



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
 - Geopolitical

➤ Processes

- Membership and vetting
- Funding
- Intelligence Collection
- Analysis
- Content development
- Facilitation of Sharing
- Third Party SME relationship

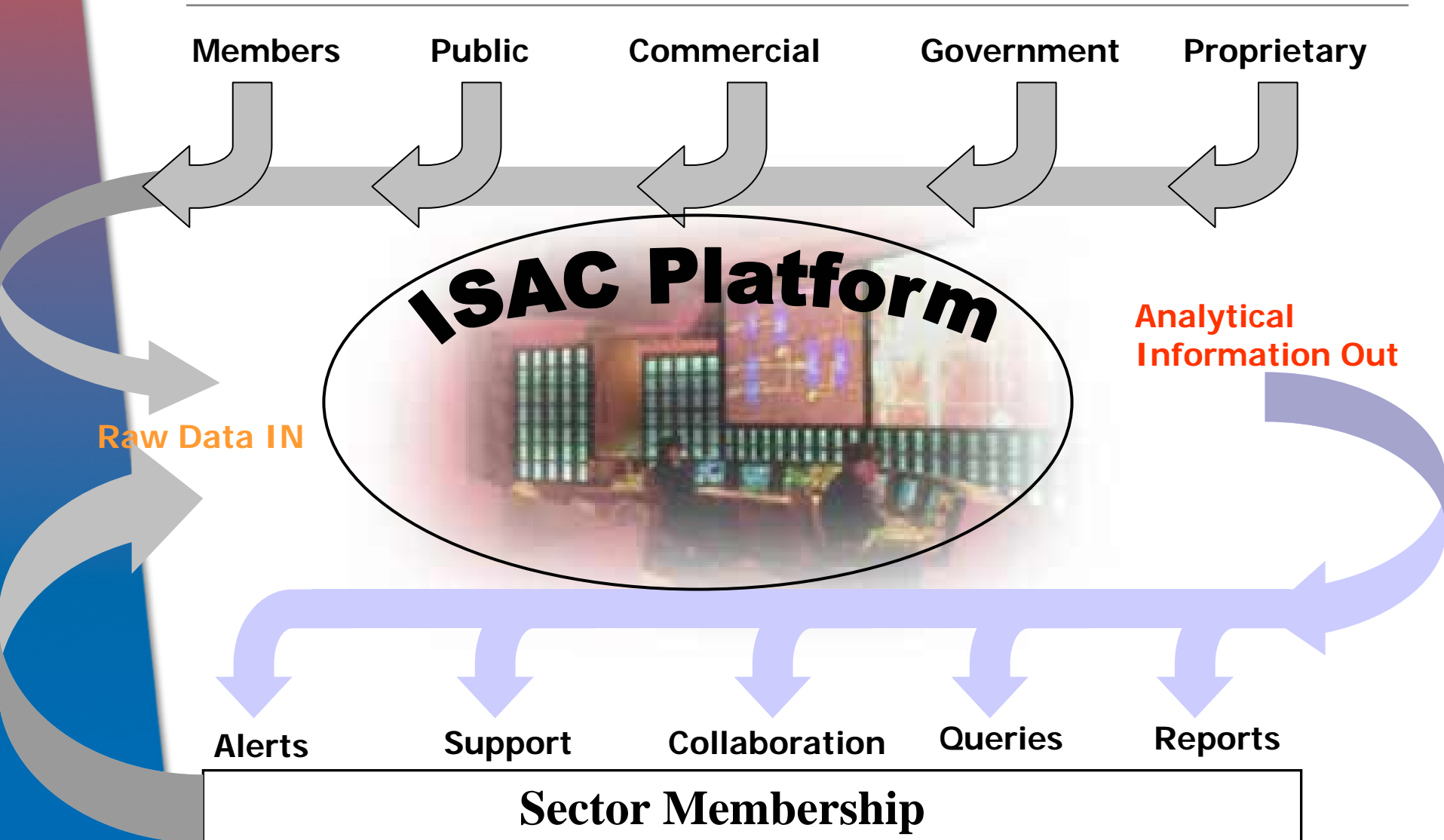
➤ Technology

- 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

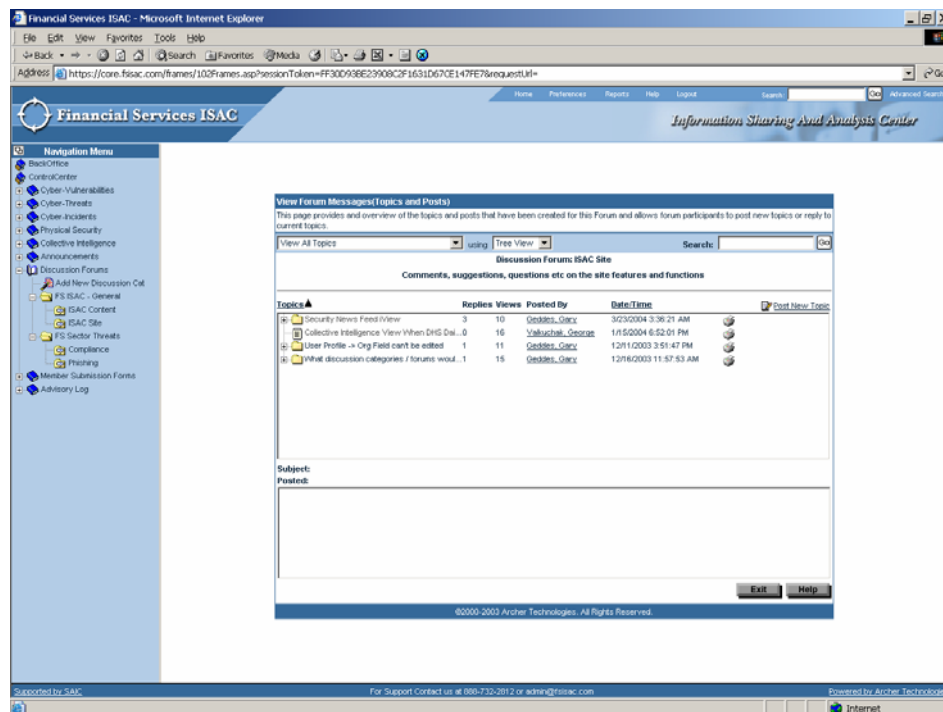
➤ **Anonymous Information Sharing**

- **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...)

The screenshot shows the 'Financial Services ISAC' website in a Microsoft Internet Explorer browser. The page title is 'New Record'. The left sidebar contains a 'Navigation Menu' with items like 'BackOffice', 'ControlCenter', 'Cyber Vulnerabilities', 'Cyber Trends', 'Cyber Incidents', 'Physical Security', 'Collective Intelligence', 'Announcements', 'Discussion Forums', 'Member Submission Forms', 'Anonymous Submissions', 'Add New', 'Attributed Submissions', and 'Advisory Log'. The main content area is a form with the following sections:

- Technology:** A search box for technology groups and vendors, with a 'Search' button.
- System Function:** A grid of checkboxes for system functions: Application Server, Database Server, DNS Server, Domain Server, E-Commerce Server, File Server, Firewall, FTP Server, Mail Server, Print Server, Remote Access, Router, Web Server, and Workstation.
- Number of Systems Affected:** A dropdown menu to 'Choose a range'.
- Incident Result:** A grid of checkboxes for incident results: Files Tampered With, Runs Slowly, System Crash, Used to Launch DoS Attacks, and Victim of DoS.
- How Detected:** A dropdown menu to 'Select How Detected'.
- Actions Taken:** A text area for describing actions taken to respond and recover from the incident.
- Estimated Value of Loss:** A dropdown menu to 'Select Estimated Value of Loss'.
- Attachments:** A text area for attaching supporting documents, log files, and white papers, with a 'Browse for a file' button.

At the bottom of the page, there is a footer with contact information: 'Supported by SAIC' and 'Powered by Aclara Technologies'. A status bar at the very bottom indicates 'Discussions not available on https://core.fsaisac.com/'.

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

Energy ISAC - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address <https://www1.energyisac.com/frames/frameset.aspx?sessionToken=A05467EA38E5E8E313FA0A50315C32EC&requestUrl=> Go Links

Home Preferences Reports Help Logout Search: Go Advanced

Energy ISAC Information Sharing and Analysis Center

Navigation Menu

- BackOffice
- ControlCenter
- Physical Security
- Cyber-Vulnerabilities
 - Search
 - Add New
 - Display All
 - By Severity
 - By Technology
- Cyber-Threats
- Cyber-Incidents
- Announcements
- Collective Intelligence
- Discussion Forums
- Member Submission Forms

AOL Instant Messenger "Away" Message Buffer Overflow Vulnerability

New Clone Save Edit Delete Prev Record 10 of 3720 Next Export Print Email

First Published: 8/9/2004 2:05 PM Last Updated: 8/9/2004 3:22 PM

General Vulnerability Info

First Published: 8/9/2004 2:05 PM
Last Updated: 8/9/2004 3:22 PM
Record Status: Updated
Advisory ID: 2004-08-031

Date/Time Reported (GMT): 8/9/2004 2:00 PM
Title: AOL Instant Messenger "Away" Message Buffer Overflow Vulnerability
Severity: 3 - Moderate Impact
Urgency: 2 - Action Recommended
Credibility: 4 - Multiple Sources
Risk: 5

CVE Number:
BUGTRAQ ID:

Summary: A buffer overflow vulnerability has been reported in AOL Instant Messenger (AIM) version 5.5.3595, which could be exploited by a malicious remote attacker to execute arbitrary code and potentially compromise a vulnerable system. The vendor has reportedly been contacted, but has not yet provided a solution.

Technical Details

Description: The vulnerability is caused by a boundary error within the handling of "Away" messages by the AIM client. The vulnerability could be exploited to cause a stack-based buffer overflow by supplying an overly long "Away" message. Additionally, exploitation could originate from a malicious Web site via the "AIM:" URI handler by passing an overly long argument to the "goaway?message" parameter. The vulnerability has been confirmed in AIM version 5.5.3595. Other versions may also be affected.

Technology: AOL Instant Messenger (AIM)

Impact and Recommendations

Corrective Action: We are unaware of any vendor-supplied patches or workarounds at this time. Users are advised to switch to another product. Network administrators are advised to restrict or ban use of messaging software.

Business Impact: Execution of arbitrary code
System compromise

Source(s): <http://secunia.com/advisories/12198/>

Change History:

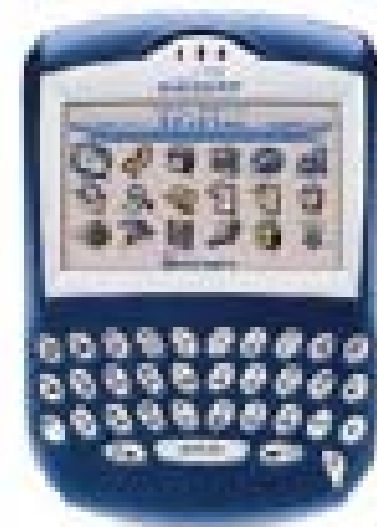
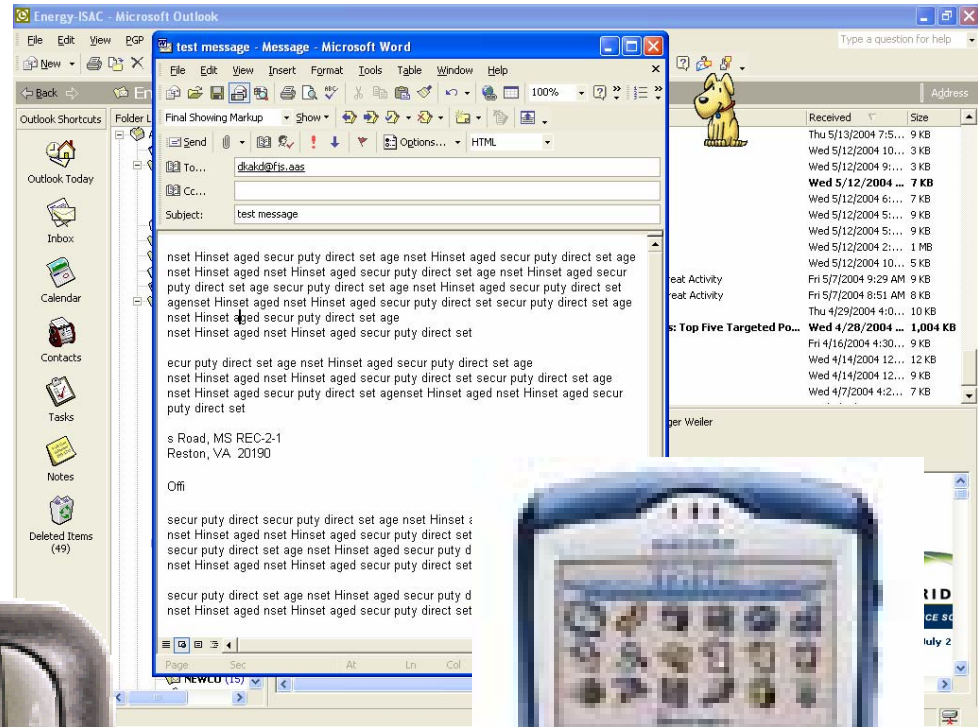
©2000-2004 Archer Technologies. All Rights Reserved.

Supported by SAIC For Membership or Other Information: 202-682-8286 Powered by Archer Technologies

Internet

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**