Cybersecurity and The Chemical Industry

American Chemistry Council

Cutting-edge technology and innovation are two mainstays for the Business of Chemistry. The chemical sector uses information and operations technology to help manage the complex process for developing, manufacturing, and delivering its products. Our industry also generates valuable intellectual property related to new chemistries and processes. Protecting the technology that helps run facilities, as well as the valuable information regarding chemical formulas and customer databases, from a potential cyberattack are critical for enhancing security for our industry.

ACC and its members have taken numerous aggressive steps to enhance cybersecurity:

INDUSTRY PROGRAMS & INITIATIVES

- Invested more than $17 billion under ACC's Responsible Care® Security Code that requires members to enhance both physical security and cybersecurity
- Implemented the National Institute of Standards and Technology (NIST) cybersecurity framework in conjunction with the Responsible Care Security and Process Safety Codes
- Created a cyber security information network within its Chemical Information Technology Center (ChemITC) toserve as a forum for IT professionals in the chemical sector to share cybersecurity information & best practices

FEDERAL PARTNERSHIPS & REGULATIONS

- Collaborate with U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) toshare information on cyber-attacks and vulnerabilities
- Support implementation of the security regulatory program for our industry, the Chemical Facility Anti-Terrorism Standards, which includes cybersecurity requirements

POLICY PRIORITIES

ACC supports federal efforts that:

Encourage the sharing of timely cyber threat information by providing protections related to lawsuits, public disclosure, and antitrust concerns, as well as safeguard privacy and civil liberties.

Recognize chemical sector efforts to enhance cybersecurity through existing voluntary standards, federal regulations, industry programs, and/or current information sharing frameworks.

Aggressively prosecute cybercrimes and **hold those accountable for perpetrating acts intended to cause harm** to critical infrastructure operating systems, for stealing intellectual property and trade secrets, or for obtaining personal information for financial gain.

For more information, visit **AmericanChemistry.com/cyber**.