

Statement of
David C. Pulham, Ph.D.
Director of Compliance
Siegfried USA

before the

United States House of Representatives
Committee on Homeland Security

On

The Chemical Facility Anti-Terrorism Act of 2008

February 26, 2008

Good morning Chairman Thompson, Ranking Member King, and Distinguished Members of the Committee. My name is Dr. David C. Pulham, Director of Compliance at Siegfried (USA), Inc. in Pennsville, New Jersey. I spent 27 years with the Food and Drug Administration as a National Expert Investigator. Part of this responsibility required inspecting pharmaceutical facilities around the world and qualifying foreign regulatory agencies. As Director of Compliance at Siegfried, my responsibilities include FDA, DEA, EPA, OSHA, and DHS compliance.

Thank you for this opportunity to share with you my company's perspective on the Chemical Facility Anti-Terrorism Act of 2008, specifically with regard to inherently safer technology. My remarks will speak generally to the issue of inherently safer technology, reference our experience with the State of New Jersey's security provisions, and conclude with our recommendation on the bill going forward.

Siegfried (USA)'s Pennsville, New Jersey, facility manufactures bulk pharmaceuticals and employs 150 personnel. Most of Siegfried's products are controlled substances. Therefore, we are highly regulated by the Drug Enforcement Administration. Siegfried takes pride in its compliance record with all Federal and state government agencies.

Siegfried (USA) is a member of the Synthetic Organic Chemical Manufacturers Association (SOCMA), which is the leading chemical industry association representing the batch, custom, and specialty chemical industry since 1921. As a member of SOCMA, Siegfried adheres to the principles of the ChemStewards® program, an environmental, health, safety, and security management system. This self-imposed program requires companies to develop systematic approaches to environmental and chemical risk management with independent, third-party verification. ChemStewards incorporates SOCMA's security vulnerability assessment methodology, which is recognized by the Center for Chemical Process Safety and is accepted by the Department of Homeland Security for Tier Four facilities under the Department's Chemical Facility Anti-Terrorism Standards. SOCMA makes this methodology publicly available in its effort to serve as a leading industry resource for assessing security vulnerabilities at chemical facilities.

New Jersey recently amended its Toxic Catastrophe Prevention Act (TCPA) rules to require existing facilities to complete an "Inherently Safer Technology Review." Siegfried's assessment of this process is that it is essentially a paperwork exercise to document, in great detail, steps and considerations that we take as a normal part of our process. Simply put, inherent safety is a concept that the chemical industry invented, and we consider it continuously as we design and modify our production processes.

Securing our products is an ongoing responsibility. So is complying with the comprehensive system of existing state and Federal laws. These regulatory regimes require extensive process hazard analysis, risk management planning, and public reporting on chemicals we handle on-site and, in some cases, prior to handling them on-site. We feel that these regulations, complemented by our own process-safety decisionmaking, provide a concrete and meaningful level of consequence reduction at all stages in the product lifecycle.

Speaking specifically of existing Federal rules, Siegfried supports DHS's existing Chemical Facility Anti-Terrorism Standards, which do not include any IST mandates. These rules require comprehensive vulnerability assessments and security plans, and those plans have to meet almost 20 rigorous security performance standards. We encourage this Committee to support the current approach.

Mr. Chairman, I've heard people say that, since the industry already considers inherent safety in its decisionmaking process, and since we're already bound by related regulatory regimes, it should be easy for us to simply comply with a new layer of IST regulation. In fact, it is never a simple task to integrate a new set of rules, imposed by a new regulatory entity, with the engineering and compliance programs we already have to manage. An IST mandate would complicate, and in some cases could undermine, existing practices or compliance. Mandating IST for companies like Siegfried that manufacture hundreds of specialty batch products every year is a much greater exercise than what may appear on the surface. Having to debate which approach is inherently safer in a given case would slow down our ability to meet customer needs. And it could be dangerous, if we are compelled to accept, or go along with, an approach that we personally think may not be the lowest-risk approach. With all due respect, this issue is vastly more complicated than most people appreciate.

Thank you for the opportunity to share with you Siegfried (USA)'s perspective on inherently safer technology and existing Federal security rules. I look forward to your questions.