security and reliability program development (see section 4.5.3).
- Methodologies for cyber-security risk assessment, which will be integrated with overall security risk assessment methodologies.
- Sector practices for specific cyber-security activities, including but not limited to: identity management practices; information classification methodologies; remote access; trading partner qualification; certification processes and tools; and performance metrics and scorecards.
- Recommended performance levels for specific cyber-security technology, including but not limited to: encryption; level of virus detection; and real-time monitoring and intrusion detection.

As part of the development process, the standards body will assess the spectrum of available options and focus on developing solutions only for those issues that are truly unique to the sector. The chemicals sector will seek to leverage existing practices, guidelines, materials and services available from other standards activities that meet chemicals sector's needs. In addition, the sector will participate in and/or lead the development of cross-industry initiatives to meet chemicals sector needs.

4.5.3. Recommended Corporate Cyber-Security Program

Consistent with overall security practices, one of the first issues that may be considered by the standards body to address is the development of recommended principles, methodology and support materials for establishing a standard Corporate Cyber-Security Program for all qualified sector participants. Although the systems, operations, vulnerabilities and risks of each company are different, all firms can use a common framework and process for establishing an appropriate program across the sector.

Industry professionals from all segments will work together to develop and recommend adoption of a risk-based program that meets both the common and unique needs of each segment and company type in the sector. This program would be integrated with the overall security program, and key elements of the recommended program could include:

- ***Management Support:*** Cyber-security should be recognized as a high priority issue within the corporate structure, to the extent that its advocacy and awareness are continual efforts and funding is appropriately regarded in business plans.

- ***Establishing Internal Policies and Voluntary Standards:*** Companies should be deliberate in developing written policies and procedures to support security expectations and to demonstrate management support and commitment. Policy and voluntary standards should be risk-driven and appropriate for the potential consequences.

- ***Risk Assessment and Management:*** Cyber-security risks should be routinely identified, analyzed and continually subjected to mitigation improvement using proven risk assessment methodologies. This risk assessment should be coordinated with physical security assessments. Information classification is another vital component to the risk management process.

- ***Identity Management:*** Companies should employ authentication technology commensurate with the risk of information exposure. Companies also should perform screening (i.e., background checks) for users with privileged access to critical resources.

- ***Security Monitoring and Measurement:*** Chemicals sector companies should develop and maintain measures of security effectiveness, including technology-based control and administrative controls.

- ***Security Awareness:*** The chemicals sector should prepare general-purpose guidelines for cyber-security awareness. All companies should provide the appropriate level of awareness, training and education for those who are authorized to use and maintain information resources.

- ***Security and Privacy:*** Chemicals sector companies must provide the appropriate measures to safeguard both company-sensitive and employee-sensitive information. Guidelines for classification of data should also be established.

- ***Data Storage and Transmission:*** Data available to the public and data transferred via public networks should be protected by a level of security commensurate with the information security risk. The chemicals sector should develop guidelines for identifying and protecting at-risk information.

- ***Application Software:*** Minimal security functionality requirements for information systems, developed or purchased, should be set forth in guidelines appropriate to the level of risk.

- ***Network Configuration Management:*** A company should exercise caution when creating connections between its internal networks and the Internet or other company networks. When inter-company connections are established, appropriate technology should be in place to protect the information assets of both entities and mitigate liability issues introduced by the connection.

- ***Change Management:*** Changes to network architecture and application systems should be subjected to a change management process to protect the stability and integrity of production environments.

- ***Incident Response and Business Continuity:*** Companies should have a documented and tested incident response plan that describes the action to be taken if a suspected or actual intrusion takes place. This plan should include both pre- and post-incident processes and business continuity plans.

- ***Audits:*** Companies should require both internal and external reviews of their security programs and processes, as well as self-assessment, to verify processes are being adhered to and to identify gaps that may have resulted from the introduction of new situations.

4.5.4. Possible Formation and Structure

CIDX, the robust standards body dedicated to standards for transacting business electronically, could potentially be leveraged as the designated standards body to address voluntary cyber-security practices and standards for the global chemicals sector. In the last year, CIDX has successfully led the development and widespread global adoption of Chem eStandards, XML-based standards for transacting business electronically between chemical companies and their trading partners. Current membership represents nearly 50 percent of domestic chemical sales in the U.S. and Europe.

CIDX is a 501 (c) 3 corporation, established in 1985, with duly developed by-laws, policies and management structure. Membership is open to all qualified companies with an interest in the chemicals sector, including chemical companies from any segment, supply chain partners, service providers and technology providers.

4.6. Establishing an Information Sharing Network

The chemicals sector will establish a formal Cyber-Security Information Sharing Network (Network) to distribute advance warnings of cyber-security threats, vulnerabilities and incidents. The goal of the warning system is to identify and reduce infrastructure vulnerabilities and to guard against cyber-attacks or speed recovery from incidents.

Initially, the Information Sharing Network will focus on:

- Providing alternative secured communication capabilities in times of emergency.
- Cost-effective dissemination of information gathered from monitoring services, government and other sources concerning threats against information and physical systems.
- Providing access to third-party databases of resolutions and solutions to specific incidents.

With appropriate resolution of the public affairs issues related to sharing proprietary information, the sector will explore expanding the Information Sharing Network to provide a secure facility for anonymous and confidential sharing of information associated with incidents, threats and vulnerabilities, as well as resolutions and solutions. The expanded capabilities of the Information Sharing Network could also include providing the reported information to the government for integration and analysis with information from other sectors, and disseminating the resulting analysis and alerts from the government to the chemicals sector.

Ultimately, the Network's primary objectives would be to:

- Provide a secure facility that enables both authenticated and, where appropriate, anonymous and confidential input and sharing of information associated with incidents, threats, vulnerabilities, resolutions and solutions.
- Permit members to voluntarily share information about incidents, threats, vulnerabilities, resolutions and solutions occurring within their environments. Submitting this kind of information will enable the Network to determine if the information is potentially relevant in the context of larger events occurring across the sector.
- Disseminate early warnings and alerts concerning threats against information and physical systems in the chemicals sector and relevant segments of the related supply chain.
- Provide a database of resolutions and solutions to specific incidents and make the database available to members of the Network.
- Provide analysis of incidents and sector applicability to members of the Network.

4.6.1. Possible Formation and Structure

CHEMTREC, the HAZMAT emergency response center operated by the American Chemistry Council, could potentially be leveraged to establish and operate the proposed Information Sharing Network. The Network could be operated by the American Chemistry Council on a contracted service basis, with membership open to all qualified chemicals sector participants.

The Network facilities will be physically secured. The various components of the Network's systems will be protected through state-of-the-art security techniques, including constant monitoring for unauthorized attempts to access, alter or disrupt systems.

4.6.2. Participation

Given the broad integration of the chemicals sector with other industries, and the systemic nature of cyber-security risks across the supply chain, participation in designated portions of Network services will be available to all qualified chemicals sector supply chain participants and government representatives. However, to provide a confidential venue for sharing sensitive and proprietary information, and to avoid creating new threats or vulnerabilities due to sharing sensitive information, certain portions of the Network's services may be limited to designated and pre-qualified representatives from chemicals sector companies only.

4.6.3. Information Sources

The Network will work collaboratively with a variety of global information sources and services to provide the broadest range of threat, vulnerability and incident data involving information hardware and software products, process control systems and physical security. Sources could include:

- Member companies: cyber-security professionals from member companies will be able to voluntarily report information on security threats, vulnerabilities, incidents and solutions (on an anonymous or attributed basis).
- Industry expert groups and forums will assess industry-specific needs and develop voluntary sector practices and standards (through a designated standards body).
- Technology vendors (e.g., Microsoft, IBM and AspenTech).
- Security associations (e.g., CERT and SANS).
- Internet sources (e.g., bulletin boards and news groups).
- Information sharing networks in other industries.
- State, national and foreign government and law enforcement agencies (e.g., InfraGard).

Information from the above sources will be assessed for applicability and for identification of potential solutions. Based upon agreed severity classifications, the Network will distribute an alert to members accordingly.

4.7. Encouraging Acceleration of Improved Security Technology and Solutions Development

Sector participants will proactively work with information technology product and service providers, government and academia to accelerate development and implementation of improved technologies and methodologies to cost-effectively address defined vulnerabilities. Subject matter experts will lead this activity in a structured process.

The sector, under the leadership of the Community of Interest, will develop close partnerships with suppliers to provide input and direction on product development. By working together with technology partners, the sector can help influence changes in technologies to better meet business needs for safe, secure and integrated operations.

This collaborative initiative will seek out and partner with other process industries with similar needs, as well as with government and academia, to sponsor research and technology development to continuously improve cyber-security capabilities.

Examples of issues to potentially consider may include:

- Models to assess the potential consequences of potential threats and vulnerabilities to the chemicals sector.
- Real-time detection of intrusions to process control systems.
- Intelligence and security risk and vulnerability assessments.
- Finding the right balance between security and cost-effective commodity technology.
- Vendor and third party certification.
- Risk assessment methodologies.
- Standard security software that operates across different technology platforms.

4.8. Program Summary

To the extent permitted by applicable law, the chemicals sector will work collaboratively across the supply chain to drive the development of improved voluntary sector standards, products and practices for protecting critical information, information systems and process control systems. Using a blend of technology, processes and people, chemicals sector companies will implement practices to protect proprietary information resources from unauthorized access or disruption and to facilitate the safe and secure operation of sector facilities. The sector needs a high-level, risk-based approach to proactively manage the industry's information assets and process control systems. This will require increased activity within selected standards setting bodies, as well as working in close partnership with IT suppliers to give direction on product development.

Appendix A: Glossary

1. ACC (American Chemical Council): A Chemicals Industry trade organization that owns the Responsible Care® code of product stewardship.
2. Chem eStandards™: Standards that specify how server-to-server, electronic business is conducted within the chemicals sector. These standards specify transactions in XML document format and how these documents are exchanged securely between companies.
3. CIDX (Chemical Industry Data Exchange): A chemicals sector trade organization that owns the Chem eStandards™.
4. Identity/Authentication: User authentication denotes a security procedure where an individual's identity is verified. The process ensures that the individual is who he or she claims to be, but does not affect the individual's access rights. User names and passwords are identity and authentication techniques.
5. Incidents: Security breaches or unexpected events that clearly go beyond daily norms, appear to have broader consequences, correlate to incidents reported by others, or correlate to specific threat information received.
6. Incident Response: An organization's planned and systematic reaction to an actual or perceived event that has adverse effects on a company's cyber-assets or real assets.
7. Information Security: Protection of information assets from breaches and misuse of information confidentiality, availability and integrity.
8. Malicious Code: See Virus Protection.
9. Monitoring and Intrusion Detection: Intrusion detection systems (IDS) monitor network system files and logins to locate intruders who attempt to break into or misuse a computer system.
10. Risk Analysis[i]: The process of analyzing a target environment and the relationships of its risk-related attributes. The analysis should identify threat vulnerabilities, associate these vulnerabilities with affected assets, identify the potential for and nature of an undesirable result, and identify and evaluate risk-reducing countermeasures.
11. Risk Assessment: The assignment of value to assets, threat frequency (annualized), consequences (i.e., exposure factors) and other elements of chance. The reported results of risk analysis can be said to provide an assessment or measurement of risk, regardless of the degree to which quantitative techniques are applied.
12. Risk Management: The overall process of risk assessment, prioritizing, budgeting, implementing and maintaining risk-reducing measures.
13. Supply Chain: Those companies directly involved in the production of goods, from raw materials through intermediate products and final use. The supply chain extends beyond the chemicals sector and includes raw material producers and manufactures of products that include chemical products. The supply chain typically includes transportation, distribution, and utility companies, but does not include producers of chemical equipment or providers of administrative services.
14. Standard: A standard is something established by authority, custom, or general consent as a model or example.[ii] For the purposes of the U.S. Chemicals Sector Cyber-Security Strategy, a standard is considered a voluntary practice or guideline that is established by consensus of the industry.
15. Threat: An event, the occurrence of which can have an undesirable impact
16. Value Chain: All those involved in the production and distribution of chemical products, including the supply chain, chemical equipment producers and administrative services (such as banks and insurance companies) through end-use consumers.
17. Virus: A virus is a program or piece of code loaded into a computer against the user's wishes or without the user's knowledge. It can use up all system memory, wipe out data and bring systems to a halt. Viruses can also transmit across networks and bypass some security systems.
18. Vulnerability: The absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact or both.

---

[i] Risk Management Terminology (Handbook of Information Security Management 1999; p. 430; ISBN 0-8493-9974-2)
[ii] Merriam-Webster Collegiate Dictionary