Examining The Boundary where Governmental, Civilian and Military Security Needs Meet

May 17, 2005

J. Iffland, BG
USAF (Ret)
Security of National and State’s Critical Infrastructure is Crucial in all Governmental, Commercial and Private Endeavor.
Challenge 1

Example Infrastructure Requiring Security

- Government Centers
- Financial Centers
- Refineries and Distribution Lines
- Power Supply and Transmission Lines
- Key and Secondary Roads, Ports, Airports
- Communications Hubs
- Emergency Responder Centers
- Military Bases and Command Centers
- Security Command and Control Centers
- Weapons Storage

The Challenge is What, When and How to Integrate Independent Infrastructure, Information, and Data - THEN PROTECT IT.
Challenge 2

Example Security Means

- Physical Security
  - Fencing
  - Ingress Barriers and Alarms
  - Security Zones
  - Entry / Exit Controls
- Information Safeguarding
  - Awareness Programs
  - Locked Storage
  - Secure Transmissions
- Work Force Selection
  - Background Checks
  - INS Clearance for Foreign National Workers
- Centralized Security Centers
  - Personnel - Access Control
  - Building and Facility – Monitor

The Challenge is What, When and How to Integrate the Security Means – HARDENING OUR TARGETS, INFORMATION ASSURANCE, AND DATA FUSION
Focus of Today’s Short Presentation

Examining the Boundary (Physical Demarcation) where Crucial Governmental, Civilian and Military Security Needs Meet
The Boundary

The Boundary where Governmental, Civilian and Military Security Needs Meet -

- Porous Boundary, a Jurisdictional Division and often immediately adjacent to a Civilian Community
- Experiences a Mix of Traffic to / from Military Facilities and Installations (Military / Civilian Personnel; Vehicles etc.)
- Water and Power most commonly supplied across the Boundary by Local / Regional Suppliers
- Communications Routinely cross the Boundary via leased Land Lines
- The Boundary requires 24 / 7 Security
The Boundary

Companies are providing new and innovative products and means that help address Security Needs at the Boundary:
The DOD and DHS can Assist these Companies by constantly evaluating their Installation’s Boundary Security from the Opposition’s Strategic and Tactical View Point i.e. as a “Red Team”.

The Boundary
The Government must apply their knowledge of Strategy and Tactics as a **Red Team** applied to Three Key Areas of the Assessment and Design Model:

- **Facilities / Assets**
- **Threats, and**
- **Vulnerabilities**
The Boundary

Industry must be the Technology Leader and Answer Cost / Benefit questions AND Government Agencies must set the Operational Requirement to Drive Technology

Let’s look at an Industry Assessment and Design Model

and overlay an Example Government Contribution
Assessment and Design Model

1. Assess Assets
2. Assess Threats
3. Assess Risks
4. Design Security Architecture
5. Make Decisions
6. Monitor

Government Requirement ➔

People ➔

Process ➔

Technology ➔

Cost Analysis ➔

Benefits Analysis ➔

Credit to: EWA/IIT and Horizon Safety and Security LLC
The Boundary

“Entry Points” can help direct Government and Industry in Development of Standardized Assessment Metrics

- **Assess Assets**: What Assets exist on the Installation? What Tactic(s) may be employed to attack?
- **Assess Threats**: What Threat exists may attack the Installation? What Tactic(s) may the threat employ?
- **Assess Vulnerabilities**: What are the Vulnerabilities within the Boundary? Power / Water Supplies; Work Force Access. What are the Vulnerabilities?

People

Process

Technology
The Boundary

In Summary to this short Presentation, I submit:

The Boundary between Governmental, Civilian and Military Properties is where Crucial Security Needs Meet and Must be Met, and that:

ANSI’s HSSP is on the Proper Track – Standardized Models need to be carefully developed, verified and validated to bring to bear all that technology can offer.