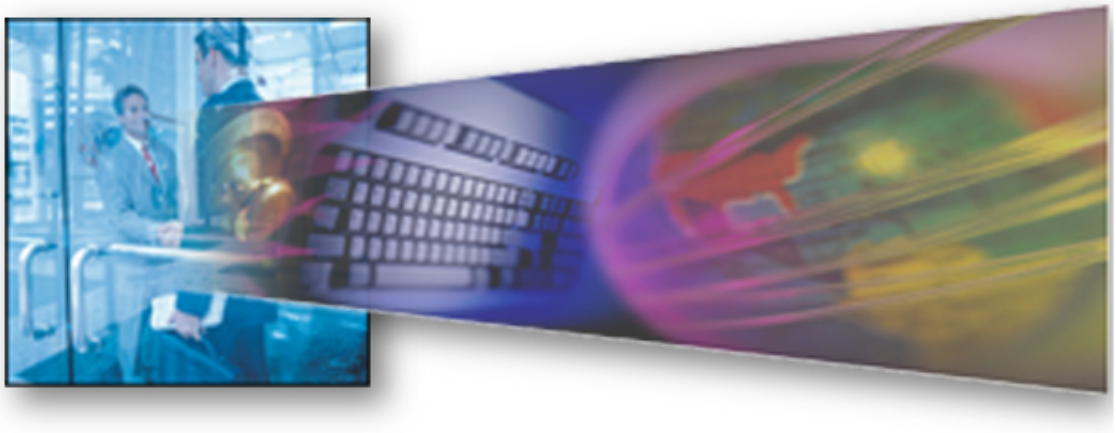


Information Sharing and Analysis Center (ISAC)

The Benefits of Information Sharing for FIRST

October 2004

Errol S. Weiss

http://home.comcast.net/~errol/isac.ppt

What is an ISAC?

- Information Sharing and Analysis Center
- Designed for Information Sharing
- Mechanism for Analyzing, Sanitizing, & Disseminating Private Sector Information
- Created in 1998 as a Public / Private Partnership with and for Critical Infrastructures to address “cyber-terrorism”

Critical Infrastructures

- Defined as businesses, organizations, and mediums that support our way of life.

- Agriculture
- Banking & Financial
- Chemical & Hazardous Materials
- Defense Industrial Base
- Emergency Services
- Energy
- Food
- Government
- Information & Telecommunications
- Postal & Shipping
- Public Health & Healthcare
- Transportation
- Water

Why an ISAC?

- 85% Critical Infrastructure Owned/Operated by the Private Sector
- Designed and Developed by Sector Professionals
  - 1998: Public/Private Sector Partnership to Protect the Critical Infrastructure
  - 2003: Updated and Re-enforced mission
- ISAC Mission - Disseminate ***trusted*** and ***timely*** security risks and information
- ISAC - Managed by Sector Security Professionals
  - Most have a Board of Managers or Directors
  - Most are owned and operated by the private sector

ISAC Components

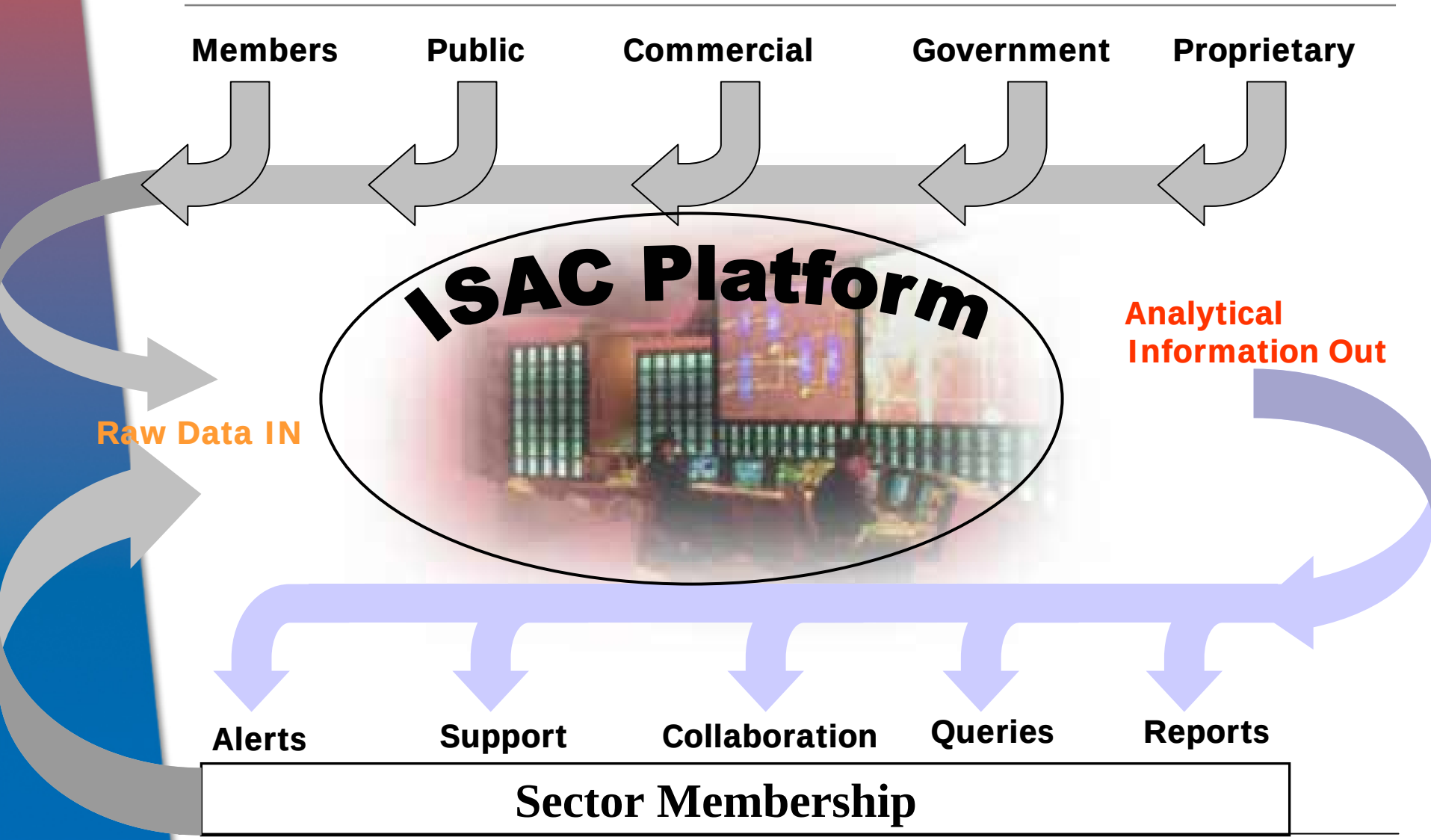
What comprises a typical ISAC? (Outside of its members)

- **People**
  - ISAC Analysts
  - Subject Matter Experts in the areas of interest
    - Cyber / IT
    - Physical
    - Bio-Terrorism
    - Geopolitcal
- **Processes**
  - Membership and vetting
  - Funding
  - Intelligence Collection
  - Analysis
  - Content development
  - Facilitation of Sharing
  - Third Party SME relationship
- **Technology**
  - Secure Knowledge Management Framework (Portal)
  - Communications
  - Information Store
  - Notification systems

How does an ISAC work?

- Security professionals anonymously share information
  - Threats
  - Vulnerabilities
  - Incidents
  - Solutions
- Members voluntarily contribute to the ISAC on either an anonymous or attributed basis
- Inputs are analyzed by security specialists and SME's
  - Trends
  - Solutions
  - Risk

How ISACs Work



Portal Components

- Cyber Security
  - Vulnerabilities
  - Threats
  - Incidents
- Physical Security
  - Regional Intelligence
  - Travel (World) Advisories
  - Incidents
  - Benchmarking & Best Practices
- Member Submission Forms
- Collective Intelligence
  - Weekly Intelligence Report
  - DHS Daily Report
  - ISAC Meeting Minutes
  - ISAC User Guides
  - White Papers
- Announcements
- Secure Collaboration
  - Discussion Forums
  - Secure Chat
- Advisory Logs

- Portal framework is content-independent
  - Able to handle cyber, physical, subject of interest …
- Granular access control and distribution mechanisms
  - Content can be shared as defined by the user and the content custodian
  - Allows for user to receive only the information they want, and allows for information owners to control information dissemination

ISAC Benefits for FIRST

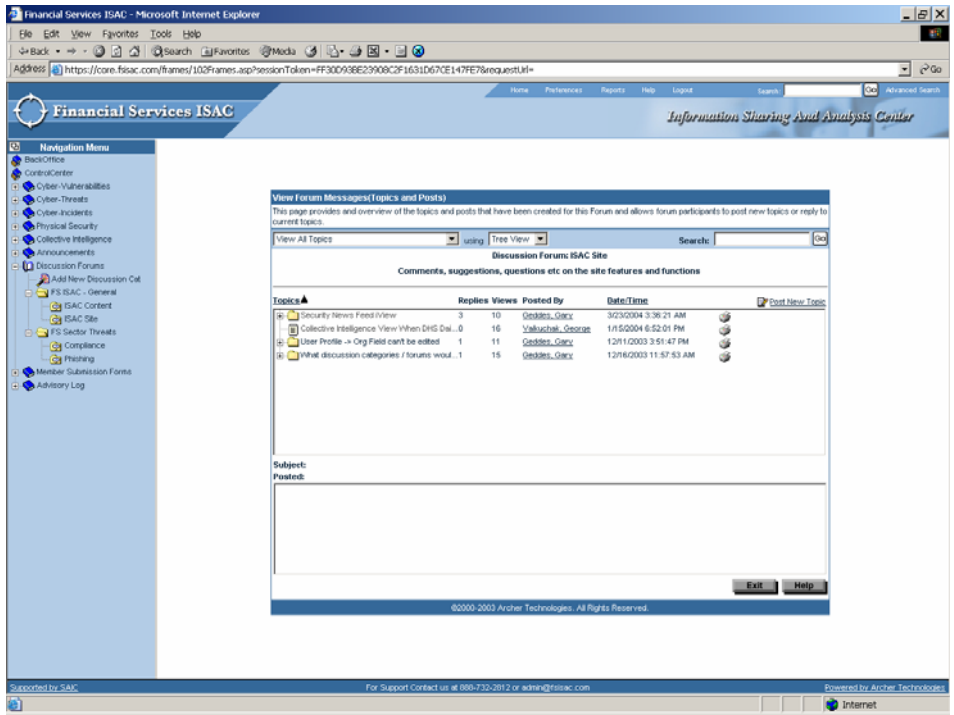
- Members take advantage of industry specific risk information
  - Security Threats
  - Vulnerabilities
  - Incidents
- Confidential venue for sharing security threats, vulnerabilities and solutions.
- Facilitates trust among participants
- Members benefit from the ISACs unique proactive means of mitigating cyber-security risks
- Participation makes each organization stronger and safer

ISAC Benefits for FIRST

- **Anonymous Information Sharing**
  - Members submit information without revealing their identity
  - ISAC facilitates cooperation while protecting proprietary interests
  - Facilitates information sharing and participation

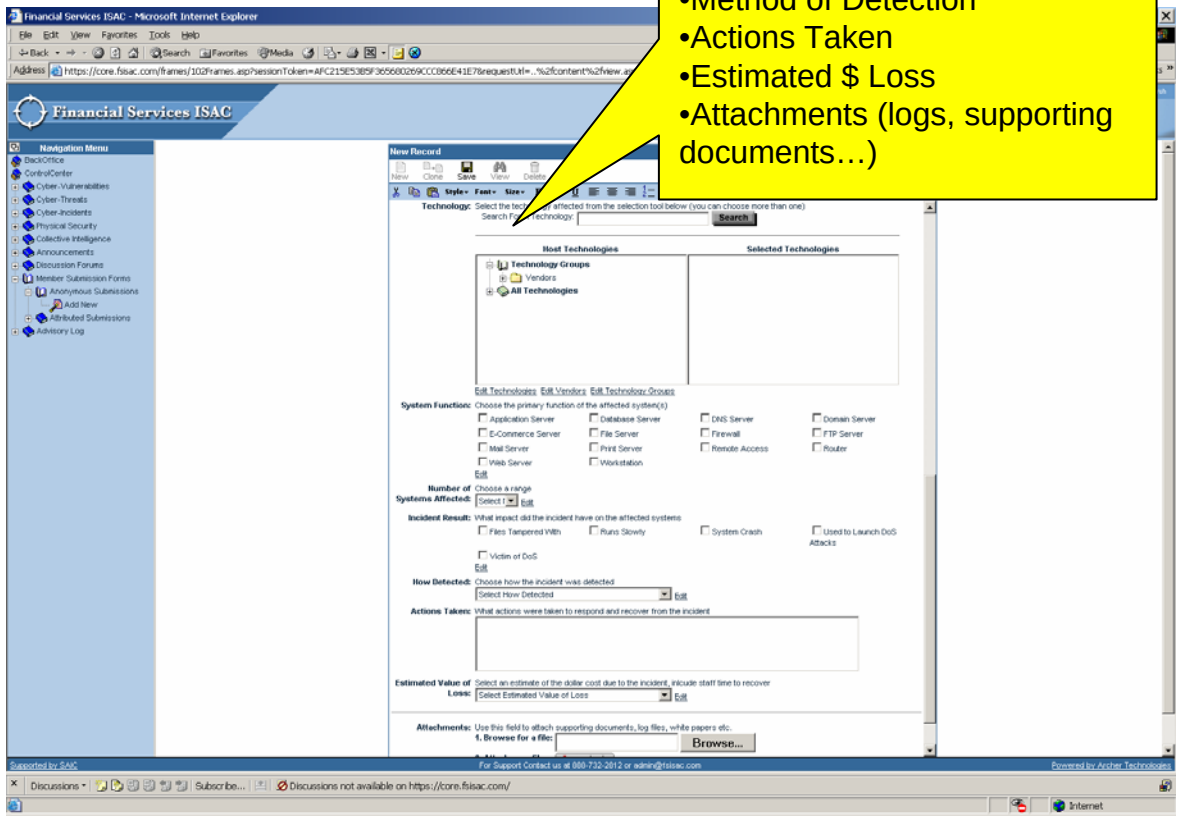
ISAC Benefits for FIRST

- **Secure Collaboration**
  - Enables the members to quickly get together to address or further understand breaking issues
    - Secure Chat
    - Protected Chat Rooms
    - Discussion Forums
    - File exchange
    - Communities of Interest on-demand
  - Establishes targeted communities of interest
  - Overcomes problems associated with list servers



ISAC Incident Analysis Process

- **Incident Submission**
- **Analyst Reviews**
- **Posting**
- **Notification**



- Technology Affected
- System Functions
- Number of Systems Affected
- Incident Result
- Method of Detection
- Actions Taken
- Estimated $ Loss
- Attachments (logs, supporting documents…)

Analyst Review Process

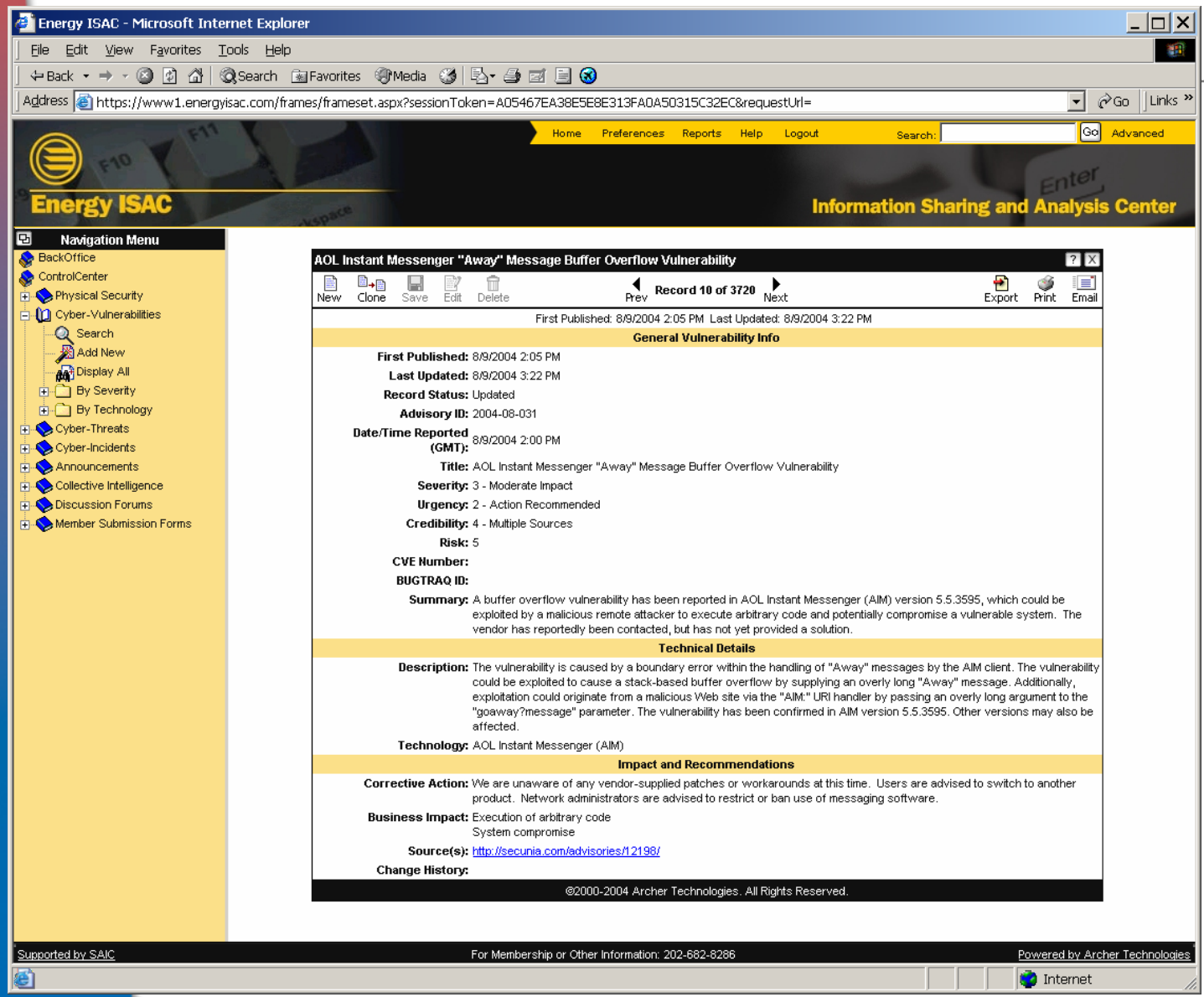
- Submission enters secure workflow queue
  - Incident Sanitization
  - Validation
- Workflow routes submission to appropriate subject matter expert
  - Technology
  - Cyber
  - Physical

Analyst Review Process (cont'd)

- Severity
- Urgency
- Credibility

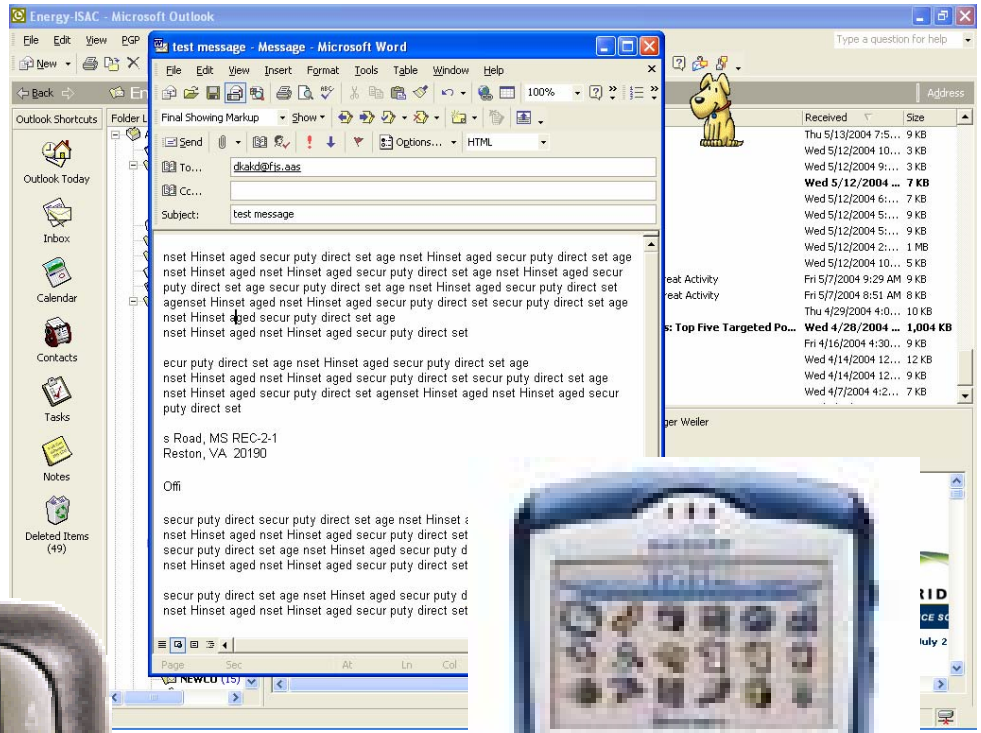
- Risk
  - 10 – Crisis
  - 9 – Urgent
  - 8 – Urgent
  - 7 – Normal
  - 6 – Normal
  - 5 – Normal
  - 4 – Normal
  - 3 – Normal
  - 2 – Normal
  - 1 - Informational

Posting



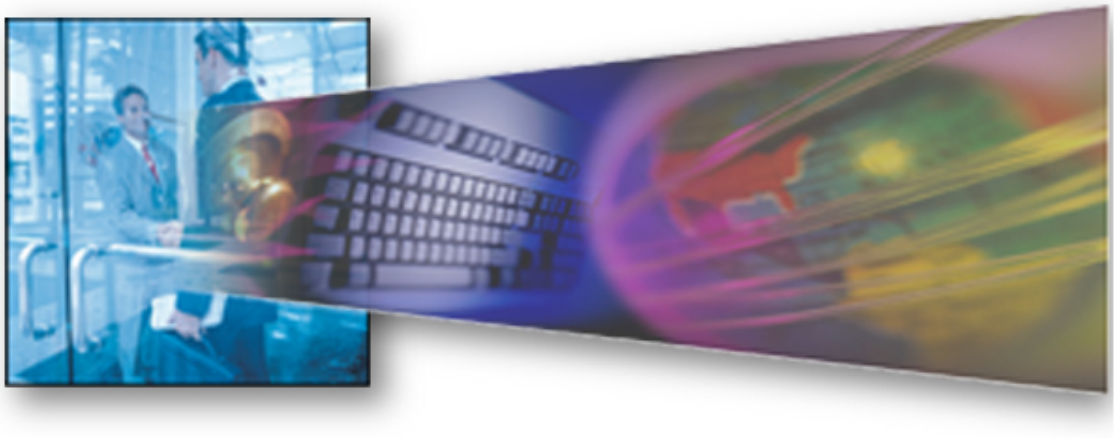
Notification

- E-Mail
- Pager
- Text Enabled Cell Phones
- PDAs
- SMS



Conclusions

- Information Sharing and Analysis Centers
  - Promotes information sharing
  - Facilitates collaboration amongst disparate groups with a common cause
- An ISAC structure can enhance the ability of FIRST
  - Distribute advisories
  - Securely share incident details
  - Establish a secure collaborative on-line environment



Questions / Next Steps?

Errol S. Weiss
Deputy Director of Managed Security Services
SAIC, Enterprise Security Solutions Business Unit
703-375-2222
WeissE@saic.com

About SAIC

Science Applications International Corporation

- Founded in 1969; Headquartered in San Diego
- Largest Employee-Owned Consulting, Engineering, and Advanced Technology Organization in the U.S.
- Fortune 500® Company, ranked 288, Fortune (04/03)
- $6.1B in Annual Revenue
- 44,000+ employees in over 150 cities worldwide
  - Environment, Energy, National Security, IT Outsourcing, Telecommunications, Health Care
- World-Class Information Systems, Integration, Knowledge Management
  - Largest Private IT Company in the U.S. (Business Week, 06/02)
  - 4th Largest Systems Integrator in the U.S. (Int'l Data Corporation (03/01)
- Leader in Security and Homeland Defense