National Association of Chemical Distributors

Cybersecurity

NACD Position

NACD priorities include:

- Congress passing legislation that facilitates the sharing of timely cyber threat information by providing protections related to lawsuits, public disclosure, and antitrust concerns, while also guarding privacy and civil liberties.
- Making practical updates to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (version 1.1), while ensuring the standards remain voluntary and enjoy broad support from the business community.
- Clarifying federal and industry roles and responsibilities in protecting from, responding to, investigating, and prosecuting cybercrime. Ensuring the departments and agencies tasked with these responsibilities have the resources and the interagency coordination they need to excel.
- The federal government aggressively prosecuting cybercrimes and holding 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.

Policy Background

As part of our commitment under NACD Responsible Distribution® Code of Management Practice, Code XIII: Security, NACD member companies recognize that protecting information and information systems is a critical component of a sound security management system.

Unlike many other critical infrastructure sectors, the federal government regulates cybersecurity for the chemical sector. Under the Chemical Facility Anti-Terrorism Standards (CFATS), chemical facilities must meet comprehensive cybersecurity requirements that address the protection of business networks and process control systems.

Beyond CFATS, the chemical sector has also been actively engaged with the federal government as the National Institute of Standards and Technology moves forward with implementing a cybersecurity framework in response to Executive Order 13650.