Situation Awareness Implementation Considerations

SAND2008-5840C

NWS Security Summit
Oak Ridge, TN
10 September 2008

Daniel A. Pritchard

Sandia National Laboratories
Security Systems and Technology Center
Albuquerque, NM

UNCLASSIFIED UNLIMITED RELEASE

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, or the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Briefing Outline

- Definition
  - What is Situation Awareness, anyway?
  - Who (or what) “talks” to whom?
  - When, how and what do they say?
- Design
  - Data vs. Information
  - Tactical vs. Emergency Operations
  - Inner Focus vs. Outer Focus
- Deployment
  - Architecture for Implementation
  - Cross-Domain Issues and Interoperability
- ‘Da End’

DEFINITION

"*Situation Awareness* is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" Endsley, 1988

- Level 1: ***Perception***

  WHO IS WHERE?

- Level 2: ***Comprehension***

  WHAT ARE THEY DOING?

- Level 3: ***Projection***

  WHAT WILL THEY DO?

Inherent in this definition is a notion of what is important.

Who is where, what are they doing and what will they do?

- Using the DoD Architecture Framework, these can be identified and documented
- Typical DoDAF diagrams include
  - Operational Activity Model (OV-5)
  - Organizational Relationships chart (OV-4)
  - Operational Event-Trace Description (OV-6c)
  - Operational Information Exchange Matrix (OV-3)

Operational Activity Model (OV-5) Example 1: Off-Site Event

Early Warning
(Bomb Threats, etc.)

1. Early Warning Alert

3. Coordination

Fusion Center

2. Investigation

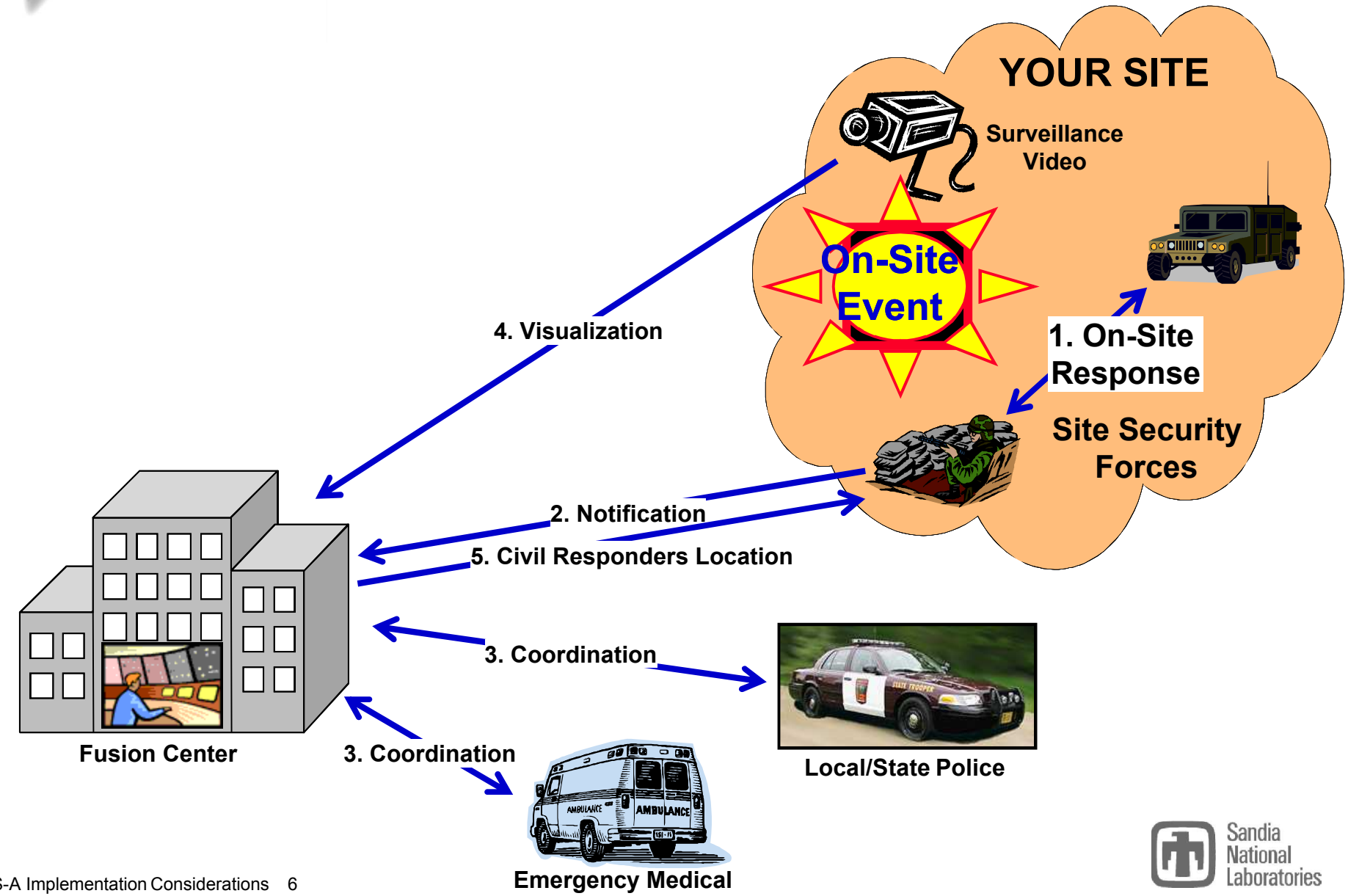
Local/State Police

3. Coordination

Emergency Medical

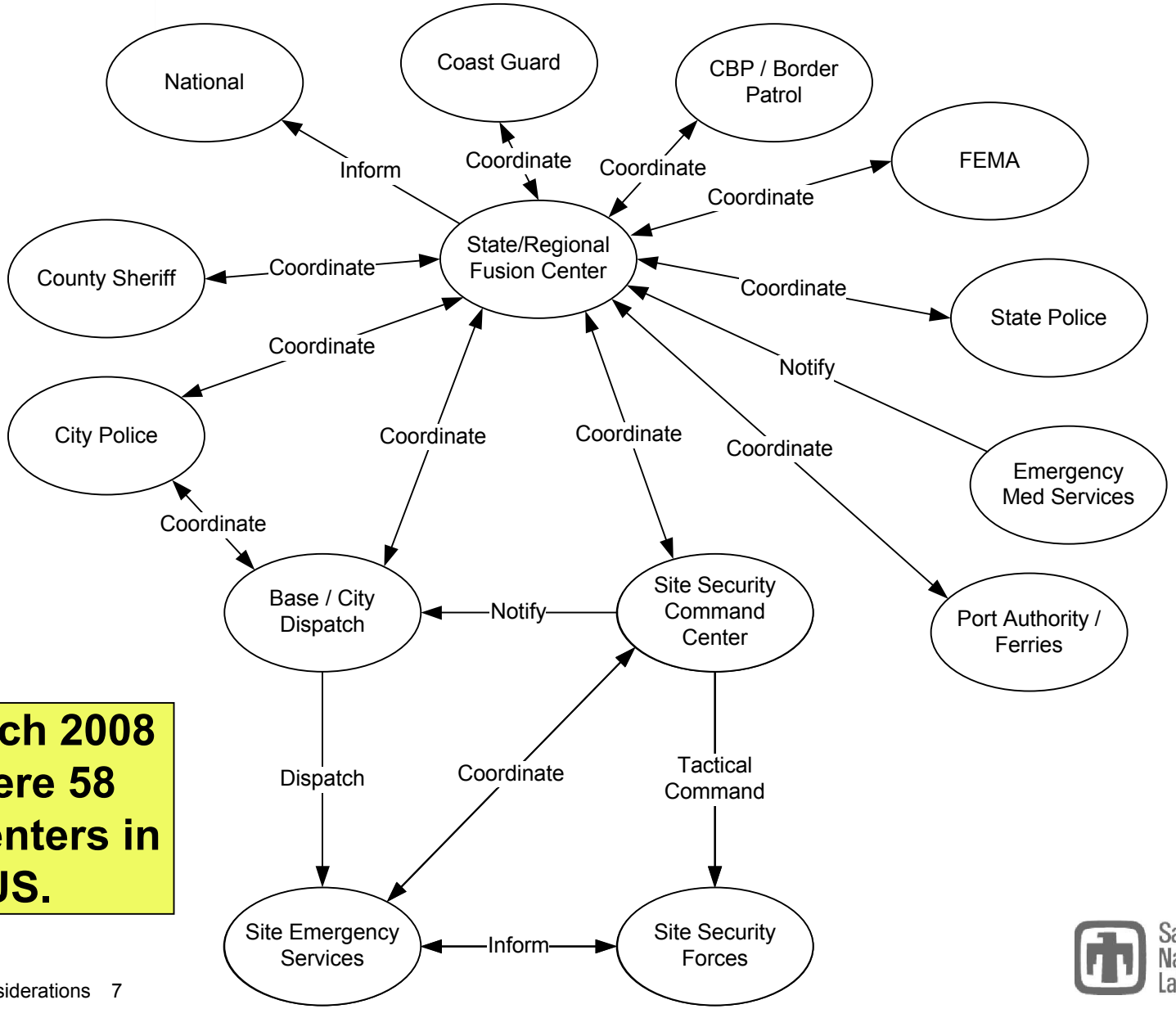
Sandia National Laboratories

Operational Activity Model (OV-5) Example 2: On-Site Event



Sandia National Laboratories

Organizational Relationships Chart (OV-4) Example



As of March 2008 there were 58 Fusion Centers in the US.

Sandia National Laboratories

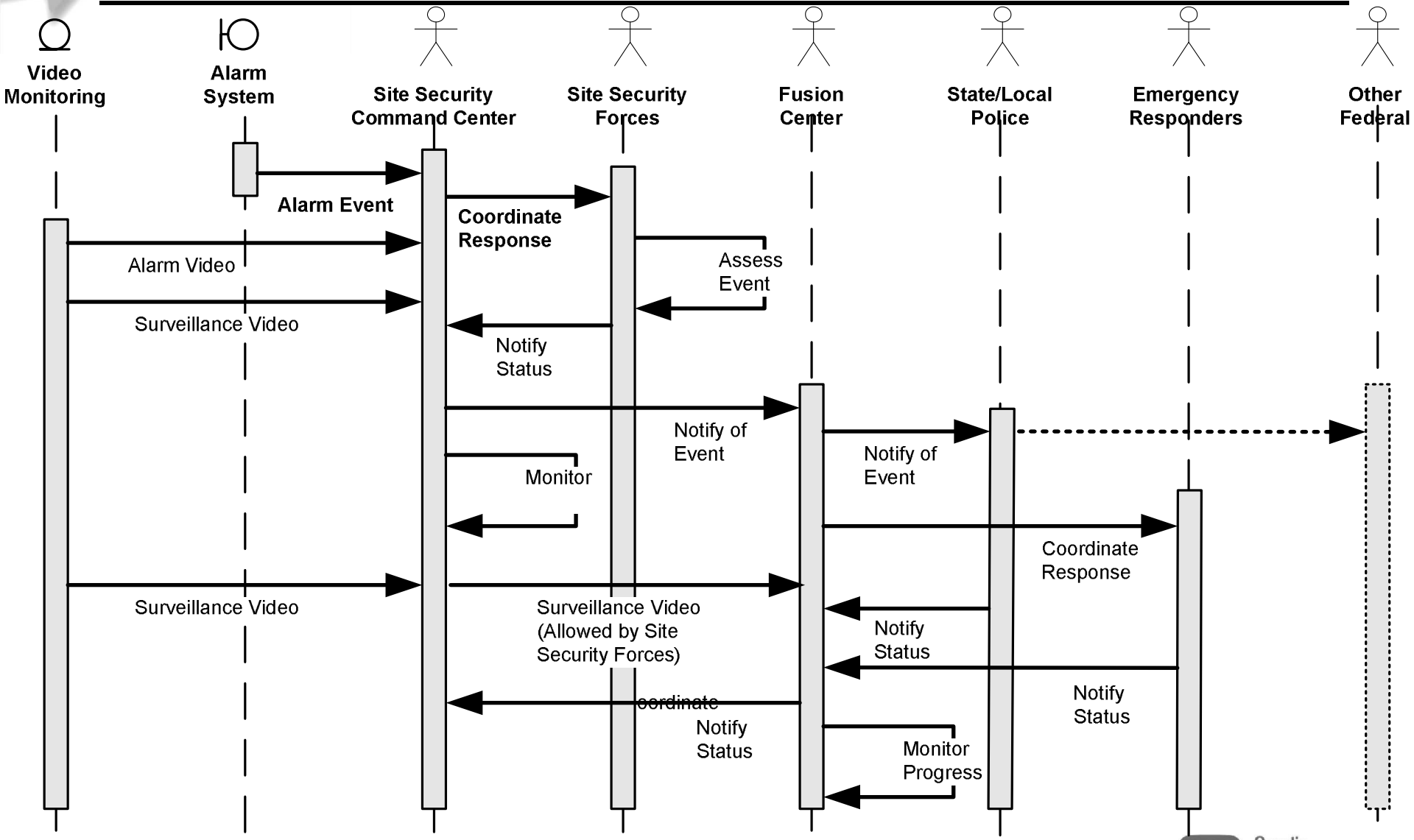
Fusion Center Floor Plan

Fusion Center: a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

Diagram courtesy of J. Britton, JIAFC

Sandia National Laboratories

Operational Event-Trace Description (OV-6c) Example 2: On-Site Event



Sandia National Laboratories

Operational Information Exchange Matrix (OV-3) Example

- Information exchanged between nodes
- With attributes
  - Classified or unclassified
  - IM, chat, phone, cell phone, radio, fax, email
  - Live/continuous, periodic, upon event, as needed,…
  - Video, text, photo, binary data, etc.
- Examples
  - Common Operational Picture – GIS-based map display
  - Force location and status
  - Collaboration, chat
  - Remote sensors and video
  - Radar, sonar track display
  - Response force vectoring
  - Mobile command and control
  - Early warning / early detection
  - ATFP support coordination

DESIGN

Data vs. Information

Data

- Remote sensors & cameras
- Perimeter sensors & cameras
- Location sensors (individuals and vehicles)
- Other video (surveillance and “external”)
- Radar and sonar tracks
- Entry control (badge reads, barrier/door/gate controls,…)
- Local, national news

Information

- Site-wide tactical picture
- Security Forces and status
- Site-wide security status
- Coordination with emergency response (fire, EMS, etc.)
- Asset location (fixed and mobile)
- Mobile Command & Control
- Intelligence-based early warning

Tends to be **UNCLASSIFIED**

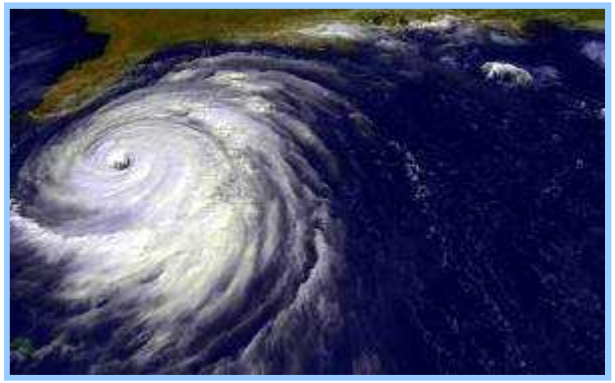
Tends to be **CLASSIFIED**

Sandia National Laboratories

Emergency Operations vs. Tactical

Emergency Ops Center

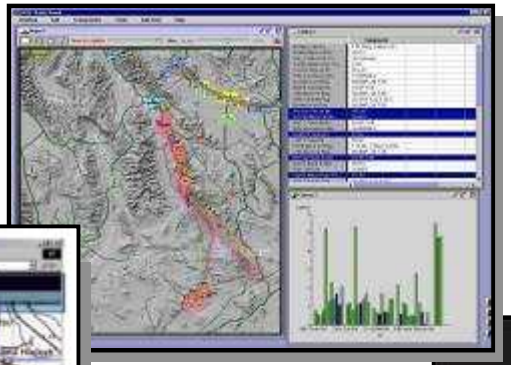
- National Incident Management System (NIMS) Compliant, includes
  - FEMA, Coast Guard
  - State and Local agencies
- Focus: Emergency Mgmt & Civil Support
  - Hurricanes
  - Wild Fires
  - Earthquakes
  - Fires and Police calls
- Mostly Unclassified
- Civil agencies often bring their own laptops and access their own applications
- Most bring their own cell phones

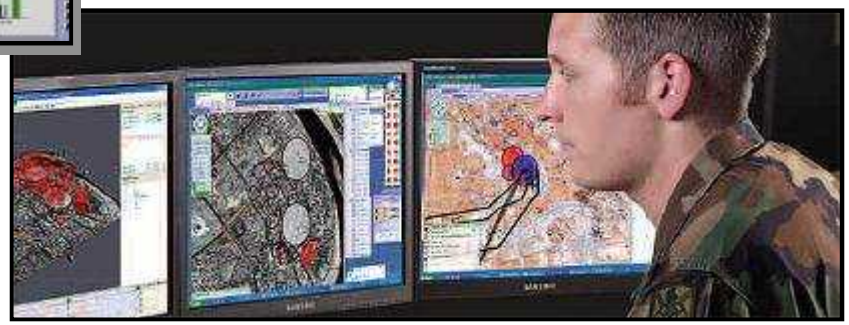


Tactical Ops (Security)

- Navy / USAF command structure
  - Air Ops, Seaport Ops, Base Ops
- Focused on security operations
  - Asset movements
  - Asset storage
  - Asset handling / maintenance
  - Anti-terrorism Force Protection
  - Situational awareness of region
- Encrypted voice comms
- Protected UCNI/Secret security network
- SCI adjunct for Intel
- Utilizes DoD communications networks for off-base comms incl. STUs/STEs, SIPRnet

S-A Workstation Examples





Inner Focus vs. Outer Focus

Inner

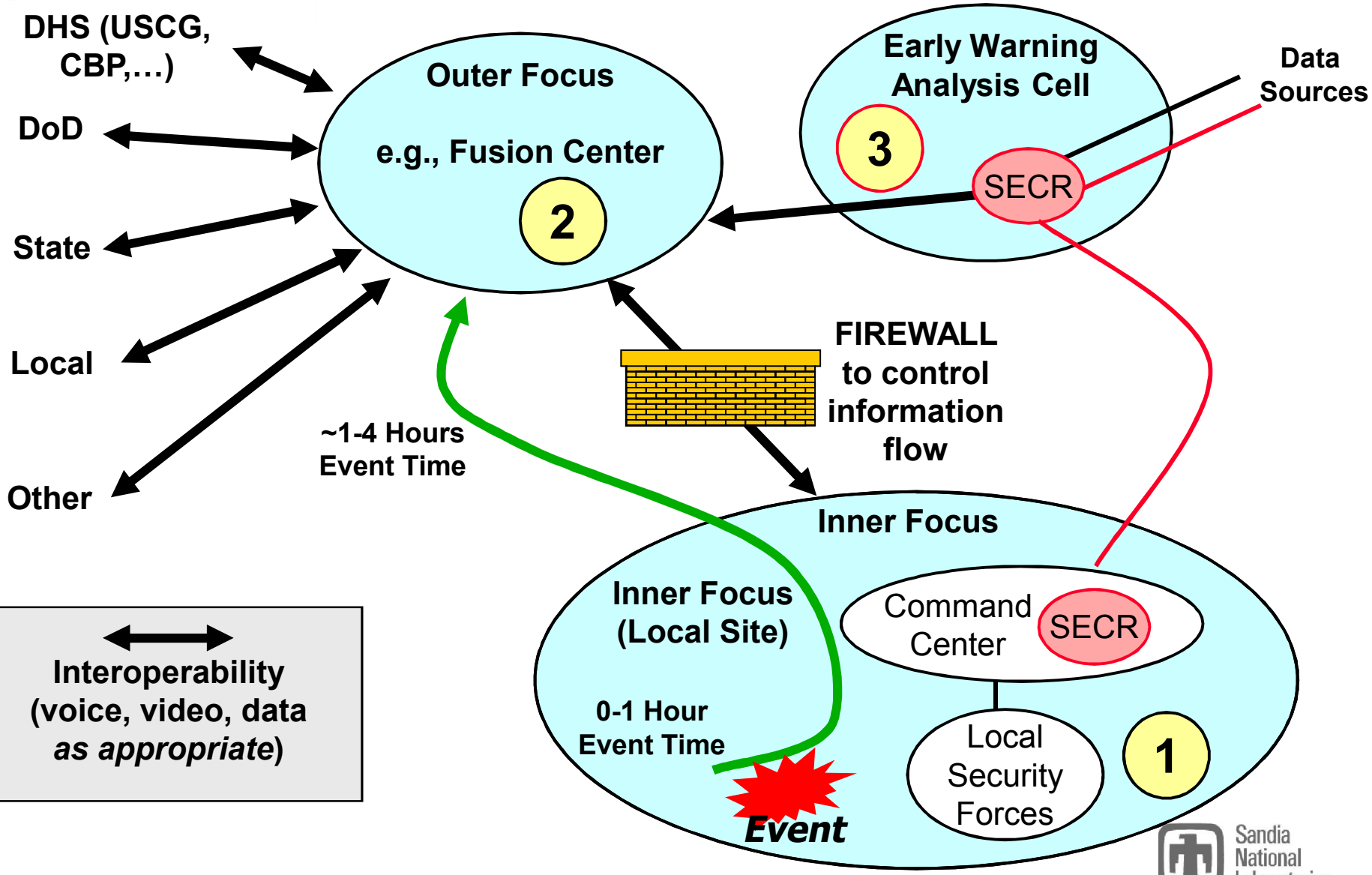
- Local site specific, internal "situation"
- Location of site security forces and emergency responders
- Local building/facility alarms
- Video alarm assessment
- Video surveillance
- Entry control ops
- Security system-of-systems status and availability

Outer

- Other sensor, video feeds
- Collaboration & interop
  - Local, state, emergency responders incl. location
  - Other DoJ (FBI, other federal LE)
  - Other DOE/NNSA
  - Other DoD, NORTHCOM
  - Other DHS (FEMA, USCG, CPB, …)
- Intel-based early warning

DEPLOYMENT

Architecture for Implementation

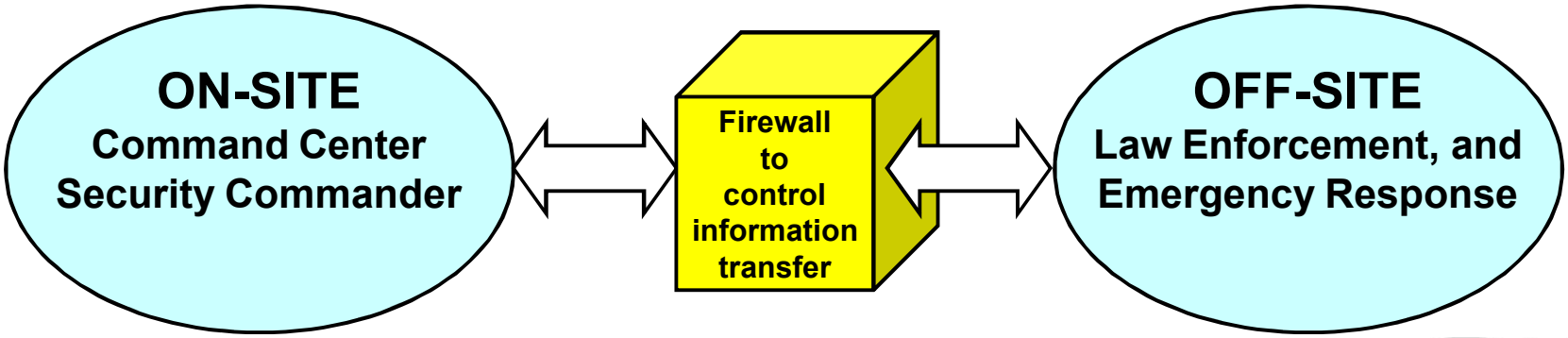


Sandia National Laboratories

Firewall Between Local Site and Off Site for Information Exchange

The local commander needs to be able to control the flow out of (and into) his/her domain.

- **Data IN to site includes**
  - **Emergency responders locations**
  - **Other video feeds, other radar (e.g., low-flier radar)**
- **Data OUT of site includes**
  - **What ever the commander wants/needs to share/export**
- **A Controllable Interface is needed:**
  - **Browser-based so that the commander can access anywhere, anytime**
  - **Easy point & click to turn-on/turn-off data feeds**



Sandia National Laboratories

Summary

- Situation Awareness is…
  - A complex, enabling technology,
  - Involving many organizations or systems,
  - That need to communicate information, that
  - Is to be protected at different levels.
- Some tools are being used today
  - Albeit at a single protection level
- Information valve or firewall needed
  - Between “On-Site and “Off-Site”
  - To permit controlled information exchange at similar protection levels

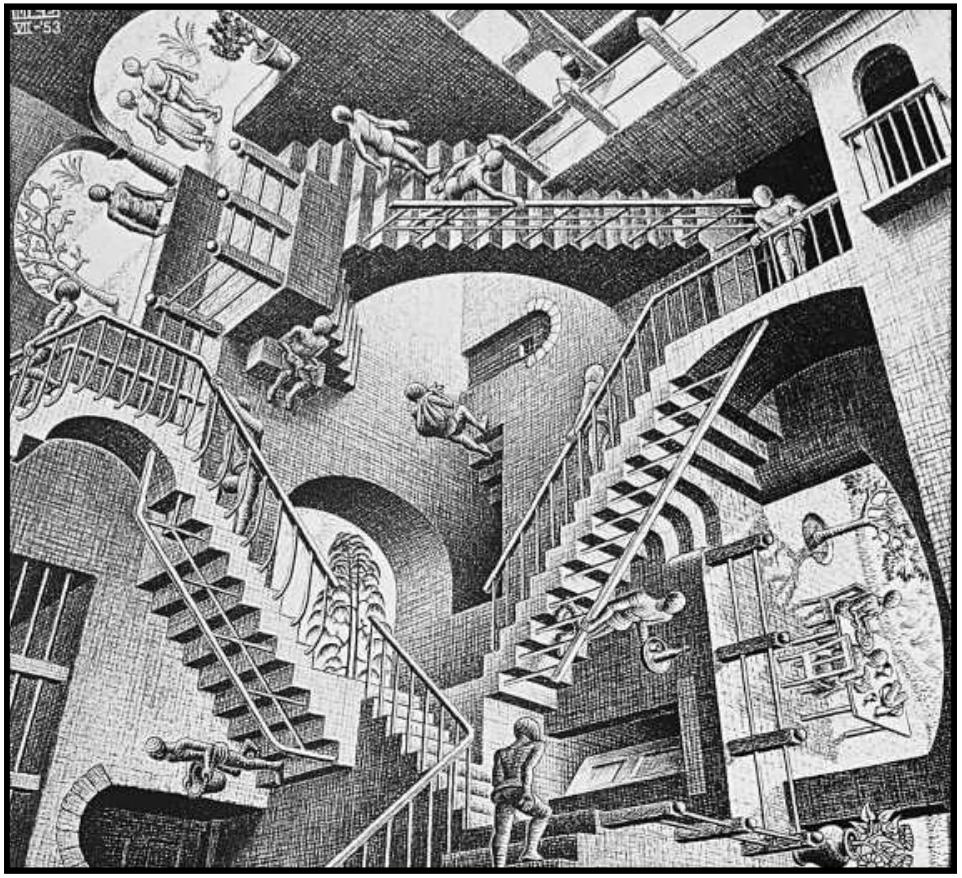
Thank you!

Daniel Pritchard

Sandia National Laboratories

dpritch@sandia.gov

505-844-7444



Coordination across diversity.

Sandia National Laboratories