



Facility Security Public Policy

As a nation, we have demonstrated firm resolve in protecting our critical infrastructures and key assets from further terrorist exploitation. In this effort, government at all levels, the private sector, and concerned citizens across the country are involved in important partnership and commitment to action.

The VMA members, large and small, have a substantial interest and concern regarding requirements and operations of a facility site security program. The majority of the nation's critical infrastructures and key assets are owned and operated by VMA members. VMA members prudently engage in risk management planning, and invest in security as a necessary component of their business operations and to assure customer confidence. In this new world of increased threat, VMA members remain the first line of defense for their own facilities. VMA members have increased their investments in security to meet the demands of the new threat environment.

The term "security" means an action carried out to ensure or enhance the protection of a manufacturing facility, utilizing appropriate means to address personnel security, unauthorized access, perimeter security, and cyber-system threats. The Maritime Transportation Security Act, the Chemical Facilities Anti-Terrorism Standards, Title IV of the Bioterrorism Act, and other statutes require and authorize enforcement of vulnerability assessments and security plans for certain private facilities.

The VMA supports the comprehensive security network established through existing federal laws, standards and public-private partnerships. As proposals related to facility site security are developed and revisions to current law are considered, the VMA recommends that any public policy or legislation continue to reflect the following principles:

- Maintain centralized federal authority at the Department of Homeland Security (DHS).
- Recognize security work already implemented by companies and stakeholders accountable for security of critical infrastructure. It is wasteful (and unfair) to require companies to add *unwarranted* layers of governmental bureaucracy onto existing industry programs, which *already meet* the requirements of other government regulations *containing* all the necessary components of security. Manufacturers should be deemed to be in compliance if they have

implemented an industry standard that DHS determines is substantially equivalent to the requirements under any *existing* facility site security law.

- Protect submitted information via appropriate sharing within the government and assurance against release to the public, which could undermine the very security that any legislation would seek to enable.
- Promote and recognize voluntary cooperation and agreement between government and industry stakeholders accountable for security of critical infrastructure; and encourage voluntary actions. Partnerships are currently providing the foundation for developing and implementing coordinated protection strategies.
- Guarantee reasonable federal preemption of conflicting non-federal requirements or requirements that pose obstacles to the accomplishment of federal laws and directives.
- Avoid requiring chemical elimination, substitution or reduction schemes disguised as security measures. The VMA has seen proposals at both the state and federal levels that purport to be based on security concerns, yet the effect would be to limit or eliminate the use of certain chemicals without accounting for the public benefits derived from the products manufactured from their use. These proposals, advanced in the name of "inherently safer technology," discount other federal regulatory programs such as OSHA's Process Safety Management Program and EPA's Risk Management Program designed to ensure safe management of these chemicals, and ignore the significant and longstanding commitment represented by industry's contribution to research and development in this country. Focusing on concepts like "inherently safer technology" distracts from the real issues of security.
- Ensure some limitation of liability from civil lawsuits in the event of a terrorist act. No legislation or rule should be construed to create a private right of action, or grant jurisdiction to a court, enabling private persons to enforce the law or rule against anyone subject to it. Allow only those parties that are directly subject to a rule to bring a petition for review against a rule, not just "any person."
- Acknowledge that only limited funding exists to privately finance security measures. Security investments reflect what is reasonable in light of threat and vulnerability conditions, and economically justifiable and sustainable in a competitive marketplace or in an environment of limited resources. Any security mandate must be based on a cost-benefit analysis in order to protect industry stakeholders accountable for security of critical infrastructure from significant disruption of commerce and to protect civil liberties.
- Allow for flexibility in achieving standards established by legislation and recognize that the level of risk and the attractiveness of a target varies from facility to facility, even within the same industry. No federal program should take a one-size fits all approach to security and should instead recognize the variable nature of risk and allow companies to achieve compliance in a way best suited to their particular situation.