PROGRAM OVERVIEW

ISART Conference

March 7, 2006

Agenda

- SAFECOM Overview
  Tony Frater

- Public Safety Statement of Requirements (SOR)
  Andrew Thiessen

- Public Safety Architecture Framework (PSAF)
  Jeff Bratcher

- Consensus Standards for Communications
  Eldon Haakinson

- Project 25 Compliance Assessment Program
  Eric Nelson

- Questions

Wireless interoperability is the ability of public safety service and support providers to talk with each other via voice and data

- on demand
- in real time
- when needed
- when authorized

OIC

The Office for Interoperability and Compatibility (OIC) was established to serve as the office within the Department of Homeland Security's Science and Technology Directorate's Office of Systems Engineering and Development to strengthen and integrate interoperability and compatibility efforts to improve local, tribal, state, and federal public safety preparedness and response.

OIC is addressing:

- Communications (SAFECOM, Disaster Management)

- Equipment

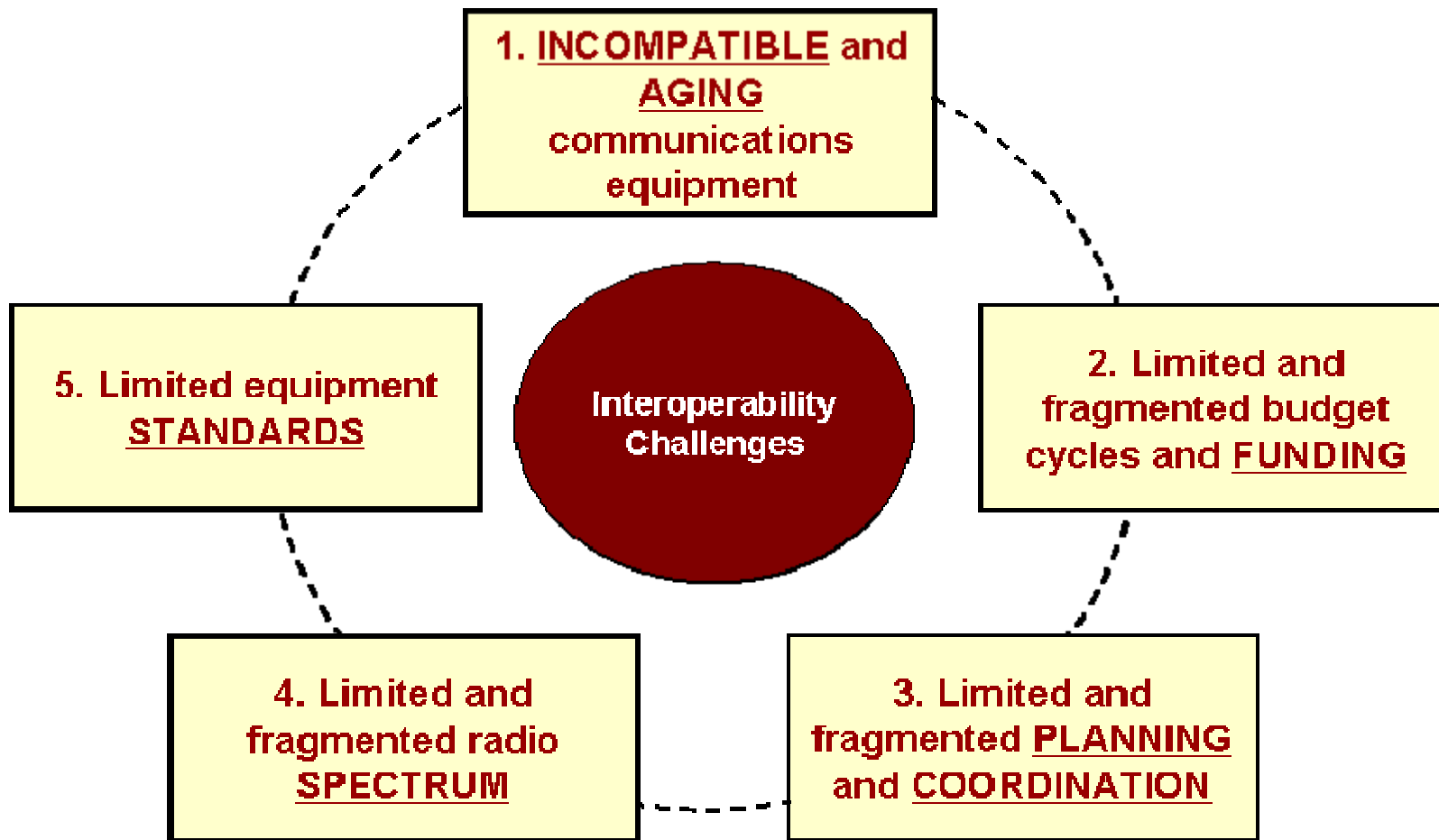- Training

- Other areas as identified

SAFECOM

SAFECOM, a communications program of OIC, provides research, development, testing and evaluation, guidance and assistance for local, tribal, state, and federal public safety agencies working to improve public safety response through more effective and efficient interoperable wireless communications.

- SAFECOM is a public safety practitioner-driven program that works cooperatively with more than 60,000 local and state public safety agencies.

- SAFECOM makes it possible for the public safety community to leverage resources by promoting coordination and cooperation across all levels of government.

With its partners, SAFECOM is working to ensure a safer America through effective public safety communications.
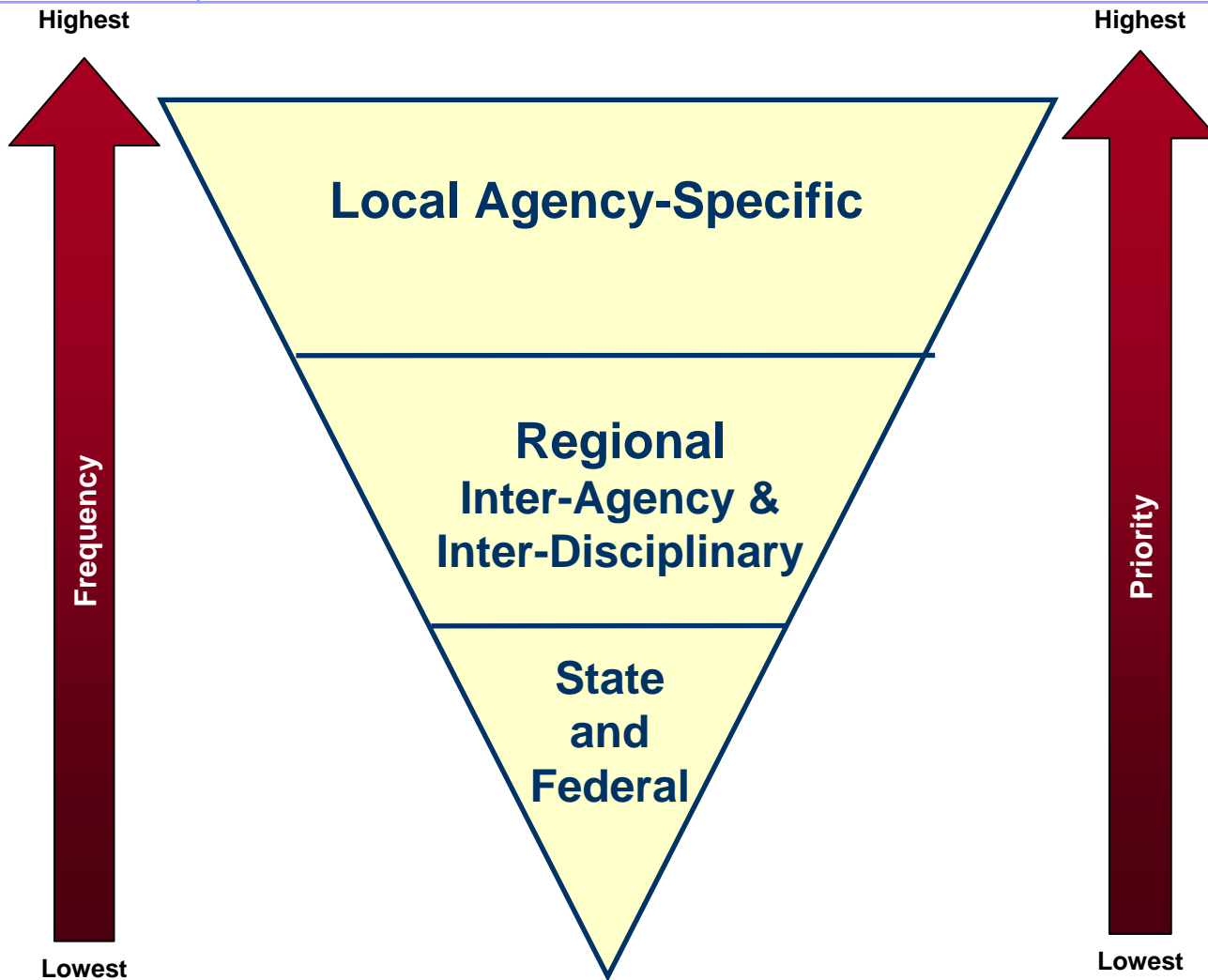
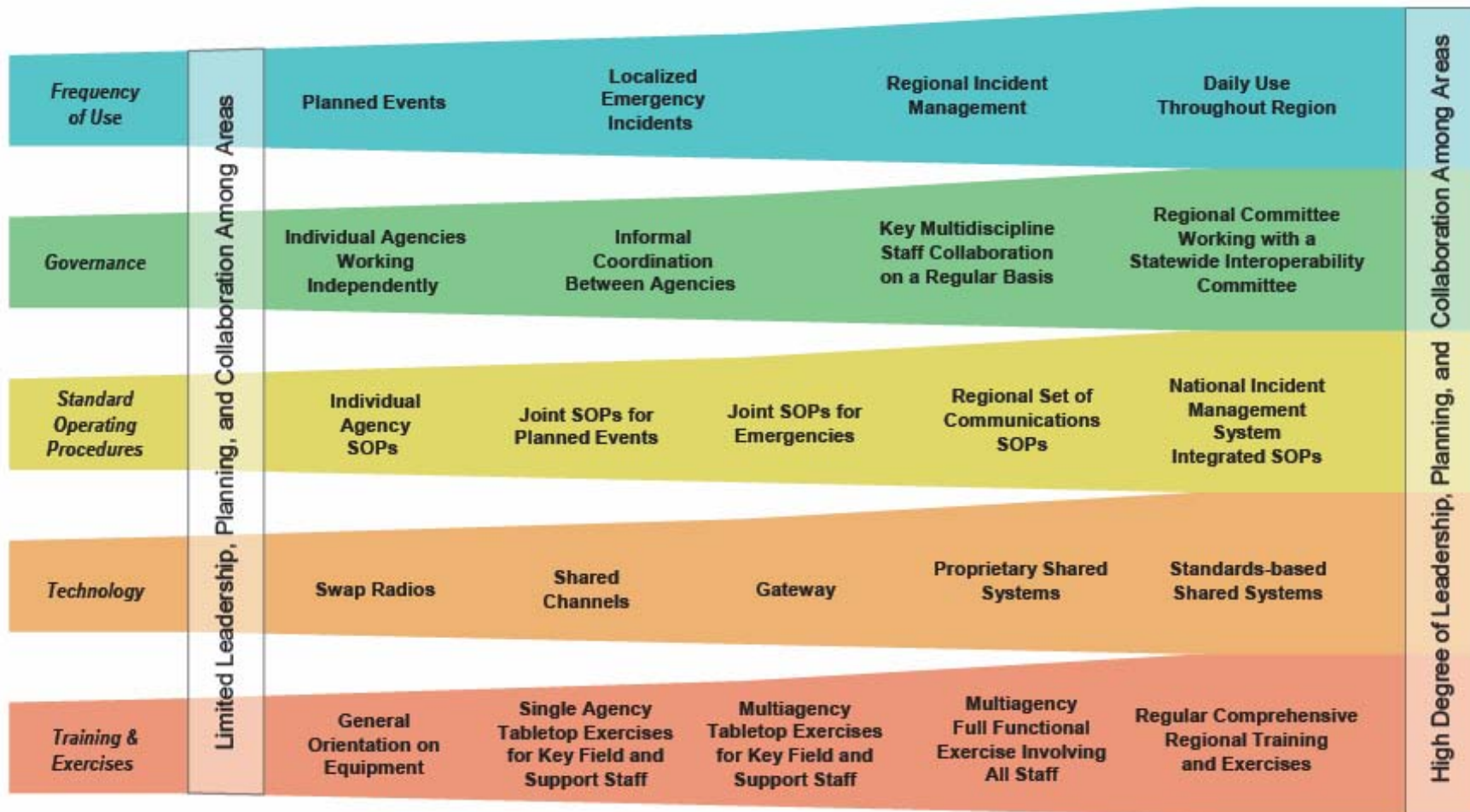1. INCOMPATIBLE and AGING communications equipment

2. Limited and fragmented budget cycles and FUNDING

3. Limited and fragmented PLANNING and COORDINATION

4. Limited and fragmented radio SPECTRUM

5. Limited equipment STANDARDS

Interoperability Challenges

Highest

Highest

Frequency

Priority

Local Agency-Specific

Regional
Inter-Agency &
Inter-Disciplinary

State
and
Federal

Lowest

Lowest

	Limited Leadership, Planning, and Collaboration Among Areas					High Degree of Leadership, Planning, and Collaboration Among Areas
Frequency of Use		Planned Events	Localized Emergency Incidents	Regional Incident Management	Daily Use Throughout Region	
Governance		Individual Agencies Working Independently	Informal Coordination Between Agencies	Key Multidiscipline Staff Collaboration on a Regular Basis	Regional Committee Working with a Statewide Interoperability Committee	
Standard Operating Procedures		Individual Agency SOPs	Joint SOPs for Planned Events	Joint SOPs for Emergencies	Regional Set of Communications SOPs	National Incident Management System Integrated SOPs
Technology		Swap Radios	Shared Channels	Gateway	Proprietary Shared Systems	Standards-based Shared Systems
Training & Exercises		General Orientation on Equipment	Single Agency Tabletop Exercises for Key Field and Support Staff	Multiagency Tabletop Exercises for Key Field and Support Staff	Multiagency Full Functional Exercise Involving All Staff	Regular Comprehensive Regional Training and Exercises

Minimal Level ⟵ Interoperability Continuum ⟶ Optimal Level

Public Safety
Statement of Requirements
(SoR)

Andrew Thiessen

Agenda

- What the PS SoR is
- How to read the PS SoR
- What the PS SoR has in it
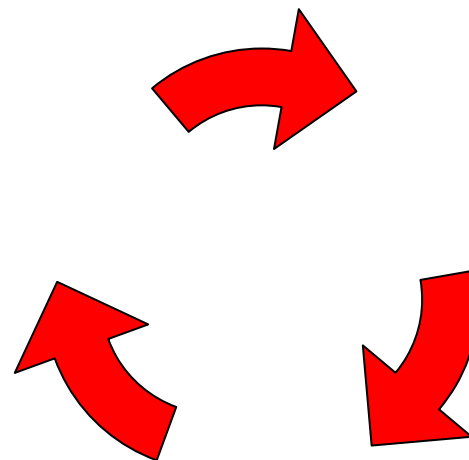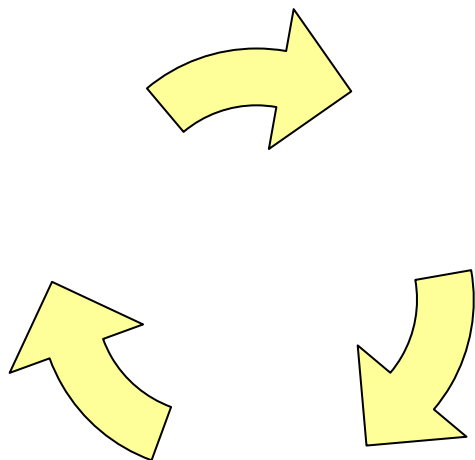- How the PS SoR is being used
- How the PS SOR is being matured

- **Qualitative**
  - Version 1.0 (April '04)
  - Version 1.1 (Feb '06)

- **Quantitative**
  - Version 2.0 (Sept '06)
  - Version 2.x (TBD)

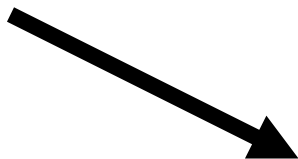Public Safety
Reader's Digest

This weeks edition contains:
Traffic Stop
Heart Attack
Residential Fire
Chemical Plant Explosion

Operational Requirements

Who talks to who

-Why

-How

-When

-What

Functional Requirements
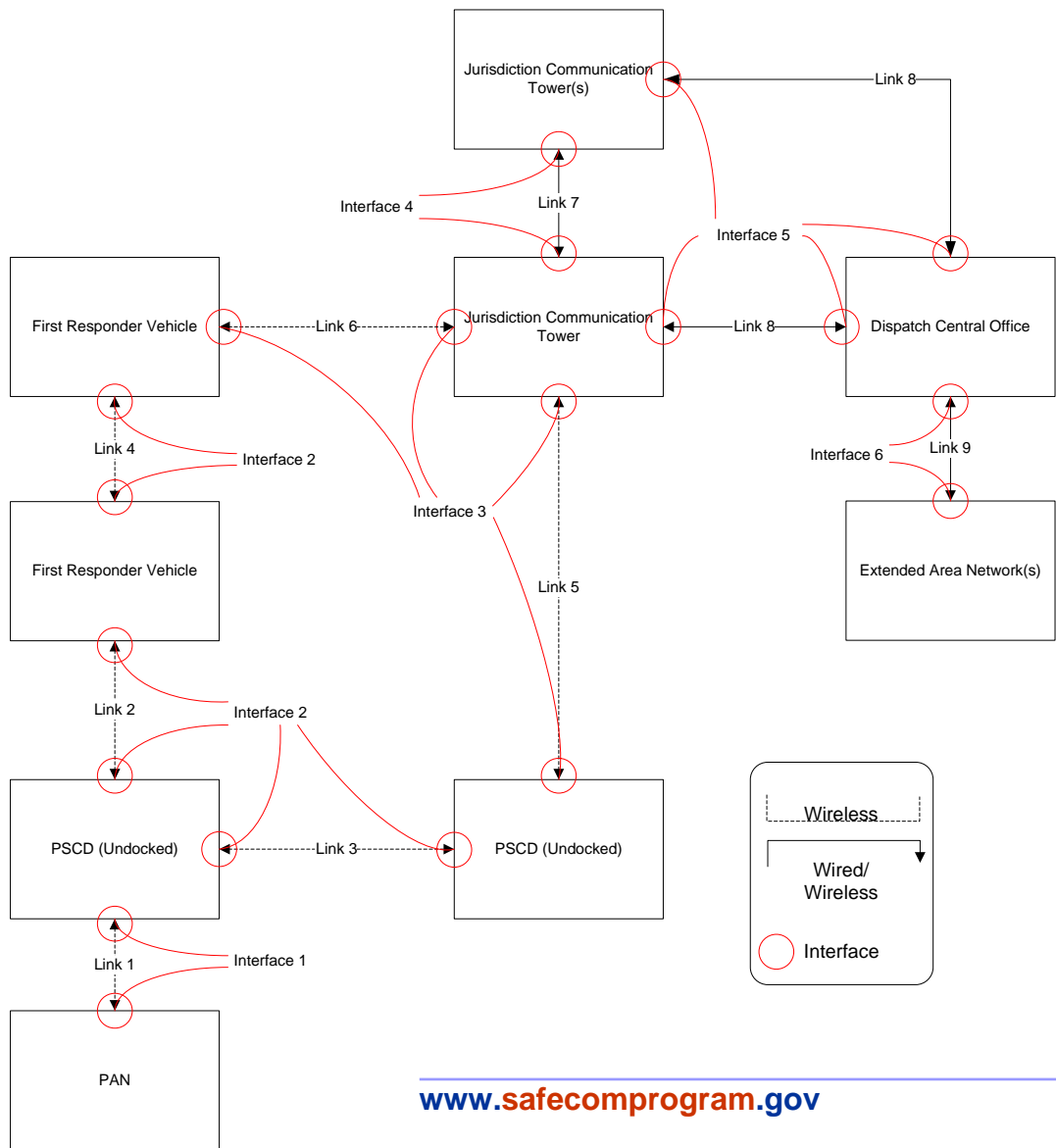
Applications/Services

Devices

Network Performance

SAFECOM

Extended Area Network (EAN)

Jurisdiction Area Network (JAN)

JAN

IAN   IAN   IAN   IAN   IAN   IAN   IAN

Public Safety Communications Device

Public Safety Communications Device

Personal Area Networks (PANs)

PANs

PANs

IAN = Incident Area Network

Wireless Network Link

Wired Network Link
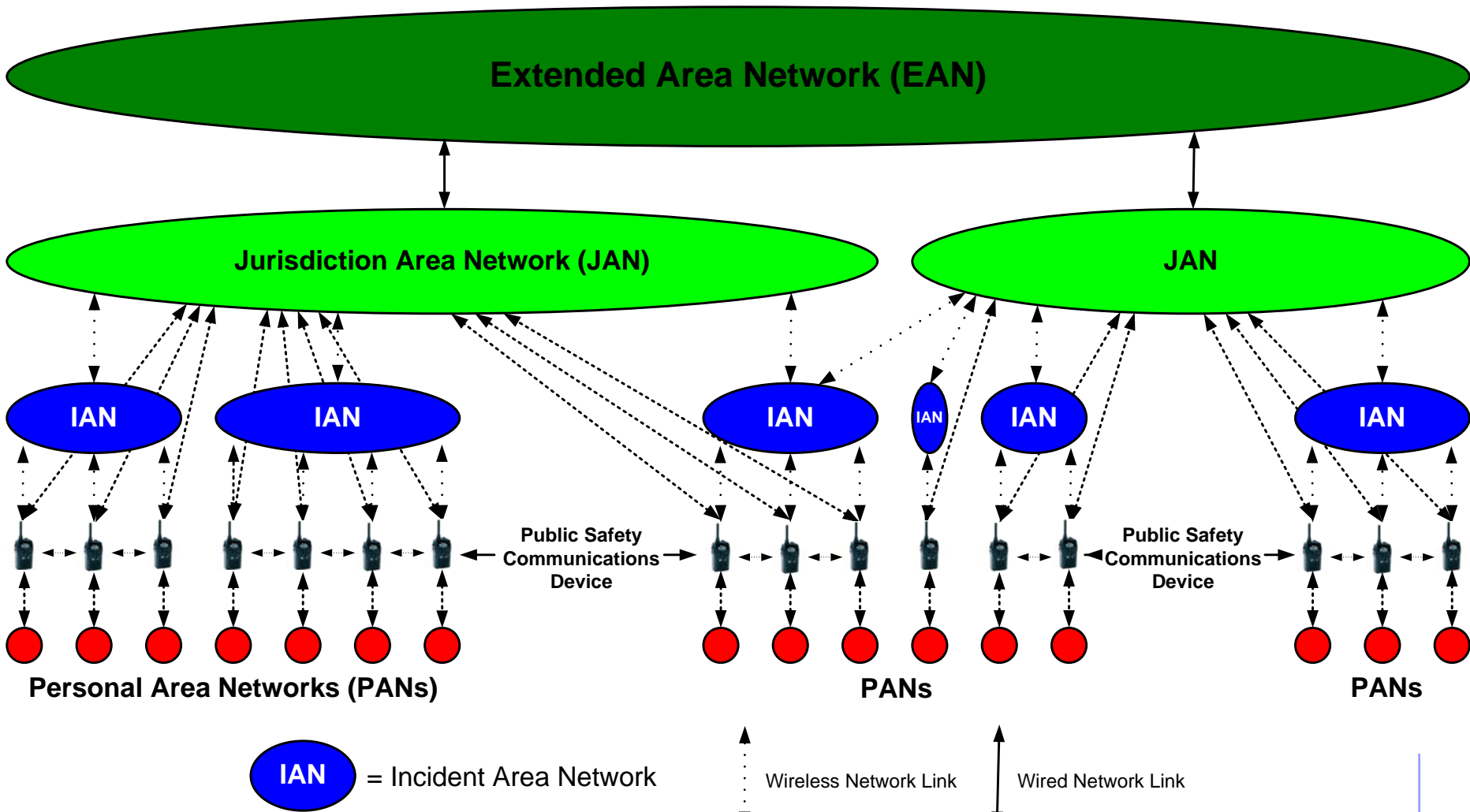
How is the PS SoR being used?

- **Research and Development**
  - SAFECOM Academic RFP
    - MANET
    - Security
    - Voice Quality
    - Video Quality
  - NIST Labs Research
    - PAN
    - Mobility
  - Industry Research
    - Products beginning to use PS SoR terminology and concepts

- **Standards Development**
  - Will be covered in more detail during Standards Panel

- PS SoR Working Group
- Vetting process with public safety organizations
  - NPSTC
  - P25/34 Steering Committee
- RFP's
  - SAFECOM 5 Year PS SoR RFP
- Outside stakeholder vetting (in progress)

Public Safety Architecture Framework (PSAF)

Jeff Bratcher

Definition of Architecture:

An <u>architecture</u> is "the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time."

- Derived from IEEE Std 610.12, 1990

Definition of Architecture Framework:

<u>Architecture Framework</u> defines what capabilities the architect/designer must deliver and how those capabilities must be constructed.

i.e. – analogous to blueprint standards or building codes

Describe information needs and sources in context with the missions supported

- What?
- Where?
- Who responsible?
- How used?

Identify and examine current and postulated business processes, systems, and technology with respect to satisfaction of stated requirements (SoR)

Refine investment strategies

- GAP analysis
- Direct Research & Development
- Direct Standards efforts
- Leverage across multiple agencies

- Consider Lego building blocks.

- An Architectural Framework is equivalent to the factory instructions that determine how the blocks are built including size, shape, number/proportions/location of holes and number/proportions/location of "bumps" AND the shipped instructions as to how they should be fitted together to produce the desired object, a Lego house for instance.

- An Enterprise Architecture is the house that results from following these instructions.

- Primary Goals of PSAF for the Public Safety community are to:

  1. *Provide the process and tools for planning of interoperable communications and information sharing.*

  2. *Assist in identifying non-interoperable areas among legacy and future architectures*

  3. *Protect the capital investment in legacy communications systems while in transition to SoR future state*

  4. *Shorten the product lifecycle by leveraging Commercial Off the Shelf (COTS) equipment that adheres to the SoR*

*The Framework is **not**...*

- **A National PS Communications Architecture developed by the Feds.**

*The Framework **is** ...*

- **Common, pragmatic guidelines for describing architectures to enable comparisons and dovetailing**

- **Tailor-able and modifiable to suit mission requirements**

- **An architectural discipline for examining processes and system alternatives in context with mission operations and the information required**

- **A specific process and methodology**
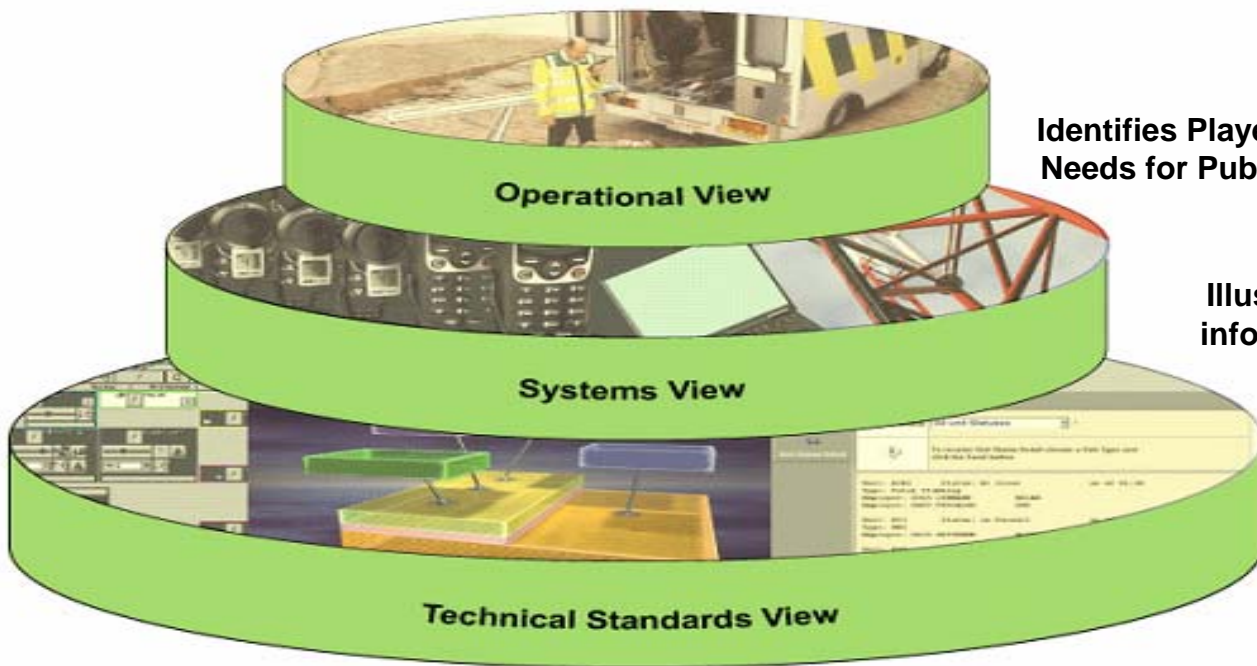
Identifies Players, Relationships, and Information Needs for Public Safety to perform their mission.

Illustrates the equipment and flows of information to support the Operations.

Illustrates the technical rules and guidelines that allow the systems to interoperate.

SAFECOM

Operational View Products

High-level Operational Concept Description
Operational Node Connectivity Description
Operational Information Exchange Matrix
Organizational Relationships Chart
Activity Model
Operational Rules Model
Operational State Transition Description
Operational Event/Trace Description
Logical Data Model

All Views

Integrated Dictionary
Overview and Summary Info

Systems View Products

| System Interface Description |
|---|
| Systems Communications Description |
| Systems Matrix |
| Systems Functionality Description |
| Operational Activity to System Function Traceability Matrix |
| System Data Exchange Matrix |
| System Performance Parameters Matrix |
| System Evolution Description |
| System Technology Forecast |
| Systems Rules Model |
| Systems State Transition Description |
| Systems Event/Trace Description |
| Physical Schema |

Technical Standards View Products
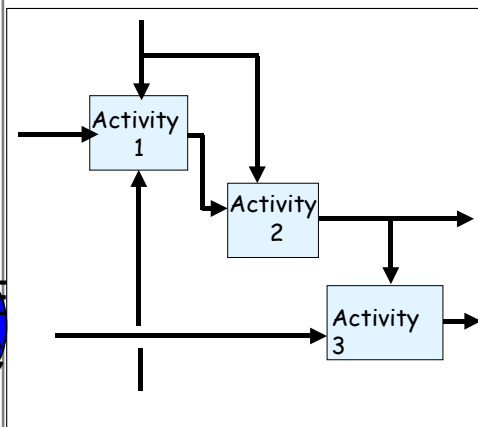
Technical Standards Profile
Standards Technology Forecast

Captures Critical Mission Relationships and Information Exchanges
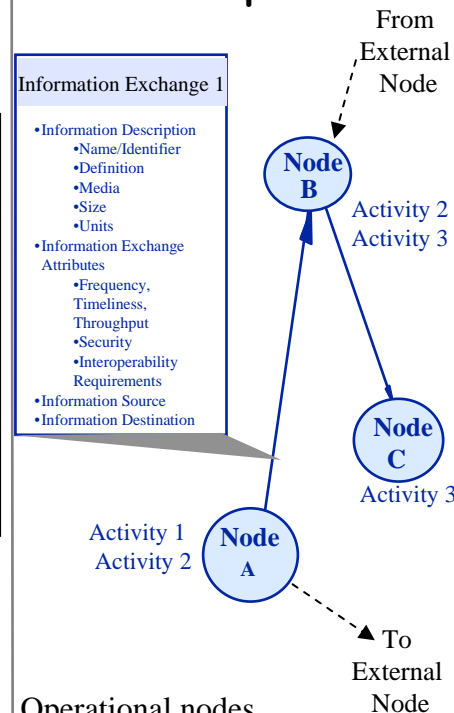
High-Level Operational Concept Description

Chemical Cloud
EMS
FIRE IC
Fire Fire
IC
LE IC
LE
EMS IC
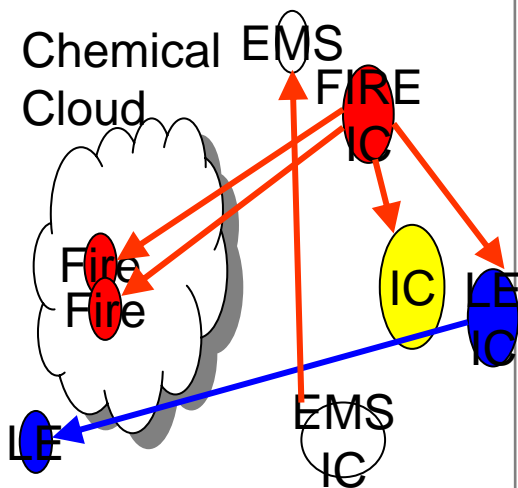
High-level graphical description of the operational concept of interest

Activity Model

Activity 1
Activity 2
Activity 3

Operational activities performed and their input/output relationships

Operational Node Connectivity Description

Information Exchange 1
• Information Description
  • Name/Identifier
  • Definition
  • Media
  • Size
  • Units
• Information Exchange Attributes
  • Frequency, Timeliness, Throughput
  • Security
  • Interoperability Requirements
• Information Source
• Information Destination

From External Node

Node B
Activity 2
Activity 3

Node C
Activity 3

Activity 1
Activity 2
Node A

To External Node

Operational nodes, activities performed at each node, node-to-node relationships, and information needlines

Operational Information Exchange Matrix

INFORMATION EXCHANGE ATTRIBUTES		INFORMATION DESTINATION		INFORMATION SOURCE		INFORMATION DESCRIPTION	
INTEROPERABILITY REQUIREMENTS							
SECURITY							
FREQUENCY, TIMELINESS, THROUGHPUT							
	CONSUMING ACTIVITY	OPERATIONAL ELEMENT & ACTIVITY					
	IDENTIFIER OF CONSUMING OE						
	PRODUCING ACTIVITY	OPERATIONAL ELEMENT & ACTIVITY					
	IDENTIFIER OF PRODUCING OE						
FEET, LITERS, INCHES, ETC.	UNITS						
RANGE LIMITS	SIZE						
DIGITAL VOICE, TEXT, IMAGE, ETC.	MEDIA						
DEFINITION	DESCRIPTION						
NAME/IDENTIFIER	OPERATIONAL INFORMATION ELEMENT						

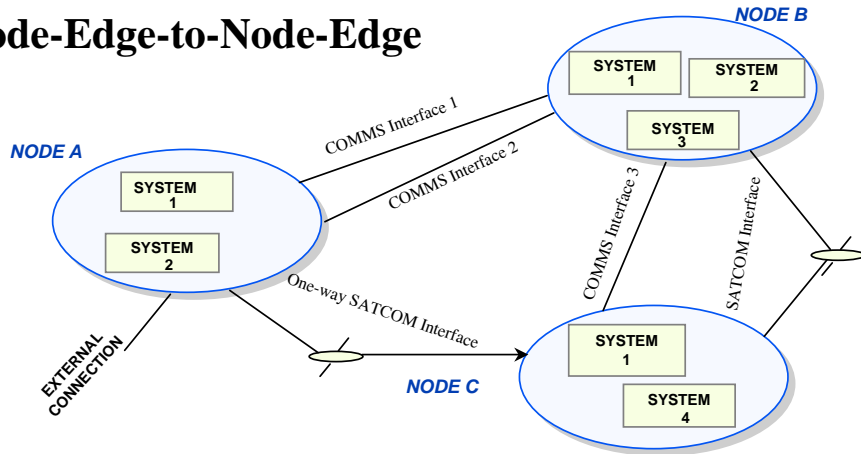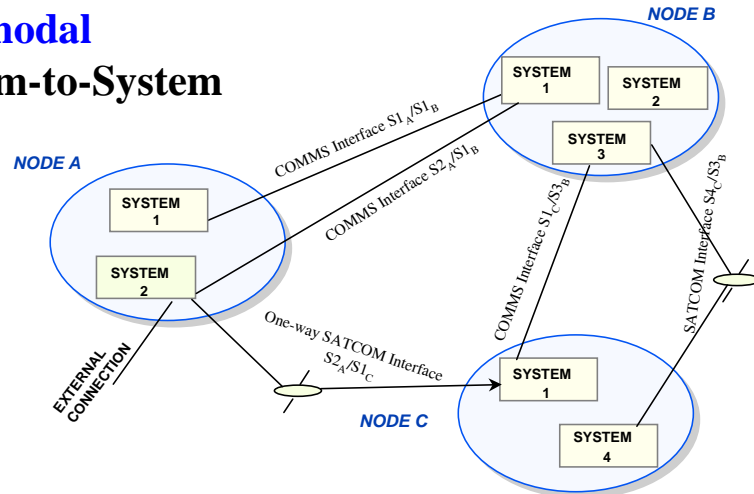Information exchanged between nodes and the relevant attributes of the exchanges

Examines Current and Postulated Capabilities in Context with Operations

Core Product: System Interface Description

Internodal
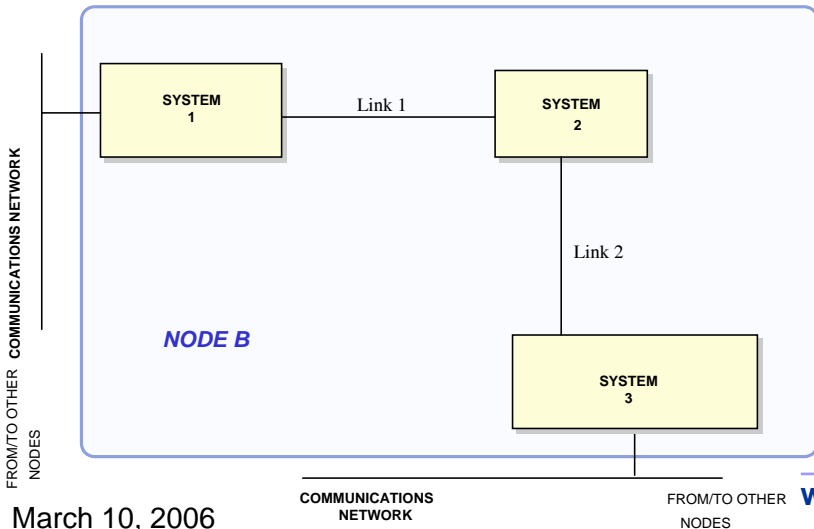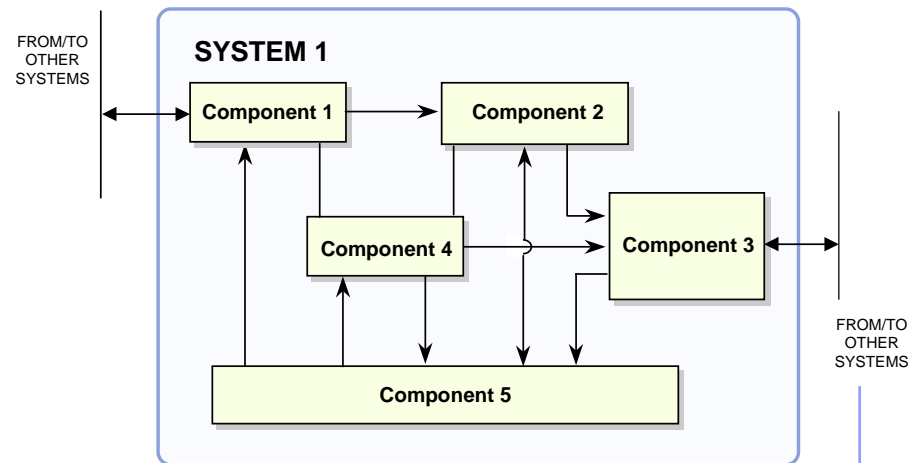### Node-Edge-to-Node-Edge

Internodal
System-to-System

Intranodal

Intrasystem

March 10, 2006

Identifies the Standards That Govern the Given Architecture

Application Software		
SERVICE AREA	**SERVICE**	**STANDARD**
Support Applications	Web Applications	Internet Explorer Version 4.X or better
		Netscape Version 3.X or better

Application Platform		
SERVICE AREA	**SERVICE**	**STANDARD**
Data Interchange	Document Interchange	XML 1.0, W3C Recommendation, 10 February 1998, Rec-xml-19980210 (Extensible Markup Language)
		HTML 4.0 Specification, W3C Recommendation revised 24-apr-1998, Rec-html40-19980424 (Hypertext Markup Language)
Communications	World Wide Web Services	IETF RFC-2616 Hypertext Transfer Protocol – HTTP/1.1, June 1999
	Electronic Mail	IETF Standard 10/RFC-821/RFC-1869/RFC-1870 Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995
		IETF Standard 11/RFC-822/RFC-1049 Standard for the Format of ARPA Internet Text Messages, 13 August 1982
		IETF RFCs 2045-2049 Multipurpose Internet Mail Extensions (MIME), November 1996
	Transport Services	IETF Standard 7/RFC-793 Transmission Control Protocol, September 1981
		IETF Standard 6/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112 Internet Protocol, September 1981
Distributed Computing	Object Services	Common Object Request Broker Architecture (CORBA) Version 2.3 Object Management Group (OMG) document formal/98-12-01, June 1999 (Proposed)
Security	Authentication	FIPS-PUB 112 Password Usage, 30 May 1985

Application Software		
MISSION AREA APPLICATIONS		
SERVICE AREA	**SERVICE**	**STANDARD**
All	Web Applications	*Interface 4D*: (Application to Web Server) Common Gateway Interface (CGI) 1.1, NCSA Software Development

Application Software		
SUPPORT APPLICATIONS		
SERVICE AREA	**SERVICE**	**STANDARD**
Communications Applications	Web Applications	*Component*: Internet Explorer Version 4.X or better
		Component: Netscape Version 3.X or better
		Interface 4L: HTML 4.0 Specification, W3C Recommendation revised 24-apr-1998, Rec-html40-19980424 (Hypertext Markup Language)
	Personal Messaging	*Interface 4D*: (E-Mail Client to E-Mail Server) IETF Standard 10/RFC-821/RFC-1869/RFC-1870 Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995
		Interface 4D: (E-Mail Server to E-Mail Client) Internet Mail Access Protocol (IMAP)

Application Platform		
SYSTEM SUPPORT SERVICES (XOS)		
SERVICE AREA	**SERVICE**	**STANDARD**
Communications	World Wide Web Services [Web Server]	*Interface 3L*: IETF RFC-2616 Hypertext Transfer Protocol – HTTP/1.1, June 1999
	Electronic Mail [E-Mail Server]	*Interface 3L*: IETF Standard 10/RFC-821/RFC-1869/RFC-1870 Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995
		Interface 3L: IETF Standard 11/RFC-822/RFC-1049 Standard for the Format of ARPA Internet Text Messages, 13 August 1982
		Interface 3L: IETF RFCs 2045-2049 Multipurpose Internet Mail Extensions (MIME), November 1996

Application Platform (OPERATING SYSTEM SERVICES)		
OPERATING SYSTEM SERVICES		
SERVICE AREA	**SERVICE**	**STANDARD**
Operating System	Kernel Operations	*Interface 3L*: IETF Standard 7/RFC-793 Transmission Control Protocol, September 1981
		Interface 3L: IETF Standard 6/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112 Internet Protocol, September 1981

- To compare architecture descriptions from different disciplines and jurisdictions to determine interoperability it is imperative that they are described with a common set of terms – i.e. a common Data Model

- PSAF approach is to leverage and extend the efforts of the GLOBAL Justice XML Data Model (GJXDM) which was created to share criminal justice information:

  – There is current activity within DHS to align the GJXDM and the NIEM – the "National Information Exchange Model".

  – Requires creating an architecture "namespace" within the existing NIEM Data Model and populating with applicable terms

- A tool to capture the architecture descriptions electronically is needed with a central repository of stored data for ease of comparison.

- PSAF approach is to pilot proposed tool and data model with AF Working Group assistance and inputs to develop tool that best fits the needs of the Public Safety community.

- Looking to leverage/extend the DHS-ICTAP Communication Asset Survey and Mapping (CASM) Tool

1. ## PSAF Volumes I and II
   - 2/17/2006 - Final Volumes submitted to SAFECOM

2. ## Data Model Creation and Standardization
   - Initial Data model created and vetted with AFWG
   - Begun discussions with NIEM on how to formally standardize

3. ## PSAF Tool Selection/Development
   - Analyze tool options with AFWG in Trial and Pilot
   - Vision is to have tool available on-line for any Public Safety agency to use via a web interface to assist them with their interoperability planning needs.
   - Determine development efforts to modify tool to fit needs and develop web front end
   - Determine hosting requirements for data repository

4. ## User's Guide Development
   - Results of Pilot will be used to develop User's Guide on tool and process

Consensus Standards
For Communications

Eldon Haakinson

Objectives

- Provide **communications** and **information sharing** by Public Safety Agencies
- Allow **operability** of Agency communication systems to support Public Safety mission
- Allow **interoperability** between Agencies to support mutual aid and task force operations

Approach

- Determine **user requirements** for Public Safety communications systems

- Describe **architecture framework** that supports the requirements

- Develop or adapt communications and information system **standards** (when none exist)

- Evaluate vendor products to ensure **compliance** with standards and requirements

- Practitioners
  - Emergency Medical Services personnel
  - Fire Fighters
  - Law Enforcement

- Public Safety Agencies
  - Local jurisdictions
  - State agencies
  - Federal departments and administrations

- 25,763 Local Agencies[*]
- 6,396 State Agencies[*]
- 2,967 Federal Agencies[*]

- 5,841 EMS Departments[*]
- 27,496 Law Enforcement Agencies[*]
- 28,495 Fire Departments[*]

960,000 Firefighters
830,000 EMS Personnel
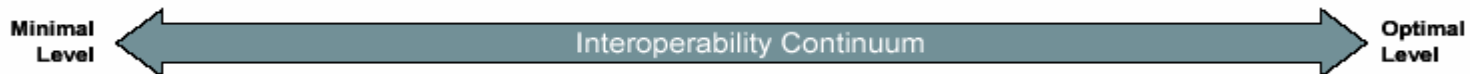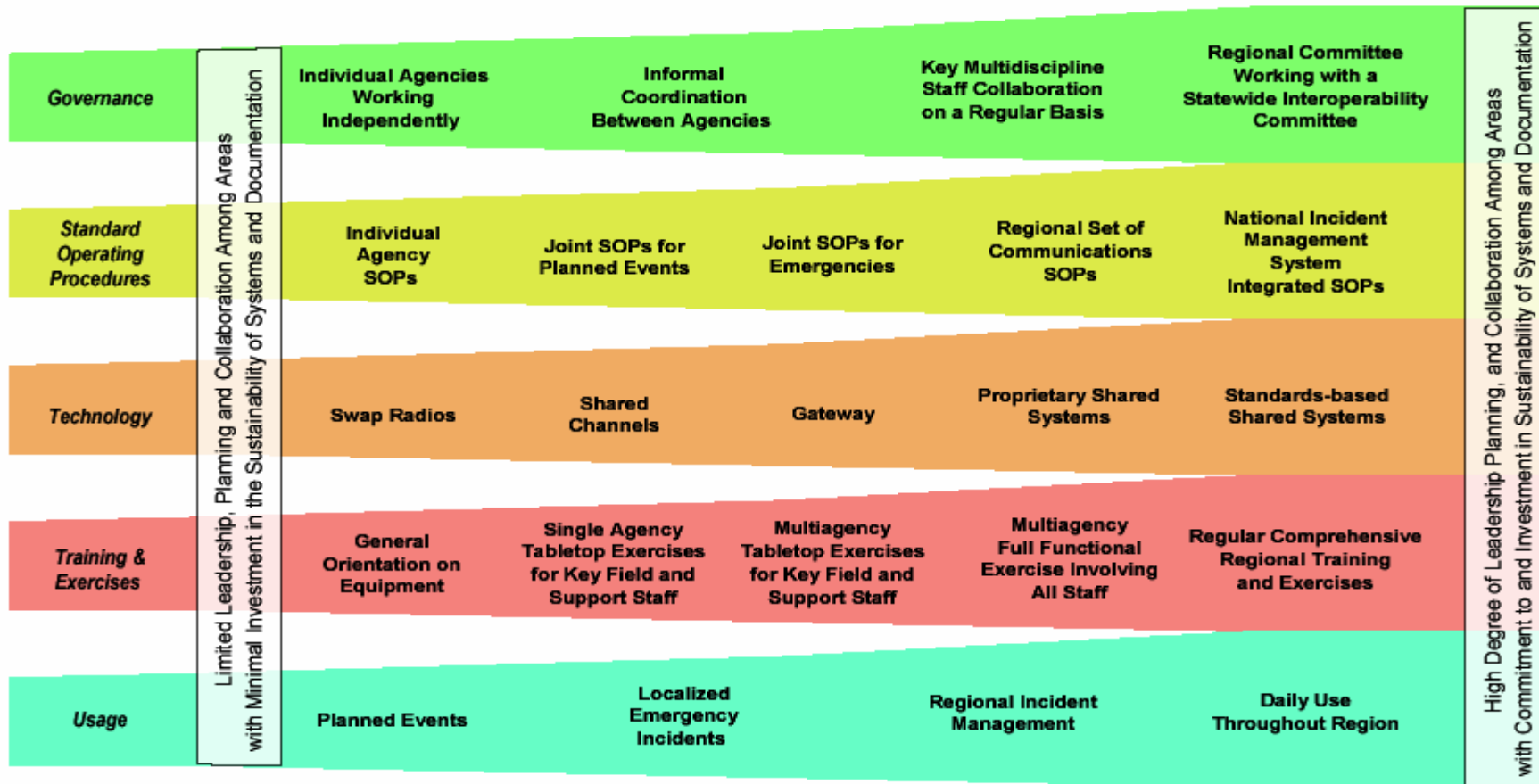710,000 Law Enforcement Officers

[*] www.SafetySource.com

- Practitioner-driven
- Comprehensive framework
  - Communications operability and interoperability
- Lifecycle approach
- System-of-systems
  - Integrates new and legacy systems
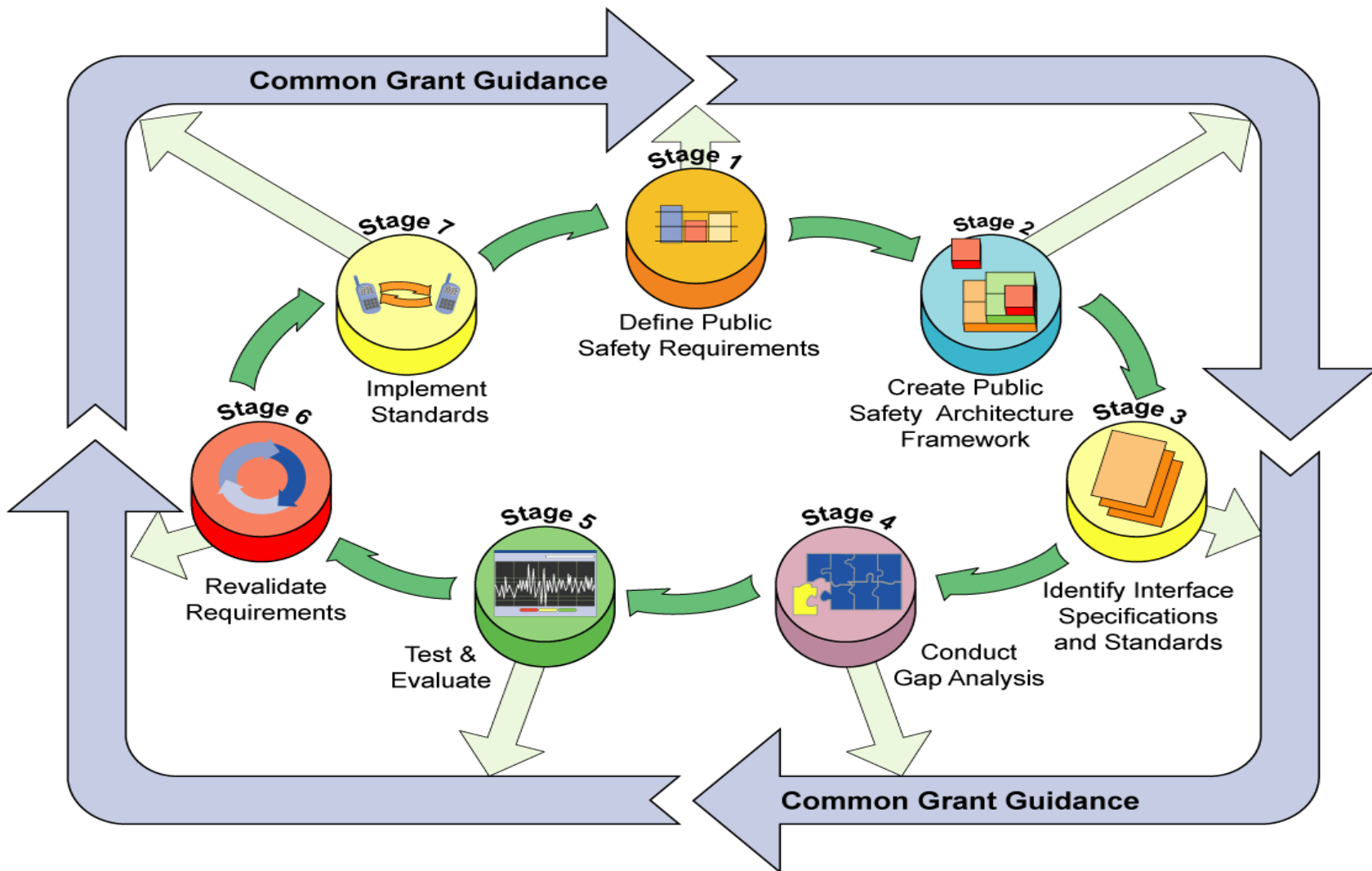- Industry and Public Safety partnership

Comprehensive Framework
Technology and Standards – one component

	Minimal Level → → → → → Optimal Level
Governance	Individual Agencies Working Independently — Informal Coordination Between Agencies — Key Multidiscipline Staff Collaboration on a Regular Basis — Regional Committee Working with a Statewide Interoperability Committee
Standard Operating Procedures	Individual Agency SOPs — Joint SOPs for Planned Events — Joint SOPs for Emergencies — Regional Set of Communications SOPs — National Incident Management System Integrated SOPs
Technology	Swap Radios — Shared Channels — Gateway — Proprietary Shared Systems — Standards-based Shared Systems
Training & Exercises	General Orientation on Equipment — Single Agency Tabletop Exercises for Key Field and Support Staff — Multiagency Tabletop Exercises for Key Field and Support Staff — Multiagency Full Functional Exercise Involving All Staff — Regular Comprehensive Regional Training and Exercises
Usage	Planned Events — Localized Emergency Incidents — Regional Incident Management — Daily Use Throughout Region

Left axis: Limited Leadership, Planning and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation

Right axis: High Degree of Leadership Planning, and Collaboration Among Areas with Commitment to and Investment in Sustainability of Systems and Documentation

Minimal Level ← **Interoperability Continuum** → Optimal Level

- # Interface Standards
  - – Provides broadest impact on interoperability
  - – Allows systems of multiple Public Safety agencies to be interconnected
  - – Allows equipment of multiple vendors to be interconnected
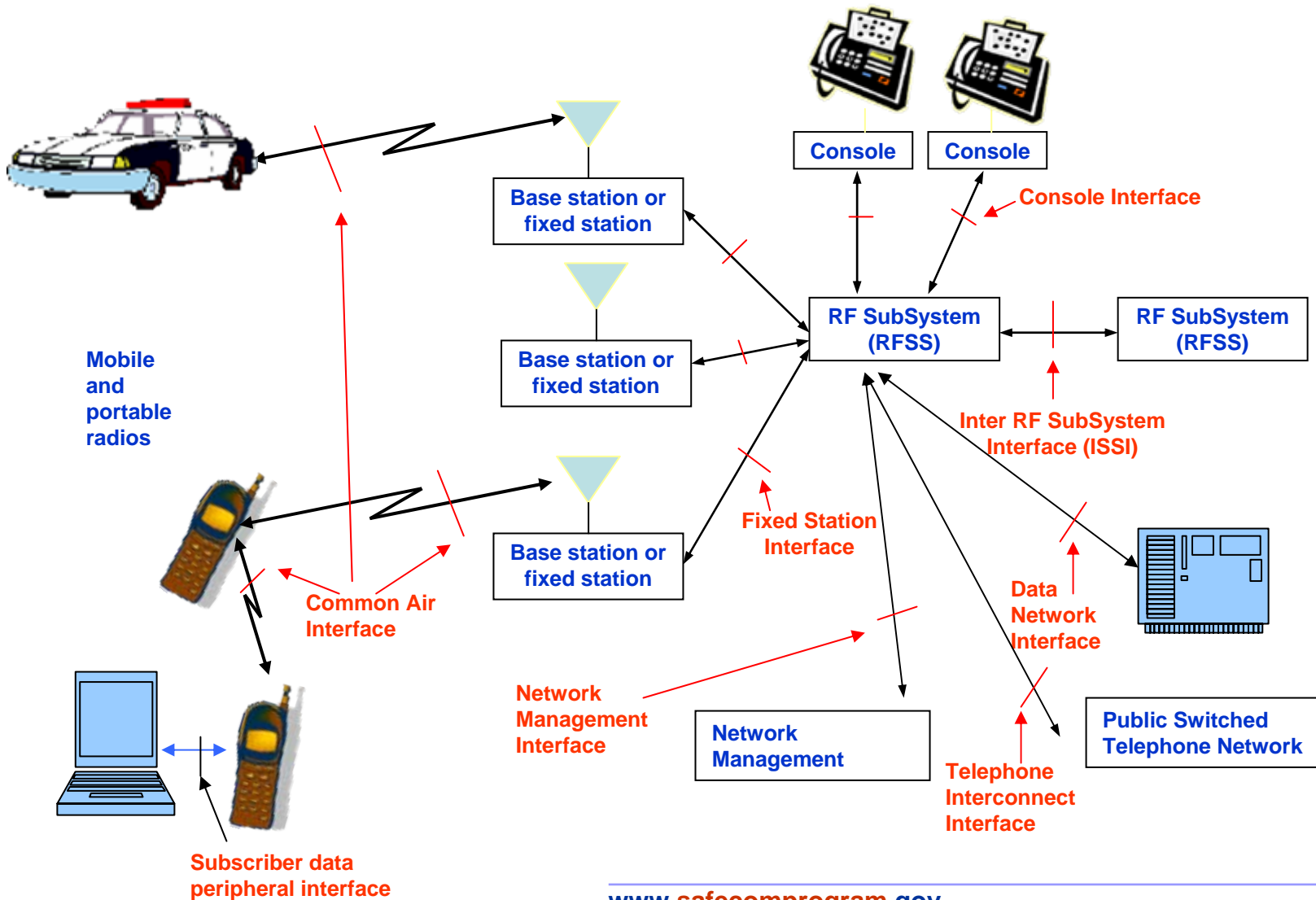 - – Allows applications and services of multiple providers to be interconnected

- # Interface Standards

  - Define wireless systems' modulation, access methods, signaling, and protocols

  - Define wireline systems' signaling, protocols, and controls

  - Define data systems' formatting, structure, protocols, and data definitions

  - DOES NOT define systems' internal operation and technology

Mobile and portable radios

Console Interface

RF SubSystem (RFSS)

RF SubSystem (RFSS)

Base station or fixed station

Inter RF SubSystem Interface (ISSI)

Fixed Station Interface

Data Network Interface

Common Air Interface

Network Management Interface

Network Management

Telephone Interconnect Interface

Public Switched Telephone Network

Subscriber data peripheral interface

March 10, 2006

DHS

DOJ

Emergency Mgt, Border Security, etc.

Law Enforcement, Intelligence, etc.

Courts, Probation, Parole, Corrections, etc.

Core

Public health, Etc.

Juvenile Justice, Welfare, Education

Etc.

Core

Universal Core

OTHER
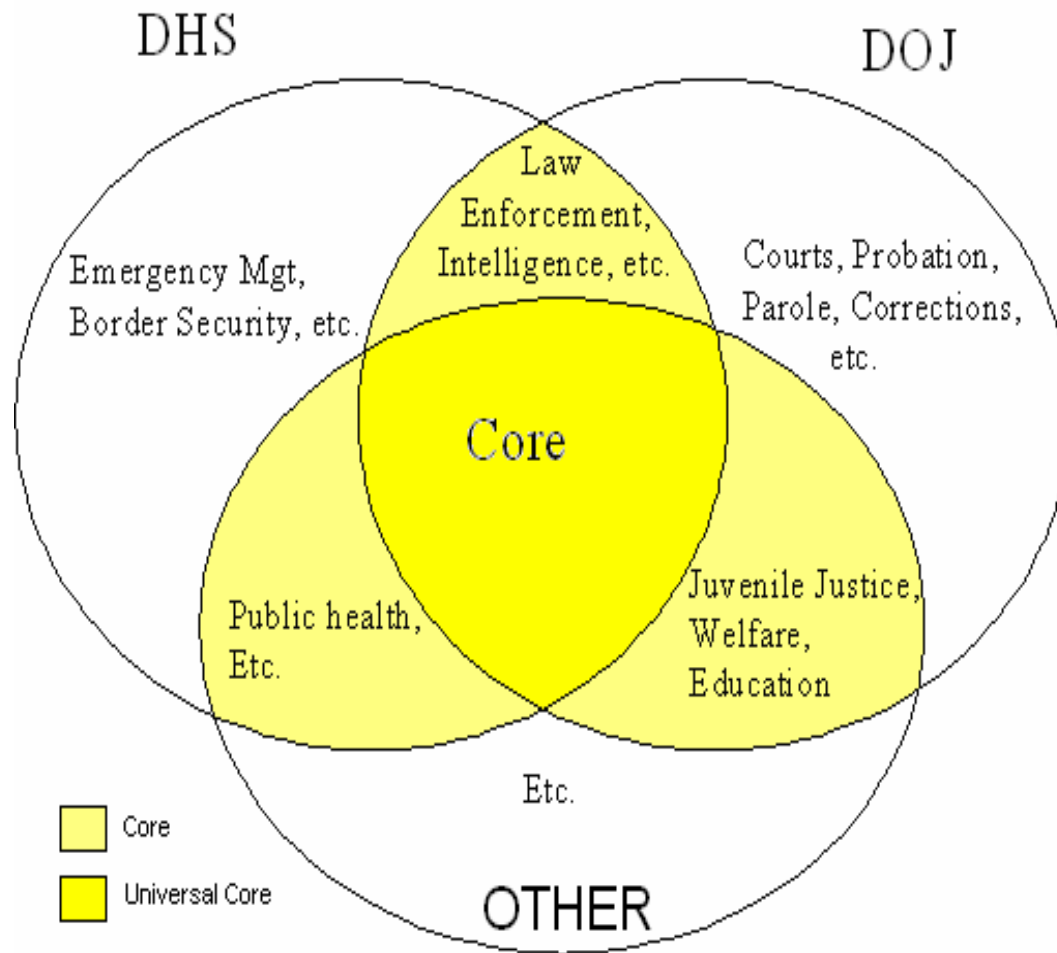
- Description and Specification Documents
  - Interface overview
  - Protocol specifications

- Compliance Assessment Documents
  - Protocol conformance test procedures
  - Performance methods and measurements
  - Performance recommendations
  - Interoperability test process and procedures

- Project 25 – a narrow bandwidth wireless solution for mission-critical voice with a promising backbone structure between systems to support voice plus broadband services

- Project MESA – an international partnership to develop globally applicable technical specifications for mobile broadband technology

- Project 34 and 4.9 GHz – a broadband solution to support services and applications for incident and jurisdictional area environments in the FCC allocated Public Safety 4.9 GHz spectrum and potentially 700 MHz

- Global Justice Information Sharing Initiative – a "group of groups" to improve inter-organizational communications and data sharing

- Standards Development Organizations
  - Telecommunications Industry Association
  - Institute of Electrical and Electronics Engineers
  - National Institute of Standards and Technology
- Non-traditional SDOs
  - Internet Engineering Task Force

Project 25
Compliance Assessment Program

Eric Nelson
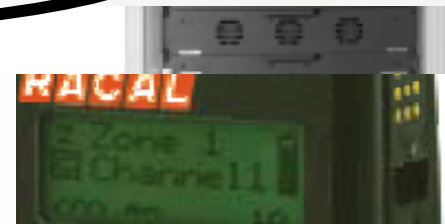
INTEROPERABILITY AND COMPATIBILITY

… The conferees direct the Office of Interoperability and Compatibility (OIC) to work with the National Institute of Standards and Technology and the U.S. Department of Justice to require, **when Project 25 equipment is purchased with such funds, the equipment meets the requirements of a conformity assessment program.** The conferees further direct such a conformity assessment program be funded by this appropriation and be available by the end of fiscal year 2006. …

… The Committee also directs that, within this report, OLES identify a process to ensure **that equipment procured using Federal grant dollars complies with the requirements of the identified standard(s).** At a minimum, the Office of Interoperability and Compatibility [OIC] within the Department of Homeland Security should consider working with NIST and DOJ to require that **all grant dollars for interoperable communication be used for Project 25 compliant equipment that meet the requirements of a conformity assessment program**.

- Of the eight P25 interfaces only the Common Air Interface (CAI) is ready to test

- However, test procedures for the CAI are not complete

- Manufacturers have historically worked in isolation

- So new entrants to P25 sometimes interpret standards differently than the incumbents

- Furthermore, fundamental documents are undergoing extensive revisions, i.e. trunking protocols

- Provide a technical underpinning for manufacturer claims through published test reports

- Increase confidence of public safety community in P25 products through a *veracious* (i.e. honest, truthful, accurate and precise) compliance assessment program

- Structure the program to complement manufacturers' existing development process

- Which will ensure that compliance is designed into P25 products

Compliance requires three types of tests:

Performance

- Do radios A and B meet specifications?

Interoperability

- Does radio A work with radio B?

Conformance

- Radio A and B work together, but do they both comply with the standard?

?
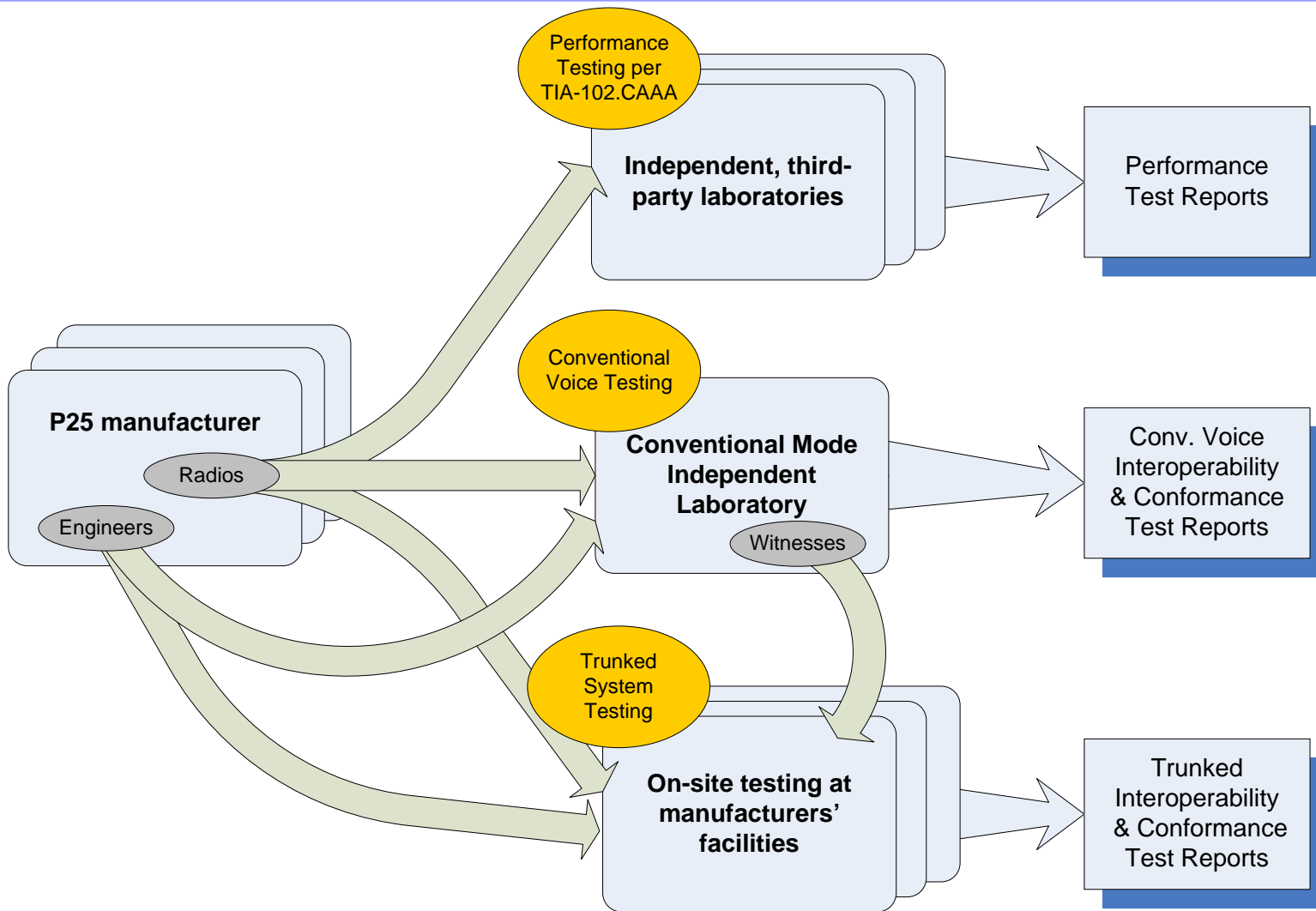
- Outside TIA TR8, leading program development effort through TIA's P25 Compliance Assessment Working Group

- Within TIA TR8, taking a lead role in developing the test procedures through the APIC Compliance Assessment Process and Procedures Task Group (CAPPTG)

- Validating conformance and performance tests for other interfaces (beside CAI)

- Developing reference implementations where appropriate

Questions?

www.safecomprogram.gov

info@safecomprogram.gov

1-866-969-SAFE

BACKUP Slides

- **Goal: Develop and approve P25 Suite of standards for public safety land mobile radio systems**
  - ISSI (Inter-RF Subsystem Interface) Messages and Procedures
    - Expected to be approved for publication by TIA in March 2006.
  - P25 Statement of Requirements (P25 SoR)
    - Expected to be approved for publication by P25 Steering Committee in April 2006.
  - ISSI Measurement Methods for Voice Services
    - Work delayed until after higher priority standards are finished. Anticipated approval 4th Quarter 2007.
  - ISSI Performance Recommendations for Voice Services
    - Work delayed until after higher priority standards are finished. Anticipated approval 4th Quarter 2007.
  - FSSI (Fixed/Base Station Subsystem Interface) Messages and Procedures (Conventional Voice)
    - A completed FSSI standard was approved by the TR8.19 group on January 11, 2006 for publication as a TIA standard.
  - CSSI (Console Subsystem Interface (CSSI) Messages and Procedures
    - Completion in January 2006 of a new TIA standard for the FSSI that enables direct console control of fixed/base station equipment serves as a basic CSSI standard. Further development of the CSSI will follow upon continued development of the ISSI and FSSI throughout CY2006. Anticipated approval 4th Quarter 2007
  - P25 Systems Architecture
    - Next draft due April 2006. Completion date unknown.
  - P25 Decision Tree
    - Ongoing report. Next update due April 2006.
  - ISSI Enhancements Standards
    - Work began February 2006, publication expected in 2007.

Multiple Frameworks exist and all of them are based upon the work of Zachman or Spewak. Some of them have direct mappings from one to the other and some are built specifically to comply to the same standards as another.

DoDAF

FEAF

SPEWAK
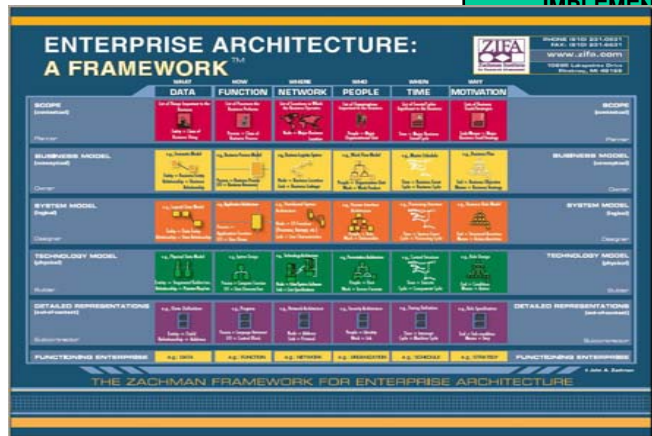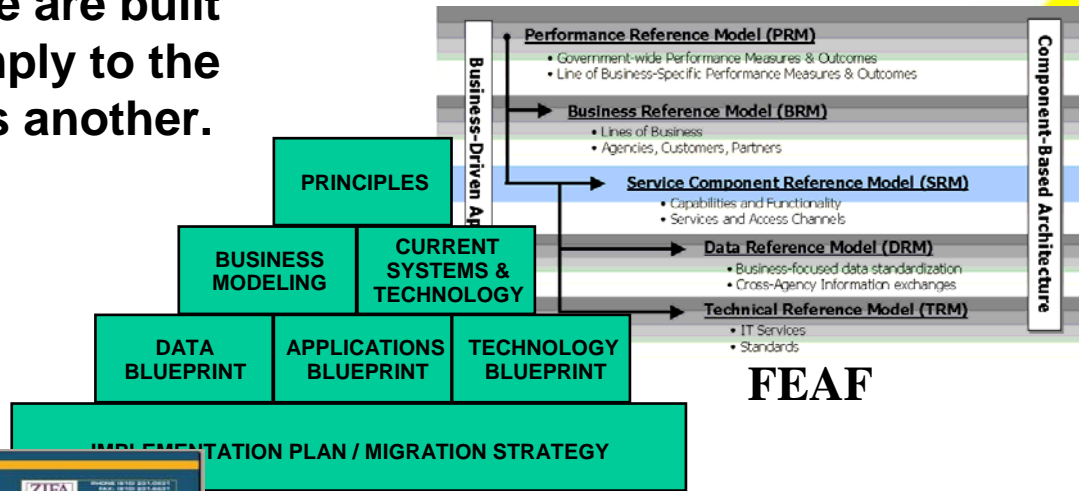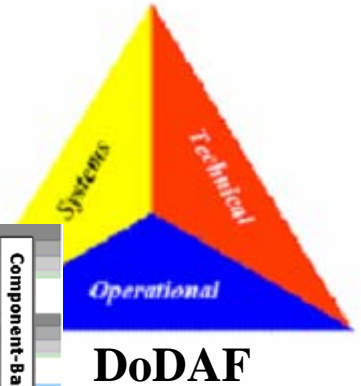
ZACHMAN

FEAF: Federal Enterprise Architecture Framework
DoDAF: Dept. of Defense Architecture Framework