NIAC
Evaluation and Enhancement of Information Sharing and Analysis (EEIS)

Final Report and Proposed Recommendations

April 13, 2004

Tom Noonan
President, Chairman and CEO
Internet Security Systems, Inc.
tnoonan@iss.net

Presentation Outline

- Charter
- Methodology
- Areas for Review
- Findings – Facts
- Findings – Issues
- Proposed Recommendations
- Participants
- Requests of the NIAC

Charter

- NIAC established the Evaluation and Enhancement of Information Sharing and Analysis in April 2003
- Tasks: to analyze the current environment for information sharing and analysis across the critical industry sectors and make recommendations to the government regarding enhancements, increased effectiveness and broader influence across industry sectors

Methodology

- Leverage existing ISAC analysis/findings
- Review existing ISAC organization, funding models, membership, and challenges
- Review government information sharing organizations
- Review GAO and other reports on critical infrastructure information sharing
- Identify funding options and incentives to gain ISAC participation of all owners/operators in each sector

Areas for review

- Establish objective-focused groups:
  - Business models for sharing and analyzing information
  - Financial models for supporting information processes
  - Level of information analysis and aggregation
  - Dissemination breadth and coverage

Findings - Facts

- Significant Changes in the landscape
  - Release of HSPD 7 and 8
  - DHS has significant staffing and procedural development
  - Major ISACs have formed the ISAC Council with eight White Papers written
  - ISAC Restructurings
  - Sector Coordinators now have more formal working relationship
- Coordination between DHS, ISAC Council and Sector Coordinators is quickening

Findings – Facts (2)

- Information Sharing has many levels
  - Strategic
  - Operational
  - Tactical
- Information Sharing has many elements:
  - Vulnerability Information
  - Exploits
  - Threats
  - Incidents
  - Best Practices
  - Early Warning System

Findings – Facts (3)

- Two levels of Private Sector delivery:
  - Critical Infrastructures
  - Non-Aligned Businesses
- Cross-Sector Operations between ISACs have begun on their own initiative
- ISAC Operations are communicating with DHS and their lead Agencies
- ISACs are at differing levels of maturity

Findings – Issues

- Information Sharing is clearly needed and Must be More Effective
  - Definitions are necessary
    - i.e. ISAC; Critical Infrastructure
  - Roles need to be more clearly defined (i.e. Sector Coordinators to ISACs and to Government)
- Various Business Model Frameworks
  - Associations
  - Government-centered
  - Market-driven

Findings – Issues (2)

- ISACs can provide unique sector analysis and research
  - Private Sector Owner/operators understand their unique operational problems
  - Private Sector analysis grows with trust and communication – focused primarily on Sector vulnerabilities (operational)
  - Able to provide more than just raw data – finished products – must understand Government requirements for analytical products

Suggested ISAC Maturity Model

Maturity >> Dimension	Level 1 Framework and Policies Established	Level 2 Procedures Developed	Level 3 Procedures for Communications and Responses Implemented	Level 4 Procedures and Responses Tested	Level 5 Procedures, Communications and Reponses are Integrated Cross-Sector
Vulnerability Analysis	Identified	Defined	Distributed – Primarily Alerting	Impact Advice and Mitigations Available	Trend Analysis and Cross-Sector Integration
Threat Analysis	Identified	Defined	Distributed – Primarily Alerting	Impact Advice and Mitigations Available	Trend Analysis and Cross-Sector Integration
Cross-Sector Coordination	None	Some	Moderate – 30% to 50% of Sector Participation	Majority of Sector Participates	Cross-Sector Integration
Data Availability – real time flow	Little Except Vendor-Specific	Some	Can Be Collected From Sector and Vendors	Readily Available	Standard Repository and Analysis Available
Response Time	Uncertain	Key Enterprises Can Prevent or Diminish Impacts	Most Sectors can Diminish Impacts Quickly	Most Threats Have Little or Localized Impact	Anticipates Emerging Threats

Proposed Recommendations

1. Adopt the following roles for ISACs and Sector Coordinators
   - The Information Sharing and Analysis Centers (ISAC) should be the central source in each sector for dissemination, sharing and communications of information on cyber, physical, and all threats, vulnerabilities and incidents in order to defend the critical infrastructure.
   - Sector Coordinators should work Policy development and sector wide vulnerability analyses for risk mitigation

Proposed Recommendations (1 cont)

- Joint work with the Private Sector to:
  - Further refine the Role and responsibilities of the Sector Coordinator
  - Further refine the Relationship of the Sector Coordinator to the ISAC
  - Establish criteria to determine if Critical Infrastructure (sector) or Key Asset meets the definition in the PATRIOT Act

Proposed Recommendations (cont.)

2. Enhance Private Sector ISAC Reach
   - Assist ISACs in delivering basic Alerts and Advisories to their sectors
   - Sponsor ISAC Operations and Leadership Security Clearances
   - Provide Sector Specific and Broad Based Strategic Information thus increasing ISAC value and government communication

Proposed Recommendations (cont.)

3. Incorporate the strengths of the Private Sector Analysis and Focus with the Reach and Communication for Alerting from Government in a two tier information node
   - General Alerts and information (Reach)
     - Good across all sectors
     - Provides warning and notices to Private Sector
   - Sector Specific Alerts and Analysis (Analytical)
     - Detailed information from the Government
     - ISAC Analysis Derived Specific info to the Sector, or across Sector and/or to the Government

Proposed Recommendations (cont.)

4. Provide for timely flow of unique Private Sector information to Government
   - Sector-specific analysis of unique data can become actionable intelligence
   - Sectors often house the only means to take action during incidents
   - Concept of Government as "supported organization"

Participants

- Working Group Chair:
  - Tom Noonan, Internet Security Systems, Inc
- Study Group members: ISS, Wells Fargo, EDS, Union Pacific, Inter-Con Security Systems, V-ONE, NERC, SIAC, ConocoPhillips, Cisco, Symantec, DuPont, US CoC, and IAIP

Requests of the NIAC

- Approve EEIS report
  - Discuss any changes and agree
  - Working group will make modifications as required
- Approve letter submitting report to President