American Chemistry Council℠

Robert K. Knake
Director for Cybersecurity Policy
The White House
National Security Staff

Mr. Knake:

Thank you for meeting with the American Chemistry Council (ACC) on November 26, 2012 to discuss the important issue of cybersecurity and the protection of critical infrastructure. During our meeting, we provided an overview of the chemical industry's progress and accomplishments to date in the area of cybersecurity. We talked about the existing regulatory structure in place for our sector, namely the Chemical Facility Anti-terrorism Standards (CFATS) program, which addresses cybersecurity. As the Administration considers the issuance and contents of an Executive Order to address cybersecurity, we believe it is essential that industry receive credit for the work that has already been done, so that duplicative and unnecessary efforts are avoided.

We would also like to reiterate the need to address the following key issues as part of any policies aimed at enhancing cyber security for the nation's chemical sector:

- Leveraging Existing International Standards: ACC encourages the leveraging of the existing work developed by the international cyber security standards development community. Much progress has been made through organizations such as ISO, IEC and ISA, who include cyber experts from both the public and private sectors. In this regard, NIST could help by providing leadership and participate in these vital standards development activities.

- Information Sharing: Two-way cybersecurity information sharing between the public and private sectors is essential. To be effective, such information sharing must be timely, specific, and actionable and protected from public disclosure. Whether included in an Executive Order or in future legislation, a collaborative approach should be emphasized by establishing a public / private partnership designed to 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 including Freedom of Information Act requests.

- Strengthening Cyber Laws: Congress and the Administration should work to strengthen U. S. laws against cybercrime and to more aggressively prosecute cyber criminals. U. S. laws should be updated to protect critical infrastructure from cyber-attacks. Those accountable for perpetrating intentional acts designed to cause harm to critical infrastructure operating systems, of theft of intellectual property or personal information for financial gain must be prosecuted fully under the law. Additionally, the U. S. Federal Government should develop strong international partnerships that work 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. ACC encourages the Federal Government to include this issue as a central component of its strategy in its fight against domestic and international cybercrime.

Thank you for this opportunity to be a constructive partner in protecting our nation's critical infrastructure cyber systems and we look forward to working with you in the future.

Sincerely,

William Erny
Senior Director
Homeland Security Policy