

# **CBDAIF QUESTIONNAIRE RESPONSE SUMMARY**

**PROFESSIONAL SERVICES  
SECTOR**

**John Ferriter**

**September 27, 2007**

# Survey Results

- 7 Responses of 53 Companies surveyed
- Results summarized in good faith to reflect original input
- Individual contributions remain anonymous
- The opinions expressed have not been researched for accuracy and are not necessarily those of the presenter.

# What are the major benefits from such sales?

## Major benefits to our industry are the following:

- Sales to state and local governments expands the available market for a wide range of products – state and local grants from DHS / FEMA total over \$2B annually.
- Expands the market for DoD CBRN detection, security, and consequence management, with the potential result of more efficient production costs.
- Sustain/expand the Industrial Base, leverage technology where the DOD market does not justify up front investment.
- Maximizes interoperability between the DoD and non-military elements

# What are the major benefits from such sales?

## Major benefits to DoD are the following:

- Commonality of equipment allows better integration of response involving local, state and federal agencies in major CBRN terrorist attack or incident
- Significant effort to open state and local markets for sale of DoD CBRN equipment, systems, designs will result in lower costs

## Major benefits to state and local governments:

- Access to state-of-the art CBRN equipment, systems, designs that will contribute to prevention, protection, deterrence, response, mitigation, and recovery
- Commonality will enhance integration of assets, response, resupply and reconstitution
- Access to Service Oriented Architecture (SOA) instrumentation to effectively perform their Homeland Security mission
- Ability to leverage DoD expertise, technology, and purchasing power
- Failure to tap DoD expertise may result in unnecessary cost, effort, and frequently “reinvention of the wheel”

**Are you aware of such sales that have been successful or viewed as beneficial to the state and local government? If so, please provide a short summary and why it is an example of a success.**

- Many state and local government agencies have for years procured MIL-SPEC CBRN Individual Protection equipment for applications that overlap various DoD missions.
- The sale of equipment and systems used by DoD is common – much of the DoD equipment have become Commercial Off The Shelf and available to state and local governments.
- From the perspective of the state and local agencies, this leverages DoD technical developments.

## What are the major risks or impediments for such sales?

- Use of CBRN equipment requires appropriate and continuous training
- Perception in the private sector that there is a safety level that really does not exist
- Most CBRN gear needs to be used in conjunction with complimentary equipment.
- Shelf life concerns
- Potential for loss of critical US technology to adversaries
- Lack of coordination between DoD and non-DoD agencies and organizations with respect to:
  - Operational requirements,
  - Scientific data,
  - Test methods,
  - CBRN terrorist threat scenarios
  - Individual protection requirements
  - Standards

## What are the major risks or impediments for such sales?

- Discordant/inappropriate Homeland Security standard-setting activities:
  - Lack of standards coordination results in different solutions for identical threat and operational scenarios.
  - Unscientific and operationally flawed Homeland Security standard-setting activities may drive DoD equipment standards and needlessly degrading operational capabilities
  - Not drawing upon DoD's unique combination of technical and operational expertise
  - Tragic loss for DoD, and for the security of the country.
- DoD CBRN technology will be in the virtually open marketplace, which could lead to compromise of CBRN technology to other nations
- Concerns are greatest for private sector applications; somewhat mitigated for State and Local Governments
- State & local governments do not have the same financial resources as the federal government

**Are you aware of any failures or any such sales that presented significant challenges? If so, please provide a brief summary**

- The InterAgency Board for Equipment Standardization adopted certain National Fire Prevention Association Standards for equipment to be used by First Responders to chemical / biological terrorist incidents.
  - The DHS accordingly has limited the availability of federal grant funding to equipment that meets NFPA standards.
  - No MIL-SPEC ensembles conform to the NFPA standards, which include requirements recently acknowledged to be arbitrary and not based on relevant threat analyses.
- Law enforcement end users no longer are able to obtain DHS grant funding to replenish their MIL-SPEC ensembles inventories or outfit new teams.
- Law enforcement procures HAZMAT-type equipment considered by some as impractical and dangerous for their particular missions.

## How would you assess the liability concerns from such sale?

- Liability risks are greater in the Homeland Security sector limiting the range of available equipment
- Unlike the federal government, state and local governments could and probably would seek damages from industry for training accidents and other misuse by employees.
- Civilian personnel have false sense of CBRN protection due to:
  - Lack of operational training
  - Incomplete ensembles
  - Shelf life management issues
- Risk of the public being injured through the use/misuse of the equipment

# What action(s) could be taken to mitigate liability?

- Training and sustainment for proper use and maintenance
- The U.S. Government could either:
  - (a) broaden the coverage available under the Safety Act, by eliminating many of the limitations that effectively preclude qualification of most existing CBRN equipment; or
  - (b) take steps to make Product Liability insurance more readily available at costs that are not prohibitive.
- There is very little that state and local governments could do alone
- Strict enforcement of ITAR regulations to limit risk of technology loss

# What protection is provided by the SAFETY Act or other risk mitigation means?

- Provides some measure of protection for companies against undue claims on perceived expectations of performance of counter-terrorism technologies
- Broad liability claims resulting from terrorist activities might include technology companies whose technologies are part of Homeland Security solutions and who might be subject to substantial legal fees or claims, even though the product has performed as warranted on a component basis.
- The Safety Act needs to be expanded for other than terrorists incidents to protect a company from law suits resulting from use. The law needs to place the responsibility on the plaintiff to prove the equipment was faulty for the purpose it was designed and built, and relieve the company from proving its equipment is safe.