Written Statement
On behalf of
The Dow Corning Corporation and
The American Chemistry Council

Presented by

Mark W. Gandy, CISSP

Global Manager - IT Security and Information Asset Management

Dow Corning Corporation, Midland, MI 48686

Before the
United States Senate Committee on
Homeland Security and Governmental Affairs

Oversight Hearing on Nov. 17, 2010

“Securing Critical Infrastructure in the Age of Stuxnet.”

Introduction

The American Chemistry Council (ACC) represents the leading chemical companies in the United States who produce the essential products critical to everyday life. The business of chemistry is a critical aspect of our nation's economy; employing nearly 803,000 Americans and producing more than 19 percent of the world's chemical products. In fact, more than 96% of all manufactured goods are directly touched by the business of chemistry. ACC members provide the chemistry used to produce lifesaving medications and medical devices; the body armor used by our men and women in the military and law enforcement; the light weight components for vehicles that help improve gas mileage; the energy saving building insulation and windows; silicon for solar panels and the durable, light weight wind turbine blades that help provide green energy.

Cyber Security is a Top Priority for ACC and the Chemical Sector

Because of our critical role in the economy and our responsibility to our communities, security continues to be a top priority for ACC members. Along with physical security, ACC members began actively addressing cyber security issues before and after the attacks of September 11, 2001.

In 2001, our members voluntarily adopted an aggressive security program that became the Responsible Care® Security Code (RCSC). Responsible Care implementation is mandatory for all members of the ACC. The RCSC is a comprehensive security management program that addresses both physical and cyber security and requires a comprehensive assessment of security vulnerabilities and risks and to implement protective measures across a company's value chain. A company's security plan is reviewed by an independent, credentialed third-party auditor. The RCSC has been a model for state-level chemical security regulatory programs in New Jersey, New York and Maryland and was deemed equivalent to the U. S. Coast Guard's Maritime Transportation Security Act (MTSA).

Since RCSC's inception, ACC members have invested more than $8 billion in security enhancements including both physical and cyber security protections. Security in all its dimensions continues to be a top priority for ACC and the chemical industry, and our record of accomplishment and cooperation with Congress, DHS and others is undisputed.

In June 2002 ACC members began implementation of the Chemical Sector Cyber Security Strategy, which was referenced by the Bush Administration's National Strategy to Secure Cyberspace of 2003. ACC was gratified that in 2009 the Obama Administration made cyber security a top priority. ACC participated in the White House 60-Day Cyber Policy Review and our cyber experts work closely with the DHS National Cyber Security Division (NCSD) in many areas including: national Cyber Storm exercises, information sharing programs, development of the "Roadmap to Secure Control Systems in the Chemical Sector." A 2009 Program Update can be found on the Obama Administration's website - "Making Strides to Improve Cyber Security in the Chemical Sector."

Public/Private Partnerships are Essential to Securing Cyber Systems in the Chemical Sector

The Chemical Sector continues to work with and align its priorities with those of the Department of Homeland Security (DHS) in order to advance the cyber security agendas of both organizations. The National Cyber Security Division (NCSD) of DHS is the government agency with primary responsibility for working with public, private and international entities to secure cyberspace and America's critical cyber assets. Over the last several years, the chemical sector has closely aligned its efforts with NCSD initiatives and plans to continue to provide sector representation in the following NCSD venues and others that may be created in the future. Examples of this alignment include:

- Cross-Sector Cyber Security Working Group (CSCSWG)

- Industrial Control Systems Joint Working Group (ICSJWG)
- National Security Exercises

In addition, the chemical sector works closely with other DHS divisions that focus on facility and transportation security issues to ensure that cyber security components of their work are appropriately addressed. These divisions include:

- Infrastructure Security Compliance Division (ISCD)
- Chemical Sector-Specific Agency (SSA)
- Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

Chemical Facilities Anti-terrorism Standards (CFATS)

On April 9, 2007 the U. S. Department of Homeland Security promulgated the "Chemical Facilities Anti-Terrorism Standards" (CFATS) regulatory program. This comprehensive Federal program requires high-risk chemical facilities to register with DHS, conduct a thorough site security assessment and implement protective measures that comply with 18 risk based performance standards (RBPS). In particular, RBPS #8 addresses performance for cyber security, requiring high-risk facilities to develop the capability to effectively deter and prevent cyber sabotage, including unauthorized on-site or remote access to critical process controls. RBPS #8 identifies the following policies and practices to effectively secure cyber systems from attack or manipulation: security policy, access control, personnel security, awareness and training, monitoring and incident response, disaster recovery and business continuity, system development and acquisition, configuration management, and audits.

Additionally, CFATS requires enhanced security measures for critical cyber systems that monitor and/or control physical processes that contain a chemical of interest (COI) or that include critical business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a COI.

In early 2010, DHS began inspecting covered high risk chemical facilities starting with Tier 1 sites that pose the highest risk.

Development of International Standards

Sustained and long-term improvements in the security of industrial control systems will only be achieved through the definition and application of well-defined and accepted international standards. Our sector is leading in the development of comprehensive international standards by the International Society for Automation (ISA), an organization that brings together owner-operators, technology providers, researchers and a several other constituencies.

Several of these standards have been published and accepted by the International Electrotechnical Commission (IEC), and several more are under active development. These standards are by design applicable to all sectors that employ industrial control systems.

The Roadmap to Secure Control Systems in the Chemical Sector

Published in September 2009, the "Roadmap" was developed in partnership with the Department of Homeland Security and the chemical sector. It provides a template for action as industry and government work together to achieve a common goal of securing industrial control systems in the chemical sector by establishing specific goals and objectives and milestones over a 10 year journey. In the desired state, all U.S. chemical sector companies will be actively working to achieve common cyber security goals. Additionally, using the latest practices and guidance will be an inherent part of company cyber security programs to help ensure proper controls are in place to protect

company systems and information. Finally, the sector will have solid working relationships with strategic technology providers and government agencies. Key elements of the Roadmap include:

1. **Information sharing**

Information sharing will be seamless within the chemical industry, between the chemical sector and government agencies including the Department of Homeland Security (DHS) and among critical infrastructure sectors at a strategic, tactical and operational level. United States cyber security activities will be coordinated with global efforts to enhance chemical sector performance worldwide. Chemical companies will be comfortable sharing appropriate yet security-sensitive information with DHS and industry counterparts.

2. **Guidance enhancement and relevance**

Chemical companies have access to new and improved practices, resources and standards created by external organizations and/or the Chemical Sector Cyber Security Program to help them address maturing cyber security needs and legislative requirements. Chemical Sector Cyber Security guidance documents will remain evergreen through periodic reviews and will be available to assist chemical companies in enhancing their cyber security preparedness and performance as well as compliance with the CFATS regulations.

3. **Sector-wide adoption**

Cyber security is recognized as a critical aspect of overall security and is addressed in coordination with physical and transportation security within the chemical industry. The increased emphasis on cyber security will lead all chemical trade associations to incorporate cyber security practices as a condition of membership within existing product stewardship programs or security programs. Additionally, the sector's activity will be managed through one consistent, coordinated program.

4. **Enhanced security in technology solutions**

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. Information technology suppliers will design their solutions to maintain highly-available systems, support future versions of these long-lived assets and meet governmental compliance standards. They will also make a more formal commitment to product reliability, integrity and security, thus more fully embracing the philosophy of secure by design.

Cyber Storm III and National Exercises

In September of 2010, DHS held its third National Exercise focused specifically on Cyber Security. Since its inception ACC and the Chemical Sector was actively involved in its planning, preparation and execution. Cyber Storm III participants included Federal, State and local governments; private sector companies; and International partners. In addition to the chemical sector, significant emphasis was also placed on the IT, Tele-communication, Electric and Transportation sectors.
The Chemical Sector objectives through Cyberstorm III were focused on testing its ability to effectively activate the ACC Cyber Incident Response Plan (CIRP). The CIRP was developed to effectively mobilize the chemical sector in responding to a significant cyber security event having national and regional impacts to economy and to public safety.

Overall Cyber Storm III Exercise Objectives were:

1. Exercise the National Cyber Incident Response Plan (NCIRP)
2. Examine the role of the DHS in a global cyber event
3. Focus on information sharing issues (requirements, classified/tear-line, etc, information condition/alert levels, thresholds, response roles & responsibilities, authorities)

4. Examine coordination and decision-making procedures/mechanisms across the constituency (Federal, state, private sector, international)
5. Practically apply findings from past exercises

National level exercises are crucial to testing the capability of the chemical sector to respond effectively in the event of a national emergency and to identify gaps and areas for improvement. ACC will be working to address the learnings from Cyber Storm III to ensure that our industry continues to take the appropriate steps to enhance our preparedness of cyber incidents.

Conclusion

The above activities and programs demonstrate the chemical sector commitment to the advancement of cyber security in the critical infrastructure. This commitment has been consistent and sustained for almost a decade and has led to the creation of very effective working partnerships within our sector, across sectors, and with the government.