

Recently Melissa Hathaway, DNI Cyber Coordination Executive, Office of the Director of National Intelligence, posed the following 4 questions, as a request for input during the 60-day Cyber Security Review for the White House. These comments are offered from the chemical sector ...

**1. What should be the federal government's role in protecting critical infrastructure from cyber attacks from nation-state/non-nation-state actors?**

Many chemical companies are global businesses operating in several countries and potential threats that they face, especially from nation-state or non nation-state actors, could either enter or be targeted at company resources outside of the U.S. The risk of cyber security incidents to public and private enterprises has potential impact to personal safety, physical structures and financial resources and as such, companies evaluate several important factors as they determine their approach to addressing cyber risk (e.g., probability of risk; potential consequences of risk; availability of proven and effective safeguards; available time and resources for responding; locations where risk could be presented; etc.) Consideration should be given to the fact that in terms of addressing risk one size does not fit all, and because many companies operate in an inter-connected world where a cyber security attack in one country could cause impacts in other locations, a company has to recognize the importance of a global approach to cyber security protection. The government should continue to pursue appropriate international legislation that calls for punishing cyber criminals who attack the U.S. critical infrastructure sectors regardless of where the cyber attack originates.

The government can play a role in mandating a minimal cyber security posture that all companies need to adhere to if any assets within the US could be accessed. This could take the form of ensuring all ingress and egress network points to the outside world are secured (and verified at least once a year) and good 'defense in depth' policies are followed.

Most chemical companies have internal incident management processes that have defined escalation paths for engaging corporate -level management as appropriate. Most companies will enlist law enforcement and/or government assistance when an obvious criminal attack has been made against the organization, or when it is not possible for the company to resolve the incident on its own. The government should maintain a position of intelligence gathering and communication coordination. Critical infrastructures need to know when to take action to prevent, deter or mitigate specific cyber attacks. One of the most important roles the government can serve is to specify who in the government is in command during a wide-impact incident of national significance, and how the information will be disseminated to the critical infrastructure sectors.

Some consideration should be given to establishing an alert/warning/communication system that provides more security safeguards than the internet-based approaches in use across the critical infrastructure sectors today.

**2. What are the thresholds at which businesses/organizations report cyber security incidents to government entities like US-CERT (ostensibly beyond what's legally mandated, such as state laws on reporting data breaches)?**

In the chemical sector, most likely a company will not report a cyber incident to US-CERT, unless it is beyond the company's ability to resolve on its own. The crisis communication process currently being implemented in the chemical sector is designed to enable chemical companies to discuss an incident within the sector to determine the sector impact, before reporting it to the government as appropriate. Participation in the process includes the cyber security professionals (IT and industrial automation & controls) and physical plant security professionals. In addition, many chemical sector companies have

well established relationships with local and state law enforcement agencies. Information is exchanged with appropriate agencies during cyber incidents.

**3. What specific changes are needed to make public-private partnerships more effective and workable? What measures are necessary to ensure an approach where “action plans” are employed which businesses/government can effectively measure progress toward a cyberspace that is “assured, reliable, and survivable”? (What are industry roles and responsibilities? How should we think about private sector accountability?)**

The chemical sector supports the findings and recommendations of the National Infrastructure Advisory Council (NIAC), published in its Critical Infrastructure Protection Strategic Assessment, dated October 14, 2008. A link to that report is included here:

[http://www.dhs.gov/xlibrary/assets/niac/niac\\_critical\\_infrastructure\\_protection\\_assessment\\_final\\_report.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf)

In addition there may be merit in considering the private sector as two separate entities: the technology providers and the users of technology. There should obviously be some differentiation in the expectations of these two entities in advancing the nation’s cyber security posture. Technology continues to advance rapidly and is being incorporated deeply into corporate processes. It may be an appropriate time for the government to establish minimum cyber security standards for technology providers to meet, when delivering solutions to companies in a critical infrastructure sector.

The chemical sector is a ‘technology user.’ Each chemical company has to play a role in educating its internal users as well.

Security in the chemical sector is now regulated and some metrics will be derived from this process. In addition, the chemical sector is working with DHS to develop the Chemical Sector Roadmap to Control Systems Security. This roadmap will have milestones that will indicate progress.

In addition, many companies participate in InfraGard. InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. This organization should be leveraged for more effective public-private partnerships.

**4. How can industry and government achieve a national cyber security posture which encourages innovation and prosperity? (How do we amplify both security and economic prosperity? Are current government structures effective? How can we create and maintain security in cyberspace while balancing the need for economic growth, privacy, etc.?)**

The government should leverage security guidance implemented in the Chemical sector rather than creating different requirements and regulations. Current government structures could improve their coordination and information sharing with the Chemical sector as defined in the feedback from the sector during Cyber Storm II. The government should continue to invest in research initiatives underway in organizations like Idaho National Labs (INL), the National Institute of Standards and Technology (NIST) and the Institute of information Infrastructure Protection (I3P).

Innovation in the cyber security space, will be greatly facilitated by the government encouraging more research by the technology companies. The government should lead the implementation of more secure technology. The federal government's procurement power should be used to support commercial

markets for secure operating platforms and network services. Such technology and services should be made available to industry for deployment of critical infrastructure. The federal government can accomplish this by including higher requirements for secure technology in their Request For Proposals (RFPs).

This document was prepared by:

Christine Adams, The Dow Chemical Company  
Director, Chemical Sector Cyber Security Program  
(202) 429-3417  
cmadams@dow.com