The Dow Chemical Company

statement for the record

of

David E. Kepler

Chief Sustainability Officer, Chief Information Officer, Business Services and Executive Vice President

before

The Senate Committee on Commerce, Science, and Transportation and the Senate Committee on Homeland Security and Government Affairs

"The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting our National and Economic Security"

March 7, 2013

The Dow Chemical Company

Statement for the Record

The Dow Chemical Company appreciates the opportunity to submit these written comments to the Senate Committee on Commerce, Science, and Transportation and the Senate Committee on Homeland Security and Government Affairs. We applaud the Committee for holding a hearing on cyber security and the necessary collaboration between government and the private sector.

About Dow

Dow was founded in Michigan in 1897 and is one of the world's leading manufacturers of chemicals, plastics and advanced materials. Dow combines the power of science and technology to passionately innovate what is essential to human progress. Dow connects chemistry and innovation with the principles of sustainability to help address many of the world's most challenging problems such as the need for clean water, renewable energy generation and conservation, and increasing agricultural productivity. Dow's diversified industry-leading portfolio of specialty chemical, advanced materials, agrosciences and plastics businesses delivers a broad range of technology-based products and solutions to customers in approximately 160 countries and in high growth sectors such as electronics, water, energy, coatings and agriculture. More information about Dow can be found at www.dow.com.

Cyber Security: A Manufacturing Company's Perspective

Cyber threat activity across the business community and the government has continued to increase over the last decade. The main driver of this change is in the profile of the threat itself which has matured from random acts primarily by individuals to now include well resourced organizations outside the United States. These new threats are targeted in areas that range from commercial espionage to terrorism to activism. Companies have a vested interest – along with a duty to their stockholders, employees and communities – to protect and defend their facilities, processes and intellectual property against these cyber intrusions.

The Dow Chemical Company and many other chemical companies have made significant investments in all of these areas to address cyber threats. After 9/11 for example, the American Chemistry Council (ACC), as part of its Responsible Care® approach, devised the Responsible Care Security Code which requires companies to adhere to the chemical industry best practices for security, both physical and cyber. Dow has invested heavily in, and is constantly upgrading, the physical and information defensive protection systems guarding our Company. However, industry must rely on the federal government to approach cyber security, working in partnership with other countries, to deploy an offensive perspective by preempting attacks when possible and through the pursuit and prosecution of the criminals behind these threats.

The management systems rely on information and knowledge, and there is a need for identifying better approaches to work with government in improving information sharing. Increased focus on real time and efficient information sharing programs should be improved to foster, incentivize and increase the sharing of threat activity.

Dow believes that protection of the country's critical infrastructure can be addressed most effectively by moving forward with legislation which strengthens the collaboration between the federal government and the private sector. The key principles of this collaboration are:

- Timely information sharing between government and industry and among industry peers.
- Reasonable protection for companies sharing threat or attack information with the government and their industry peers.
- Aggressive pursuit and prosecution of cyber criminals.

IT and telecommunication suppliers must continue to improve the security of their products and services and be unified in providing services that their customers can rely on for threat response.

Dow does not support prescriptive regulatory legislation on specific technologies or methods. Legislation that sets up a system requiring significant resources to simply comply with a regulatory scheme diverts resources from addressing the threats and risks in need of mitigation. Issues surrounding cyber security are in constant flux and proper management requires a fluid and fast response. Complex regulatory schemes will only slow the advancement of cyber risk management systems.

Background

The internet has become critical to the operations of business, government and global commerce. It is an open and dynamic venue for the exchange and collection of ideas and information. For the United States it has been a key enabler for maintaining the country's competitiveness. Some elements inside and outside the country, however, have seized on this open framework and have found innovative ways to use it for illegal financial gains, victimization of the innocent and to advance ambitions that are not in the interest of the United States. Today, companies regularly have to manage major information security issues, including: corporate espionage, intellectual property theft and malicious activism. Companies also must be prepared to manage and mitigate risks such as acts of terrorism or sabotage that could have severe physical and/or financial consequences. The Dow Chemical Company, like many large corporations, is regularly attack from sources that are advanced, persistent and targeting our intellectual property. In many cases, the highly sophisticated attackers are based in foreign countries.

Efforts to develop a public-private partnership to protect against cyber-attacks has a long history. In 2003, one of the key objectives of the National Strategy to Secure Cyberspace was to provide a framework for public and private partnership including the sharing of information. Much progress has been made, but today's cyber-attacks are much more advanced and it is clear that more ongoing progress is needed to ensure the continued prevention of a severe systemic failure of public or private critical infrastructure. It will require a more responsive, integrated, and resilient national system to prepare for and respond to these threats.

Chemical Industry Cyber Security Leadership

Large companies such as Dow are seeing an increase in the risks we face. The internet, including the growth of social media, has elevated our exposure to threat actors such as hacktivists (hackers with a targeted malicious intent to vandalize or stop business as their protest method) and nation states sponsoring industrial espionage or cyber criminals. As society and industry move toward increased mobility and pervasiveness of

information technology, the frequency and cost of cyber-incidents will continue to increase. These risks require a joint public and private effort to be managed effectively.

In 2001, Dow and other American Chemistry Council (ACC) members voluntarily adopted the Responsible Care® Security Code (RCSC). The RCSC is a comprehensive security management program that addresses both physical and cyber security. It requires a comprehensive assessment of security vulnerabilities and risks to implement protective measures across a company's value chain.
Since RCSC's inception, ACC members have invested more than $11 billion in security enhancements including both physical and cyber security protections. Security, in all its dimensions, continues to be a top priority for Dow and the chemical industry. Our record of accomplishment and cooperation with Congress, DHS and others is undisputed.

Dow has led in several business and public forums which focus on advancing cyber security within the chemical sector. Dow regularly provides leadership or participates with the following organizations:

- **ChemITC**
  - Chemical Information Technology Center (ChemITC®) of the American Chemistry Council (ACC) is a forum for companies in and associated with the ACC to address common IT issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC® is committed to advancing the cyber security of its member organizations.
- **Chemical Sector Coordinating Council (CSCC)**
  - Pursuant to the Homeland Security Act of 2002, the purpose of the CSCC is to facilitate effective coordination between federal infrastructure protection programs, the infrastructure protection activities of the private sector and those of state, local, territorial and tribal governments.
- **National Infrastructure Advisory Council (NIAC)**
  - The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructures, both physical and cyber, supporting sectors of the economy.
- **International Society for Automation (ISA)**
  - ISA has primary responsibility for the development of the ISA-62443 series of standards addressing cyber security for industrial automation and control systems (IACS). As each standard is developed it is submitted simultaneously to ANSI and IEC as a U.S national and international standard, respectively.

Cyber Security Management at the Dow Chemical Company

Dow has a comprehensive set of policies, standards and procedures based on guidance from organizations such as the National Institute of Standards and Technology (NIST) and established industry standards such as ISO 27001 and the ISA/IEC 62443 series for industrial automation. Due to the very fluid nature of cyber threats, Dow is continuously refreshing its practices and technology based on its experience as well as the best available information from the government, industry and other public sources. We frequently benchmark with peer Chemical Sector and broader Manufacturing Sector companies as well as other industries to manage the risk of a cyber-attack. We also enlist external private entities to evaluate our security posture.

Dow's information security is based on a multi-layer defense strategy. This includes continuing to enhance our IT infrastructure to meet the standards of other companies with high-value security profiles as well as

elevating the protection for the Company's most sensitive intellectual and physical assets. Dow uses a risk-based approach for the implementation of these controls. Developing strong partnerships between Dow's Information Security group and all Dow business units is vital to managing the flow of sensitive information and protecting critical infrastructure.

Strong collaboration with security vendors and partnerships with government agencies have been essential in preventing, detecting and responding to threats. We work closely with the chemical sector liaisons from the Department of Homeland Security and in forums such as the Industrial Control Systems Joint Working Group (ICSJWG). Working with government agencies has been valuable due to their collaborative nature. Dow believes that a public-private sector collaborative approach to cyber security is the best way to achieve common security goals for individual companies as well as the country. Using a risk-based approach that leverages the existing work of the international cyber security community will facilitate implementation of practices that are both effective and flexible.

Dow's multi-layer defense strategy begins with employees. Our ongoing security awareness programs help employees understand the ever-changing threats in the cyber landscape. People are the new perimeter – our greatest defense, and if not informed and educated, could be our weakest link. We have an ongoing global awareness campaign to:

1) Educate users on policies and the risks we face;
2) Drive commitment to the security program by making security initiatives a personal responsibility;

We continue to evaluate and improve the technical and non-technical response capabilities related to cyber threat incidents and we have made significant investments in state-of-the-art technologies to detect anomalous cyber activity which is the predecessor to most cyber-attacks. Dow has defined threat response processes to handle these issues when detected and has established a core team of highly skilled employees to coordinate response and proactively mitigate risk to the Company's systems. In order to maintain a highly secure environment, Dow has a team of security professionals who regularly leverage and collaborate with security vendors and government resources to implement and improve security controls.

Private Sector Needs from Congress and the Administration

Dow believes that protection of the country's critical infrastructure can be addressed most effectively by moving forward with legislation which strengthens the collaboration between the public and the private sectors. This collaboration must recognize the benefits of a risk based and performance based approach, its relationship to physical security, two-way information sharing, prosecution of cyber criminals and protection from liability. This should be done in a way that does not impact the relationships developed over the last decade.

Effective two-way cyber security information sharing between the public and private sectors must be timely, specific and actionable, and protected from public disclosure. A public/private partnership will vastly improve the flow of information and ideas to quickly identify threats and vulnerabilities. To help promote the flow of information, information voluntarily provided by the private sector should be adequately protected from public disclosure. The unintended consequences of Freedom of Information Act requests must be addressed.

Liability protection for the private sector as a result of a cyber-attack must also be provided as long as appropriate management systems have been applied to address potential threats. This will help promote participation amid the more rapid penetration of emerging technologies. The liability protections afforded under the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 are appropriate to consider.

Companies such as Dow are in a defensive mode when it comes to cybercrime. There must be better enforcement of U. S. laws against cybercrime with more aggressive prosecution of cyber criminals in an attempt to deter the act. U. S. laws should be updated and strengthened to protect critical infrastructure from cyber-attacks and hold those accountable for perpetrating intentional acts designed to cause harm to critical infrastructure operating systems or for stealing intellectual property and personal information for financial gain. Additionally, the U. S. federal government should develop strong international partnerships that work together to identify international threats. Without a focused strategy to address the borderless nature of cybercrime, the private sector will continue to fight an uphill battle.

Dow believes the federal government has a role in setting an example, by ensuring higher quality security-embedded solutions and services by technology suppliers are built into their systems. 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, to understand their vulnerability before releasing items into the marketplace. Information technology suppliers and software developers must design for critical infrastructure high-availability and long-lived assets in accordance with rigorous compliance standards. The IT industry is in the best position to enhance security controls. If they do not, it passes an additional burden downstream, and duplicates effort and costs onto the customers in regulated industries. Just as the chemical sector adopted the Responsible Care model, the IT and telecommunication industries must be encouraged by their customer based to create self-regulated security practices and services.

Legislation

Dow advocates for legislation that codifies the principles outlined above. In summary, legislation that facilitates information sharing between industry and government and among industry peers is needed. Ideal information sharing legislation offers liability protections for early sharing threat or attack information with the government and provides antitrust relief to share with industry peers. Information should include strategic assessments, best practices, and lessons learned from events and incidents. Cyber criminals and nation state actors must not be allowed to continue to operate with relative impunity. They must believe that there are consequences for their actions. Finally, the IT and Telecommunications industries must create products which are inherently more secure.

Dow does not support prescriptive regulatory legislation on specific technologies or methods. Legislation that sets up a system requiring significant resources to simply comply with a regulatory scheme diverts resources from addressing the threats and risks in need of mitigation. Cyber security is a constantly changing portfolio and proper management requires a fluid and fast response. Complex regulatory schemes will only slow cyber risk management systems.

Executive Order on Improving Critical Infrastructure Cyber Security

Dow supports the information sharing initiatives included in the recent executive order. However, Dow is concerned with the proposed approach of a voluntary program for critical infrastructure industries to adopt cyber security standards. Voluntary programs, normally, allow industry to develop their own standards that are risk and performance based that consider the specific sector environment, and are followed by a certification system to ensure compliance. Responsible Care Security code, for one, is a successful example for the Chemical sector.

Government defined or selected standards can miss the specific challenges that are required to be addressed by each industry sector. It is initiated as a voluntary program, but it could develop in such a way that companies will be forced to adopt prescriptive standards due to the fact that information on program adoption for "high risk" industries may be made public. More concerning this could be done without a review process and could be used to leverage in ways that may not be beneficial to lowering overall risk. The president or Congress should not allow pseudo- regulations without legislation to occur.

Dow will actively participate in industry forums like ACC, Chamber of Commerce, the Business Roundtable and all government initiatives to fully support successful implementation of any cyber security efforts which better protect our communities and Industries