DEFENSE INDUSTRIAL BASE SECTOR COORDINATING COUNCIL

Improving the Sharing and Reliability of Public and Private Threat and Hazard Information

April 9, 2008

Panel Objectives/Takeaways

- Objectives
  - Exchange information
  - Discuss gaps and opportunities for better provision/utilization of global threat and natural disaster intelligence
  - Explore case studies, best practices, and successful strategies for combating and understanding the insider threat
  - Identify opportunities for public/private intelligence sharing partnerships
- Takeaways
  - Information sharing, integration mechanisms, and how they enhance rapid response

NIPP Implementation Actions

“The effective implementation of the NIPP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to CI/KR and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced.”

NIPP implementation will rely greatly on critical infrastructure information provided by the private sector. Much of this is sensitive business or security information that could cause serious damage to companies, the economy, and public safety or security through unauthorized disclosure or access to this information

Improving Information Sharing

- Numerous models of mechanisms that work …
  - Google “Info Sharing” 20,400,000 hits
  - Google “Trust Models” 2,730,000 hits
- Implies “no ideal”
  - Contemporaneous venues with similar objectives are okay
  - Helps bridge blockers
  - Cues parties to desired common solution
  - Enriches information streams
  - Builds relationship opportunities
    - Dialogue between DIB and DoD
- Gaps
  - Includes policy, classification, communication system issues
  - Issues enhance or impede key “lubricants”
    - Trust, confidence, shared equity

Business Structure

- DIB companies have grown to large entities through the acquisition process
- Many unknowns come into play
  - Policy differences
  - Cultures
  - Vetting procedures
  - Foreign connections
  - Organizational control

CI Strategy for Business

- Companies must realize they have a real threat present
- Senior Management must support the CI effort or it will not work
- Awareness of the workforce is key to success
- Have a CI program in place with trained personnel to manage it

Government Interface with the DIB

- Not all companies are managed the same in regards to security
  - Legal Department
  - Human Resources Department
  - Operational Management
- Be aware all have their own equities to protect

Government Interface

- Important to establish key relationships early
- Ensure “hand-offs” are handled appropriately
- Attempt to limit the amount of agents dealing with a particular firm, i.e., cyber, humint, etc.
- If possible, manage interface through the senior security official
- Offer various support assistance to firm

Issues remaining

- Lack of collection capabilities
- Lack of efficient means of secure data access and dissemination
- Training, investigative resources
- Duplications of efforts (multi-agency overlap)

Cyber Issue

- #1 issue facing industry
- Lack of convergence between security and IT functions exist in some companies
- Being treated as an “Information Assurance” issue, not as an “Intelligence” issue
- No real solutions being developed to halt threat as long as firms continue to operate and store data connected to the internet