



Testimony of

Beth Turner

Director – Global Operations Security
E.I. duPont de Nemours and Company, Inc.
1007 Market Street
Wilmington, DE 19898
302-774-1000

Before the
Senate Homeland Security
and Governmental Affairs Committee

“Chemical Facility Security: What is the Appropriate Federal Role? (Part II)”

July 27, 2005

Madam Chair, Senator Lieberman, and distinguished Members of the Committee, my name is Beth Turner. I am the Director of Global Operations Security for DuPont. In this role, I am responsible for the security of our operating assets around the world. I also chair the Chemical Sector Coordinating Council, a mechanism that enables our critical sector of the nation's infrastructure to interact with the Department of Homeland Security (DHS). I co-led the American Chemistry Council (ACC) team that developed the original Responsible Care® Security Code in 2002 and the team that reassessed the Code in 2004. I have been a member of the ACC Security Team since its formation. Thank you for this opportunity to speak today. My testimony will first address the actions DuPont has taken to protect our employees, the communities in which we operate, and our facilities; second, our work on industry programs; and third, our views regarding critical legislation in this area.

DuPont is a global corporation founded 203 years ago. The founders of our company established an uncompromising commitment to safety that continues today. DuPont began as a manufacturer of black powder for the U.S. government in 1802, operations that, by their very nature, required a focus on safety and technology. The company's founder, E. I. duPont, built safety into the very fabric of DuPont culture by requiring his managers to live on the first manufacturing sites. That culture and clear personal accountability remain just as strong today. These form the foundation for every system and process in DuPont. In fact, it has been the underpinning for many DuPont products through the years. Our discovery of nylon, for example, made safer parachutes for D-Day, and our development of Neoprene®, a synthetic rubber, made military transportation easier and safer. In today's war on terrorism, products such as Kevlar® high-performance fiber, for example, are used in applications such as body and vehicle armoring; and our Sentry-glass® technology helps to protect the occupants of the Pentagon, embassies and civilians around the world.

Today, our core businesses often involve producing valuable products from a wide range of chemical feedstocks in high temperature, high-pressure reactions. This requires an intense focus on safety and security. DuPont is recognized as one of the safest companies in the world. In fact, the DuPont workplace safety record in the 1920s was actually better than the U.S. industry average in the year 2004. Our focus on safety and security is driven by what we at DuPont know as our core value commitment to our employees and our communities.

DuPont Voluntary Implementation of Security Measures

While security has long been part of our site operations, the world-changing events of September 11, 2001, compelled us to view security in a different light. Our reaction was both tactical and strategic. We immediately hardened security at our facilities and then began focusing on a longer-term strategic program that we are implementing in phases and continually strengthening. We have also

truly integrated security into our DuPont culture so that we safeguard our employees and our neighbors, as well as protect the company's assets. I'd like to review some of the steps we took to make this happen. I will discuss physical security actions, as well as process safety measures, administrative procedures, and emergency response preparedness, all of which have a vital role in an integrated security plan.

Quickly after the 2001 attacks, senior corporate leadership made security an even higher priority by integrating security into the company's longstanding safety core value. This move sent a very clear and powerful message throughout the corporation. It immediately resulted in organizational changes and revisions to corporate policy, as well as extensive communications with employees throughout the company. Since the fall of 2001, security has continually been reinforced as an integral part of our long-standing safety culture. This corporate leadership decision to manage security as we have managed safety for over 200 years allowed DuPont to aggressively step up to the new realities we face as a nation and a world.

In early 2002, DuPont launched a global security survey to better understand specific security measures in place at over 500 locations around the world. We assessed operating facilities and prioritized them using a risk-based approach. In conjunction with the criteria established by the American Chemistry Council, we placed approximately 1/3 of our U.S. sites in the highest priority grouping named DuPont Category 1 sites. Of these, about 2/3 are covered by the U.S. EPA Risk Management Program. The remaining DuPont sites had no potential for off-site release or theft of materials and were placed in Category 2.

A site security leader at each location was designated as the focal point for security. Networks of site security leaders were formed around the world and function today to exchange best practices and to enhance security skills. I want to give special recognition to these site security leaders who have worked tirelessly since the 2001 attacks. It is their outstanding work that I review with you today.

To develop our vulnerability assessment (VA) methodology for high priority sites, we collaborated with the Sandia National Laboratories. DuPont trained U.S. Category 1 site security and process safety leaders in July of 2002, and those individuals led the site security assessment teams, with oversight and support from corporate headquarters.

The assessments identified potential vulnerabilities and appropriate upgrades to procedures, equipment, staffing, and manufacturing processes. Local law enforcement, emergency planning and response organizations, and others conducted third-party verifications of the upgrades at U.S. sites. DuPont accelerated the timing for the overall vulnerability assessment process and

completed upgrades and verification at all DuPont U.S. Category 1 facilities between 9 and 12 months sooner than the American Chemistry Council deadline.

Vulnerability assessments were also conducted at DuPont U.S. Category 2 facilities. Security enhancements were identified and implemented at these sites as well.

Category 1 sites in Asia, Europe, and Latin America were identified using this same risk-based approach and assessment methodology. Security upgrades at these facilities are currently being implemented.

While I cannot speak publicly about specific actions at specific sites, I can describe in general terms the types of upgrades that have been implemented at our U.S. Category 1 sites. Upgrades have been, and continue to be, made to equipment, staffing, processes, procedures, and preparedness to secure the sites from a range of reasonably predictable and defensible threats.

First, I will review security equipment upgrades. These varied from site to site but included fencing, motorized gates, turnstiles, signage, access control systems, video surveillance, lighting, electronic intrusion detection and alarm monitoring, crash gates, and barricades. We have, subsequently, implemented a special maintenance program to ensure the new equipment remains functional and reliable.

In addition to new capital equipment, security practices were enhanced as appropriate at every site. Perimeter patrols were increased, and strict site access control measures were implemented. These include significant reductions in on-site vehicular traffic and increased inspections of rail cars, trucks, and other vehicles, as well as stricter policies for checking the identification of those seeking access to the sites. Suspicious activities are quickly identified with the new equipment and immediately reported to law enforcement for immediate investigation.

Security officer staffing has been significantly increased, and we have added officers with prior experience in security, the military, or law enforcement. Security officers received additional training and are continually retrained. Security supervisors receive an incentive to take additional training and become professionally certified as Certified Protection Officers.

Second, strong process safety management is one of the most important means of protecting our employees and our communities. A typical large chemical facility includes miles of piping and thousands of pressure vessels, tanks, pumps, valves, instruments, and other components. Each process unit is uniquely sized and designed to handle a range of chemicals and operate under a variety of temperatures and pressures.

The long-standing DuPont process safety management system is designed and applied to address these complexities. It includes engineered safety systems such as interlocks, excess flow and automatic shutoff devices, relief valves, spill containment structures, and emergency shutdown devices. Our strong process safety program also includes extensive operating procedures, testing and inspection of equipment, and thorough safety reviews of any process and equipment changes. Process safety also includes formal, detailed, and regular analyses of operations. These analyses are one of the most critical components of process safety. Such analyses are complex and must be conducted by engineers and other experts skilled in hazard evaluation methodologies and chemical processes. Process safety analyses for both new and existing facilities consistently include evaluation of opportunities to use inherently safer approaches and lower risk chemicals. I will expand upon the topic of inherent safety in a moment.

Another key component of process safety is the DuPont requirement to conduct detailed audits on all individual process units. The audits are conducted by highly experienced auditors who use a formal protocol of nearly 300 items. Each audit takes a team of two to three auditors approximately five days to conduct. Corporate headquarters tracks audit results and suggested improvements until all items are completed. An external third-party auditor conducts an annual evaluation of the audit program effectiveness. Results are reviewed with senior leadership, and findings are addressed.

DuPont has long had a robust cyber security program aimed at ensuring business continuity. In 2002, we implemented a program to secure all high and medium risk process control systems at sites around the world. Sites conducted cyber security vulnerability assessments on critical manufacturing and control systems. As a result of the assessments, measures were taken to install special firewalls to protect critical process control systems from remote access.

Key programs in place prior to the 2001 attacks have been further strengthened. As one means to provide a safe and secure work environment, DuPont has a robust workplace violence prevention program. We aggressively respond to all threats made against employees or contractors. Formal training is conducted periodically to train supervisors on how to recognize, respond to, and investigate all threats made in the workplace.

Screening workers' backgrounds is a critical, longstanding part of our safety and security program. In the U.S., and as laws allow in other countries, DuPont requires criminal background checks of all employees upon hiring and all contractors seeking access to a DuPont site. The U.S. background check looks for misdemeanors and felonies for the seven-year period prior to the proposed date of access to the site. The checks must be of court records. In addition, DuPont does not accept checks performed under other programs unless they are conducted in strict conformance with our own internal standards. To provide

perspective, one of our large facilities has a normal work force of 2600 employees and contractors. This swells by an additional 600-700 contractors during major maintenance overhauls. Contract firms that work at this site conduct about 2500 criminal background checks per year.

Long-standing relationships with local law enforcement and emergency planners have also been reinforced, and new relationships have been formed at the local level with federal groups such as the FBI and the Joint Terrorism Task Forces. DuPont sites and these local and federal groups work together to train, identify and investigate suspicious activities, patrol areas around our sites, and conduct tabletop and full-scale exercises. In addition, strong relationships have been developed with the Coast Guard at DuPont facilities regulated under the Maritime Transportation Security Act of 2002. Each of these sites has been successfully inspected by the Coast Guard. Perhaps a few brief examples of interactions with local law enforcement and first responders would be helpful:

- One site, for example, sets aside a month each year where all local community response units (i.e, HAZMAT, rescue, divers, river boat, fire, etc.) tour the facility to understand the layout, chemicals, fire system, and capabilities of the DuPont emergency response team. This allows for a much more effective, integrated response.
- In 2004, one site's annual emergency response drill with local volunteer fire departments was a simulated railcar accident releasing a flammable material. The drill resulted in the local departments gaining an appreciation for DuPont's capability to supply firewater, and an agreement was reached to work on improving the unified command and control structure.
- Another site drilled with the local SWAT team on a scenario of a hostile employee taking a hostage inside the plant. After the drill, the site met with the SWAT team, other local law enforcement agents, emergency responders, and the DuPont emergency preparedness team to discuss what had been learned.
- At one of our sites, the Coast Guard has visited several times to witness our response to drills. The local area conducted a drill, using \$250,000 of funding from the federal Department of Homeland Security. It simulated two terrorist attacks, one at the airport and the other on the highway. As part of the drill, the Coast Guard escalated security to Maritime Security Level 3, allowing us to test the site's preparedness.

We work with a range of trade associations and federal government agencies, including the Department of Homeland Security, to develop effective national programs to secure key operations. As illustrated by the examples provided above, we have frequent interaction with many local, state, and federal entities

and have found government agencies to be willing and helpful partners in furthering our security efforts.

Emergency response planning has long been a DuPont priority. Our sites have formal emergency response plans and, as noted above, conduct drills and exercises with both our own response personnel and with local first responders. We actively participate in Local Emergency Planning Commissions (LEPC) and believe that these organizations are very important in creating strong, integrated emergency management systems. The most effective LEPCs are those in which the members share a strong commitment to protect the local community, have strong leadership and participation, and are adequately funded. DuPont site participation in LEPCs across the country includes, for example:

- Regular meetings and collaboration on security preparedness.
- Security drills involving police, SWAT forces, emergency services and fire departments.
- Committee leadership.
- Joint review of and learning from community incidents ranging from gasoline spills to a small chemical release in a local high school chemistry class.
- Shelter-in-place awareness campaigns.
- Joint support and guidance for local emergency warning systems.

DuPont also works with the American Chemistry Council CHEMTREC® program to provide technical assistance for chemical emergencies. In addition, we are active in the TRANSCAER® program to provide training, conferences, and other educational programs to local communities, law enforcement agencies, and first responders. DuPont is actively involved in many local mutual aid groups. These groups frequently discuss procedures and lessons from incidents, participate in drills, and share unique expertise. It allows members to have access to wide-ranging emergency response capability and equipment.

In addition, DuPont maintains its own regional transportation emergency response teams for incidents involving our own materials and as mutual assistance to other companies. In 2004, we provided assistance to approximately 35 communities throughout the US. In addition to incident mutual aid, DuPont has rail tank cars and other transportation containers that are used to train public sector emergency responders in managing chemical releases during rail, ocean or highway accidents. In 2004, 5000 first responders were trained in approximately 150 communities in the United States, Canada, and Mexico. In Asia last year, DuPont also trained various government agencies and 1200 first responders.

In addition to site security, there is a significant focus on transportation security. DuPont actively works with the railroads to better coordinate rail service to our sites and to store cars within the secure site perimeters. Rail carriers work with us to secure key shipments and have implemented significant security plans. For

truck transportation, DuPont has partnered with truck carriers on measures such as anti-theft devices and electronic surveillance, formal driver security training, planning safe routes, and improved identification of drivers.

My company became one of the first members of the voluntary Customs-Trade Partnership Against Terrorism (C-TPAT) program in November 2002 and is actively working to tighten security of goods entering the U.S. Product security and other aspects of securing the value chain have been, and continue to be, integrated into processes to screen new customers, audit contractors, and conduct product reviews and risk assessments.

Each DuPont U.S. Category 1 site has carefully planned for special security actions that might be required in extreme circumstances – e.g., routing all deliveries and people to remote locations for special screening. Operations security is a critical component of the global crisis management process. A special automated crisis notification system has been implemented so that the security leaders at all DuPont U.S. Category 1 sites can be contacted within 10 minutes or less.

When the national threat level is escalated, security measures are immediately assessed by both headquarters and sites. This assessment occurs even if there is no direct connection to the chemical industry or DuPont. Additional measures are determined based on the specific threat environment at the time. Measures may be implemented broadly or in a more focused manner. An example is DuPont's internal response to the recent London bombings. Although the DHS escalation to orange pertained only to mass transit, we directed all DuPont U.S. Category 1 sites to inspect 100% of inbound rail cars, along with trucks and all other vehicles, if they were not already doing so.

Perhaps the most powerful security preparedness initiative activated since 9/11 involves the ongoing vigilance of our individual DuPont employees and contractors. A cornerstone of DuPont safety has always been the personal accountability each of us has as a DuPont employee for our own safety and that of fellow employees and neighbors. The same is now true for security. Our employees and contractors have readily accepted this new responsibility. We have delivered extensive security awareness training to all employees and contractors and routinely communicate information to maintain the awareness.

We often find that individuals who do not have direct security responsibility are some of the best security officers. I'd like to share a few examples of actions by employees eager to contribute to our security effort:

- Employees question unknown cars in the parking lot or aircraft flying near the site. They ask questions or bring things to security's attention if something is different. They notice if a door isn't locked when it should be, and they report unusual activities on and around the plant.

- At one of our sites, an employee observed a contractor taking pictures at the plant. This is a violation of site policy. The incident was immediately reported, investigated, and communicated to everyone on site. At the plant manager's weekly meeting, employees discussed the incident, the proliferation of photographic devices, and the site policy.
- Security is fully integrated into site safety in the minds of our employees. When a site leader asks at a safety meeting, 'How many people are responsible for security at our site?', the reply from employees is always, 'All of us.'

I've touched on a wide range of security measures DuPont has implemented. It is important to note that the American Chemistry Council's Responsible Care® Security Code has certainly raised the bar by setting high standards for its members. Those companies that have implemented the Code have been recognized by agencies such as the Department of Homeland Security, the United States Coast Guard, U.S. Customs and others as having strong security practices in place across the country. On a global basis, the U.S. Responsible Care® Security Code has been a foundation on which site-specific, country-specific, and company-specific elements have been added to further strengthen our efforts.

As I have described, DuPont has very strong, thorough security systems and processes. However, we recognize that an effective security program is a journey. Hence, our security enhancements are ongoing. It requires constant vigilance and continual improvement. As with safety, there will **never** be a time when DuPont says, "We have done as much as we can on security."

Federal Chemical Security Legislation

Let me turn now to the issue of federal legislation. We appreciate the thoughtful approach this Committee has taken to this issue, and we look forward to working with you as you develop legislation.

While we believe DuPont has taken appropriate actions and that the Responsible Care® Security Code has helped other members of the American Chemistry Council do the same, we recognize that government has an important role in protecting this critical sector and ensuring all chemical sites are taking appropriate actions. Accordingly, we support meaningful and effective federal chemical security legislation. We also support the core principles for chemical security that were outlined on June 15 by Department of Homeland Security Assistant Secretary Robert Stephan in his testimony to this Committee.

I would like to briefly share our thoughts on important elements that should be addressed in the legislation and resulting regulations.

First, and foremost, it is important that the legislation have a clear security focus. We think it is critical to keep facilities focused on core security activities to ensure that they can get the job done in a timely and effective manner. To do this, legislation should not direct facilities to pursue actions that are fundamentally not security matters. Doing so would potentially delay and dilute essential security enhancement work.

Second, it is important that the legislation be risk-based so that government and private sector resources are allocated where they are most needed and can provide the greatest benefits. The prioritization of DuPont sites, as I discussed earlier, has been invaluable in channeling resources commensurate with the potential risk. Department of Homeland Security Secretary Chertoff and his predecessor Secretary Ridge have consistently emphasized a risk-based approach for the agency's work. A risk-based approach, which allows security measures to be escalated when the threat environment changes, is key to helping our country and the chemical industry be secure and competitive.

Third, DuPont believes that regulatory authority for chemical security should reside with the Department of Homeland Security. The main reason DHS was created was to provide central federal oversight of security. The agency has established a close relationship with the chemical sector through mechanisms such as the Chemical Sector Coordinating Council that I currently chair and the DHS Chemical Sector Specialist role that serves as a direct liaison with the individual sites and companies in the chemical sector. While DHS faces challenges as a new agency, it is making good progress in addressing them.

DHS and the chemical sector are already working together on programs such as the Risk Analysis and Management for Critical Asset Protection (RAMCAP), the Homeland Security Information Network (HSIN), and the Buffer Zone Protection Plan (BZPP). DHS is also a critical conduit for intelligence and threat information and is connected into other government agency threat streams. In addition, DHS is the means by which the chemical sector connects with all other infrastructure sectors, many of which are vital to the business continuity and security of our sector. Finally, DHS already administers the Maritime Transportation Security Act of 2002, which is the only existing set of security regulations impacting chemical facilities. In providing DHS with regulatory authority over chemical security, it is critically important that the program DHS is asked to implement be appropriately resourced and staffed.

With lead regulatory authority vested in DHS, we believe other agencies should continue to play a role, in consultation with DHS. These include the Federal Bureau of Investigation, the Department of Transportation, and the Environmental Protection Agency that administers the Risk Management Program (RMP) of the Clean Air Act Amendments of 1990. Regulatory jurisdiction for facilities already covered by the Maritime Transportation Security Act of 2002 should remain with the Coast Guard in DHS. We believe chemical

plant security should be guided by a clear federal program rather than a patchwork of state and local programs.

Fourth, it is important to recognize the different, yet complimentary roles for government and the private sector in security matters. The private sector can, and should, take reasonable steps to secure its facilities against reasonable threats. However, there are clear boundaries where industry's capability ends and the government responsibility for defense of the nation's critical infrastructure begins. We cannot be expected to fully defend against military-style assaults, when it is clearly a lead role for government. Requirements for chemical plant security must be developed in the context of public security measures.

Fifth, flexibility is important. Prior witnesses have discussed the significant diversity of facilities producing and managing chemicals. DuPont operates thousands of different processes employing a wide variety of raw materials. These range from facilities producing soy protein to plants managing flammable materials and from rural to urban locations. Chemical security legislation should establish the main principles that are fundamental to a risk-based approach. Then, the legislation should allow flexibility in the rule-making process and implementation to accommodate the significant diversity of the chemical sector. Legislation needs to permit DHS to tailor its regulations to implement a timely and efficient program, focus its oversight, and deploy its resources on those matters that will best enhance security.

Sixth, the Maritime Transportation Security Act of 2002 (MTSA) has proven to be an effective security regulation for DuPont facilities covered under Part 105 of the Coast Guard rules. I respectfully recommend that it be used as a model for chemical security regulation of the highest priority facilities. MTSA Part 105 addresses the essential elements of a strong security program including staffing, training, security vulnerability assessments, facility security plans, exercises, incident reporting, and audits. It provides for protection of sensitive security information, as well as civil penalties for non-conformances. Parts of the MTSA regulations would need to be broadened beyond maritime transportation and considered for other minor modifications; but, fundamentally, MTSA is strong and effectively secures covered facilities. A case in point--one of our DuPont facilities, initially covered by MTSA Part 105, no longer receives regulated materials at its wharf. However, since the facility has already invested in meeting the MTSA requirements and believes that these requirements are enhancing site security, the facility has decided to voluntarily continue using the MTSA Part 105 requirements as the basis for their site security program.

Next, for both efficiency and fairness, new legislation and regulation should take into account the work already done under programs such as Responsible Care® and the Maritime Transportation Security Act. Both of these have materially enhanced security at impacted facilities, and the prior efforts should be given credit as a regulatory framework is developed.

Another important issue is protection of information that could present a security risk if made public. We believe strongly in transparency and accountability. However, in the security arena, information disclosure presents unique risks. Two federal rules have proven to be effective in protecting sensitive information from disclosure. These are the “Sensitive Security Information” (SSI) rules of the Transportation Security Administration and Department of Transportation, and the “Protected Critical Infrastructure Information” (PCII) rules of the Department of Homeland Security. However, limitations to both rules could leave some sensitive information requested or obtained by the government unprotected from disclosure. The SSI rules apply only to transportation security and, for the most part, only to the aviation and maritime industries. The PCII rules apply only to information voluntarily submitted to the PCII Program of DHS. PCII does not protect information that is required to be submitted to the government or information that is submitted to other branches of DHS or to other federal or state agencies. Finally, PCII does not support the ability of DHS to share information with state and local governments unless formal, written agreements have been reached with those governments. Any new chemical security legislation must have comprehensive provisions to ensure security-sensitive information is protected and to facilitate an effective exchange of information to and between governmental agencies.

My final comments pertain to inherent safety, commonly referred to as inherently safer technology (IST). At DuPont, inherent safety has been an integral part of our plant design and process safety systems since the 1960s. Over the decades, we have assessed and implemented many inherently safer solutions. The following are examples of inherently safer process modifications that DuPont has recently implemented after extensive analysis and re-engineering:

- Converted from shipment and temporary storage of propylene (a flammable) in river barges to on-site storage of a much smaller quantity, resulting in inventory reduction by a factor of 5.
- Redesigned the process chemistry and manufacturing technology to eliminate sulfur dioxide (an inhalation hazard) and convert to sodium bisulfide (very low toxicity).

These solutions cover all facets of risk reduction, not just the “chemical replacement” option that is frequently cited at the exclusion of other options. DuPont does not support that narrow definition. Instead, we must also include reducing the quantities of hazardous materials, moderation of operating conditions such as pressures or temperatures, simplification of process equipment, and provision of containment structures.

While inherently safer analysis is fundamentally risk-based, it consistently includes an evaluation of opportunities to reduce the inherent hazard of our processes and raw materials. Inherently safer solutions must be applied at the

local chemical process and technology level and not through a "cookie cutter" approach. Each process segment must have the flexibility to evaluate inherently safer options on a case-by-case basis. This is necessary because each option for change has unique implications that must be considered.

Evaluations must assess technical feasibility, benefits of risk reduction, introduction of new risks or trade-offs, impact on proprietary technologies, effects on product quality, and implementation and ongoing operating cost. It is important to ensure that risk is not reduced in one place and increased in another and that the site can continue to operate the process reliably and safely. It is also important to ensure the ability of our suppliers to provide timely delivery of any new raw materials. In addition, changes to our product formulations must not create unintended consequences in our customers' operations. Finally, we must not disrupt the supply chain as we produce high quality products at competitive prices that customers demand.

Given the breadth and depth of an inherent safety evaluation, it typically takes several months or years to complete. This needs to be considered relative to the kind of short timeframes appropriate in a security context. Another factor to consider is technical capability. The expertise for inherently safer analyses resides in the business enterprises themselves with the technical and operations personnel who are intimately familiar with the technology, hazards, and overall risk of each process - and not in government.

For years, the Responsible Care® Process Safety Code has required consideration of inherent safety approaches. The ACC Responsible Care® Security Code additionally required members to consider inherent safety approaches to process design, engineering and administrative controls, and prevention and mitigation measures to address risks identified in the security vulnerability assessment. The security vulnerability assessment methodologies developed by the Sandia Laboratories and the Center for Chemical Process Safety, and used by ACC members, focus on intentional acts. These methodologies expressly require consideration of alternatives for safer technologies and chemicals. DuPont security vulnerability assessment teams include both security and process safety experts to ensure that both perspectives are considered at every site.

DuPont believes that inherently safer technology and chemicals are mainstream components of process safety and have a role to play as companies evaluate security. However, DuPont does not believe that inherent safety can, or should, be mandated by regulation. Previous testimony has discussed material substitutions at water and sewage treatment plants. This is a very straightforward and basic inherently safer application because it involves a simple mixing operation and no chemical reactions. These basic water and sewage treatment processes are very different from the complex processes at most chemical manufacturing plants. This complexity, along with the unique

nature of each process, means that companies need the flexibility to assess and decide options. Prescriptive inherently safer technology requirements are unworkable. As Chairman Collins stated in her closing comments at the last chemical security hearing, a risk-based approach will provide incentive to companies to consider inherently safer options as a means to move to a lower risk tier.

Chemical Sector Coordinating Council

I was also asked to comment on the Chemical Sector Coordinating Council, in my role as chair of this group.

Many across the chemical sector share the commitment to security. That is why, in June of last year, a group of 16 national chemical trade associations, with DHS' guidance, formed the Chemical Sector Coordinating Council (CSCC). President Bush, in Homeland Security Presidential Directive-7, encouraged formation of such sector-specific bodies to "(a) identify, prioritize, and coordinate the protection of critical infrastructure and key resources, and (b) facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices." The sector councils fulfill many of the operational roles that the Homeland Security Act establishes for private sector members of critical infrastructure.

While membership in the Chemical Sector Coordinating Council is composed of trade associations, DHS asked that an owner/operator representative serve as leader, or chair, of the Council to provide specific, front-line perspective and guidance. I presently serve in that capacity.

Members of the Chemical Sector Coordinating Council define the sector as "entities engaged in the production of chemicals, as well as those engaged in the storage, transportation, delivery and use of chemicals not adequately addressed by other critical infrastructure sectors." For example, it does not include water treatment facilities or transportation modes, both of which have separate and robust sector coordination mechanisms.

It is also important to note for the Committee what the Chemical Sector Coordinating Council is not. It is not a trade association, and there are no dues. The Council does not receive any federal funding – it is a sweat equity activity. Further, because it is an operational rather than an advisory body, the Council does not take policy positions. Each member association is responsible for developing and communicating its own policy positions and is free to develop independent relationships with DHS. So, for example, the Council will not take a position on any proposed legislation affecting security in the chemical sector.

In addition to serving as a routine information-sharing mechanism, the Council helped develop and ensure broad participation in a DHS-sponsored "tabletop

exercise” earlier this year; provided critical input to the development of a Terrorist Threat Reporting Guide for use by companies in the sector; participated in the recent TOPOFF-3 exercise; and is working closely with DHS to develop, refine and disseminate its “Risk Analysis and Management for Critical Asset Protection” (RAMCAP) methodology. RAMCAP will allow DHS to compare the vulnerabilities of disparate assets and resources against a series of benchmark threat scenarios, thereby enabling DHS to allocate protective resources rationally, on the basis of risk, across all critical infrastructures and key resources.

I’m pleased to report the Council enjoys a high level of participation and engagement from its member organizations and, after only one year of existence, has tackled a number of substantive subjects.

In closing my remarks, Madam Chair, I want to thank you and the members of the committee for allowing me to share what DuPont has done to build strong security systems and processes. We have very successfully integrated security responsibility and engagement into our culture. We also know there is more to do. We take very seriously the confidence and trust placed in us by the public and government. DuPont leadership is committed to continually strengthening security at our sites, in transportation, and along the value chain. We recognize that the security and safety of our operations are critical to our employees, our neighbors and, in fact, essential to the future of our company. Thank you for the opportunity to testify before the Committee on the important issue of chemical plant security. We appreciate the important work of this Committee and stand ready to work with you as you move forward.