Joint Warning and Reporting Network (JWARN) Briefing to CBIS

January 2007

CDR Michael Steinmann, USN
JWARN Acquisition Program Manager
Joint Project Manager Information Systems
michael.steinmann@jpmis.mil

JOINT Warning and Reporting Network (JWARN)

Mission:

Enable immediate and integrated response to threats of contamination by weapons of mass destruction through rapid warning and dissemination of Chemical, Biological, Radiological and Nuclear (CBRN) information.

Warfighter Needs

- Collect, generate, edit and disseminate NBC reports and plots and provide a means of ensuring all addressees have received a sent message
- Application support for FBCB2, C2PC, GCCS-J, GCCS-M, GCCS-A, and GCCS- AF COE Level 7 / DODIIS
- Allow NBC reports (NBC-1/NBC-4) to be formatted and transmitted within 2 minutes and allow operator selection of automatic, delayed or on-command sending of NBC reports
- Automated sensor interfaces for M8A1, M21, M22, IPDS, ADM 300, AN/VDR2, JBPDS

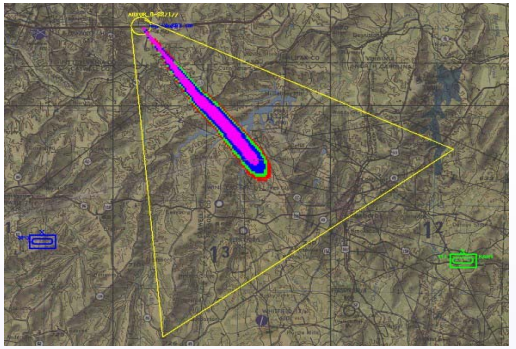
Description

- JWARN is an ACAT III (DOT&E Oversight Program) information system that networks NBC sensors, mission application software tools, and C4ISR systems
- JWARN builds on current manual capabilities by fully integrating with COE-based and tactical C4ISR systems
- Automatically generates alerts for warning and dewarning affected forces
- Automatically generates hazard area plots

Core Capabilities

JWARN provides the Joint Force Commander with the capability to:

- **Report CBRN and Toxic Industrial Materials (TIM) hazard detection**
  - **Collect, generate, edit and disseminate NBC plots on Command and Control (C2) platforms to provide a common operational picture (COP) for the warfighter**
  - **Collect, generate, edit and disseminate NBC reports (NBC-1/NBC-4)**
- **Analyze detections to enable identification of the hazard and plot affected locations**
  - **Auto generation of ATP-45 hazard warning area**
  - **Generation of more detailed hazard area plots using JEM**

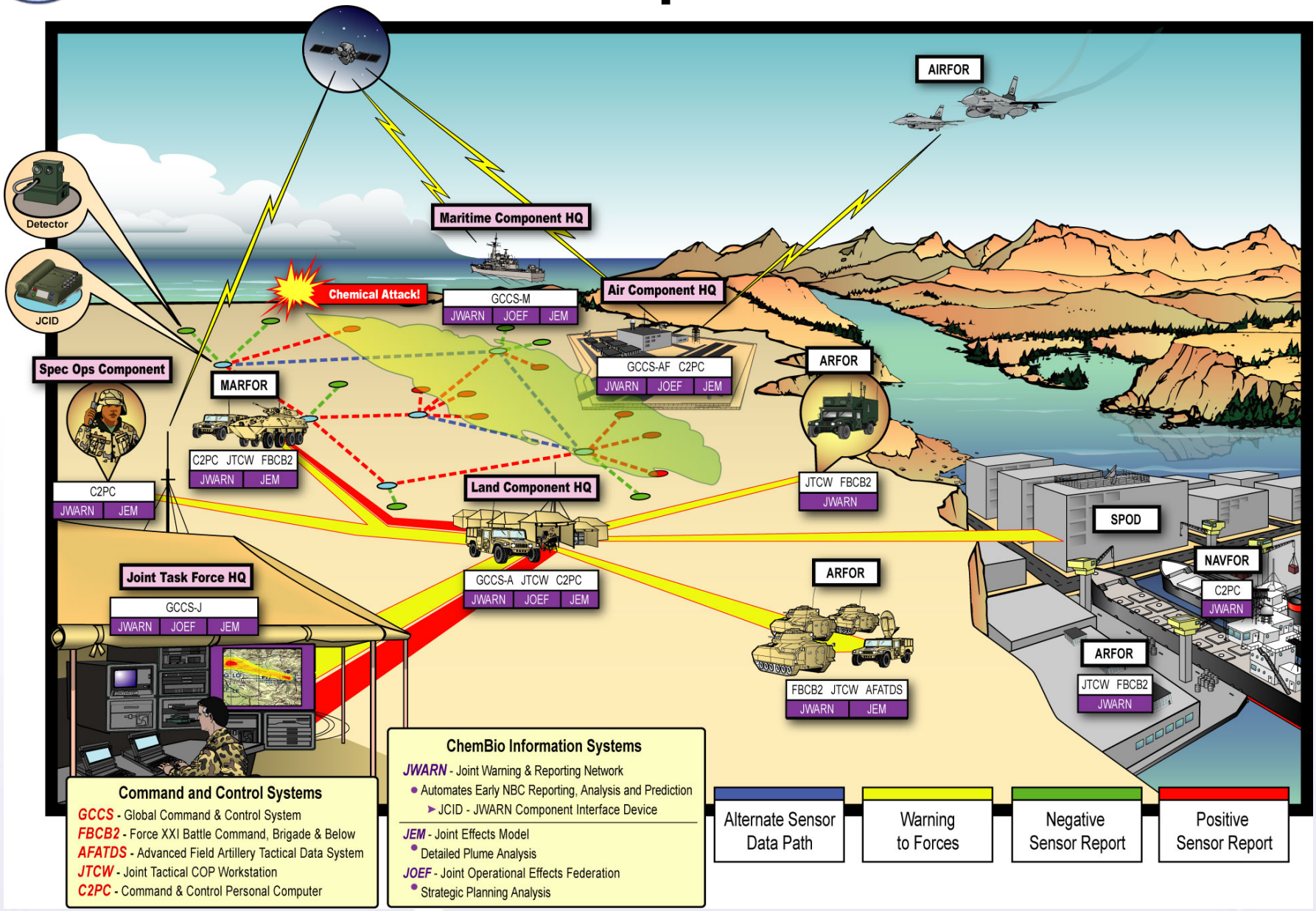


- **Disseminate warning and de-warning information to affected units**
- **Auto retrieval and archiving of event data to enable post-operations forensic evaluation**
- **Control and configure a local sensor network**
  - **Auto sensor interfaces for M8A1, M21, M22, IPDS, ADM 300, AN/VDR2, JBPDS**

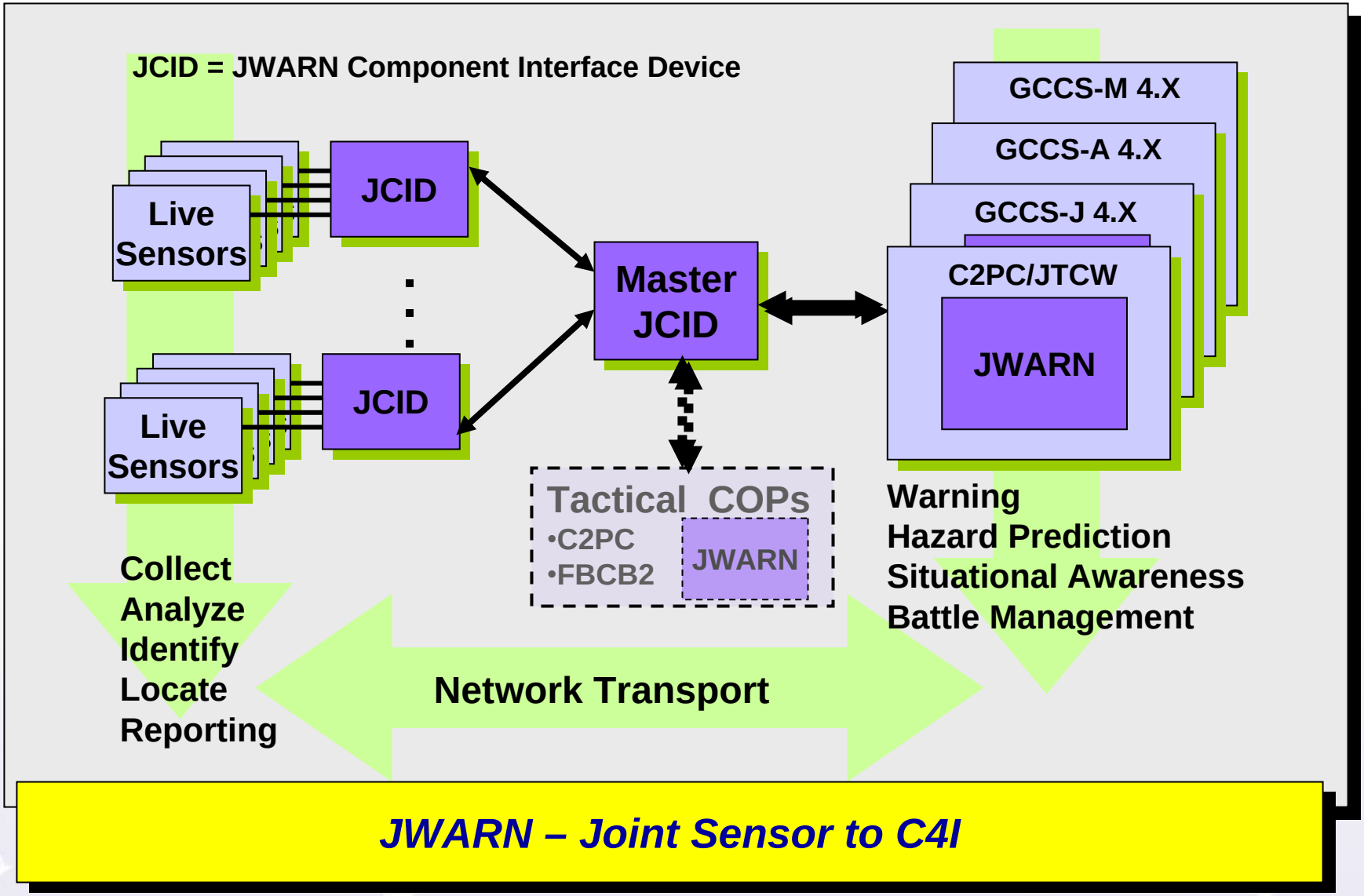
Benefits to the Warfighter

- Automates a process which was previously manual and error prone
- Minimizes time from detection to warning (less than 2 minutes)
- Provides timely warning and de-warning of affected units to maximize combat effectiveness
- Automates recording and archiving of exposure data which will enable more effective forensic analysis
- Compatible and integrated with current and future Command & Control systems

JWARN Operational View



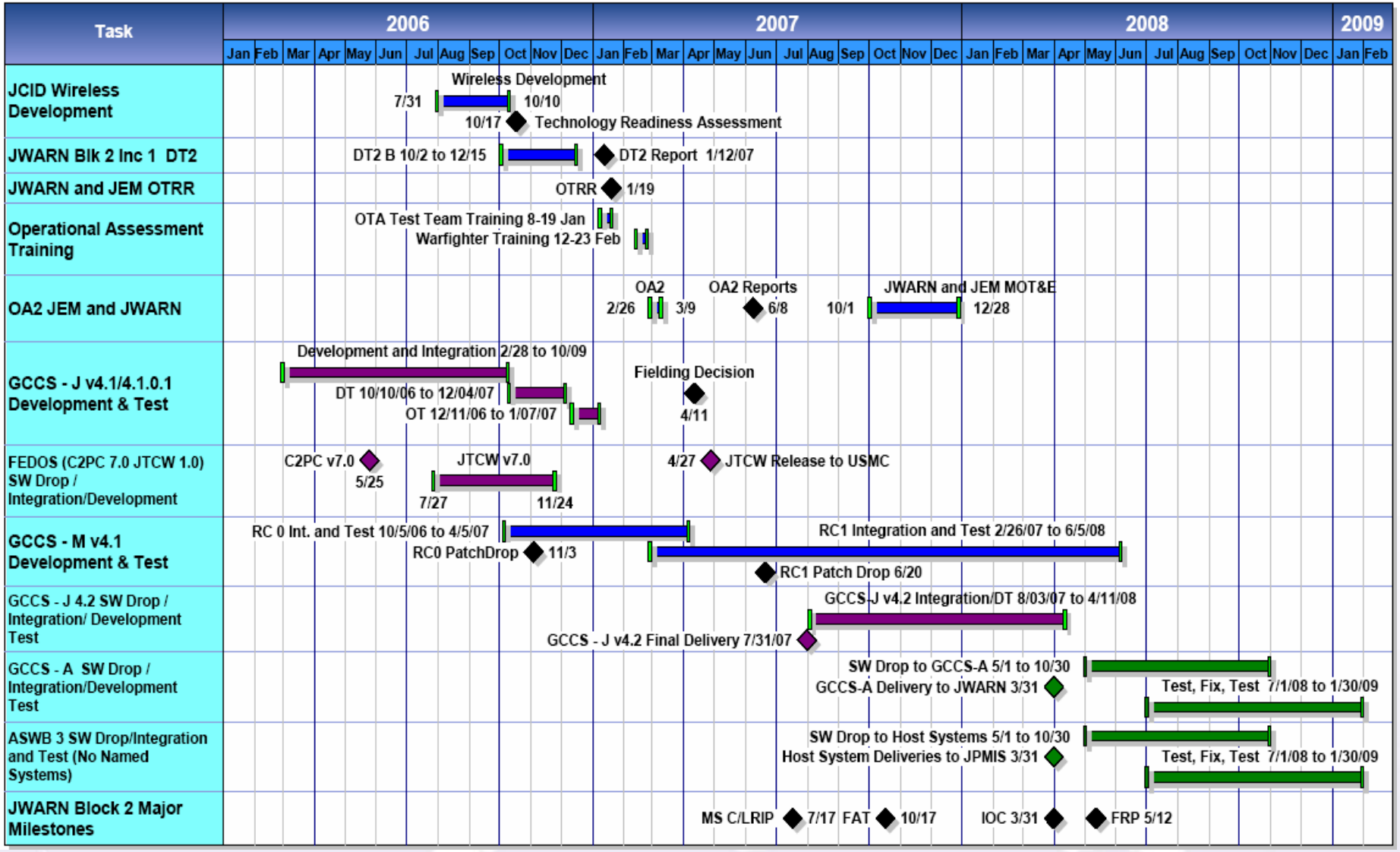
JWARN System View



Program Acquisition Strategy

- **Two Increments of development followed by Pre-Planned Product Improvement**
- **Increment 1 (FY06 – FY09)**
  - **Increment 1 development complete**
    - **Developmental Testing and Operational Assessment in progress**
    - **Milestone “C” - July 07**
- **Increment 2 (FY08 – FY 12)**
  - **Increment 2 design and development FY08 – FY09**
    - **Maintain JWARN Baseline for various C4ISR systems**
    - **Accommodate new C4ISR systems**
    - **Web enabled**
    - **Full integration with JEM & JOEF**
    - **IOC FY10, FOC FY12**

JWARN Program Schedule



JWARN Technical Challenges

- Integration of multiple Chem-Bio sensor interfaces (Legacy and Developmental)
- Compatibility with multiple Service-specific implementations of C2 systems
- Evolving national C2 system architecture(s)
  - Net Centric Enterprise Services (NCES)
  - Joint C2 (JC2)
- Web enablement
- Wireless connectivity incorporating Information Assurance (IA) requirements
- Integration with JEM, JOEF and other major acquisition programs

Interim Wireless JCID Solution

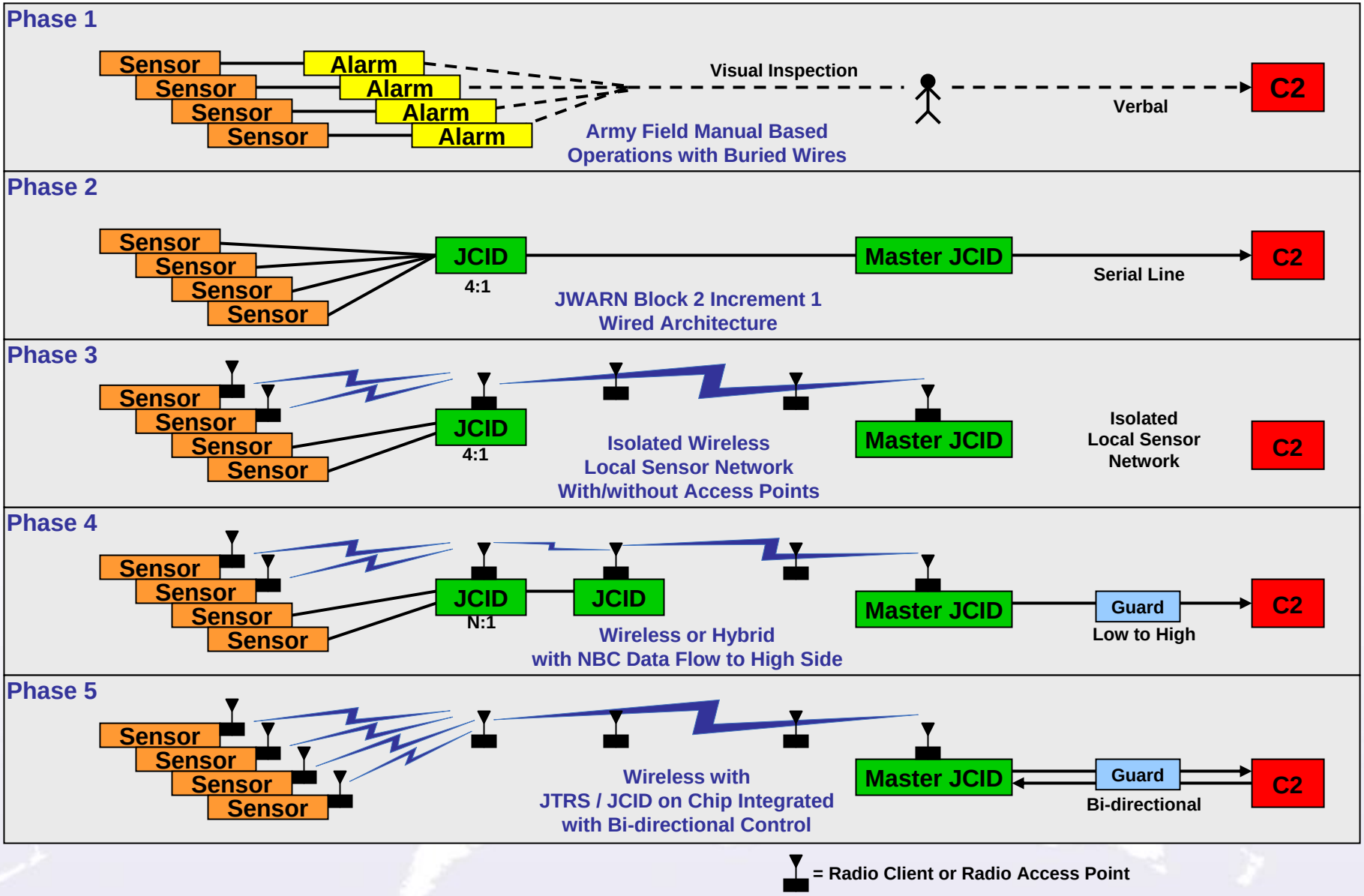
- **Wireless technology solutions exist**
  - **Provide sufficient coverage for typical air base**
  - **Supports rapid mobile dismounted deployment**
  - **Meet IA requirements**
  - **NSA certifiable**
- **Supports a “crawl”, “walk”, “run” development cycle**
- **Solution is radio and network “agnostic”**
  - **Preserves capability to backfit JTRS solution when available**

Requirements

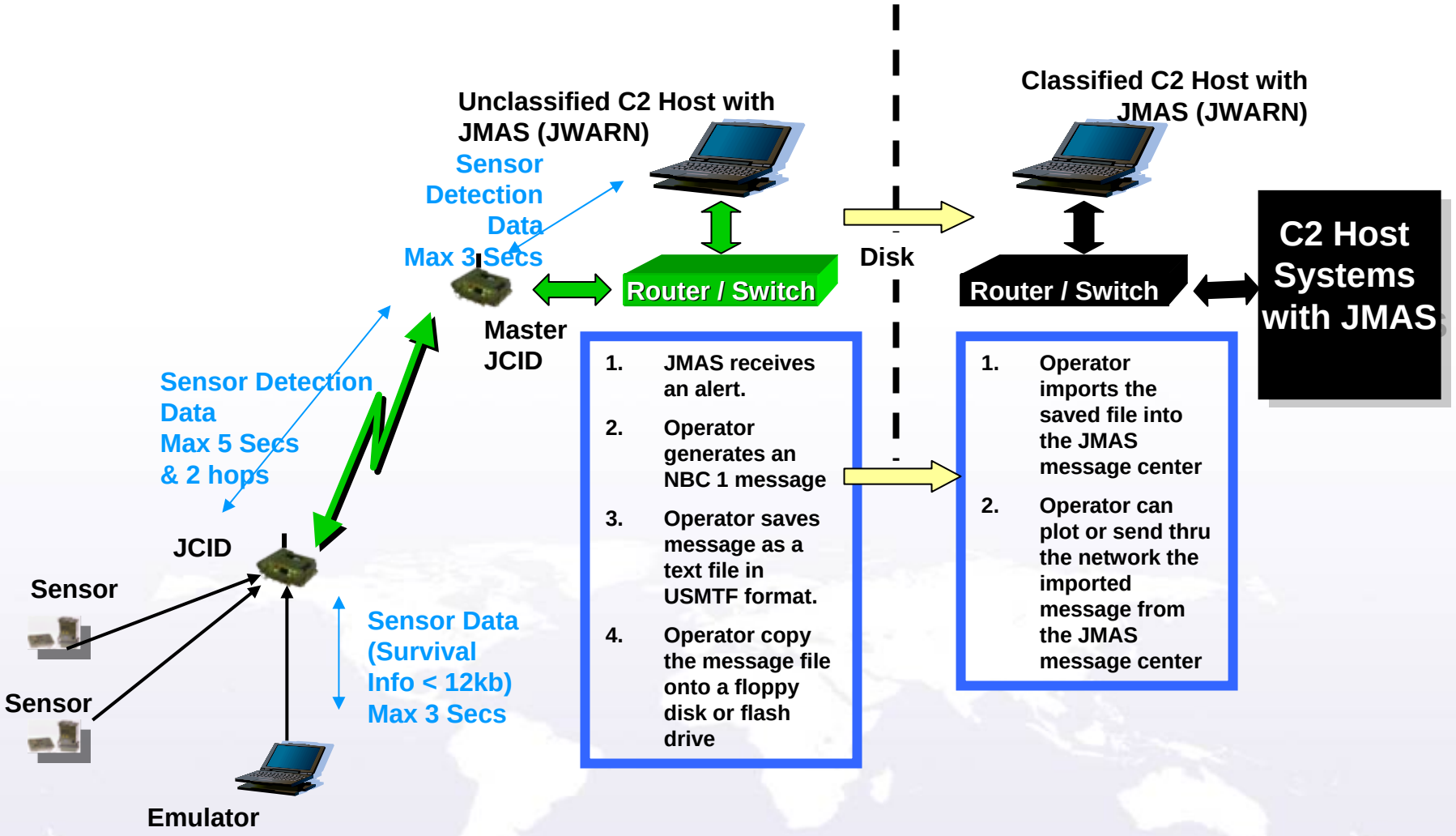
Simple “Radio Shack” solution

- Technology available now
- COTS/GOTS hardware
- Radio agnostic
- Currently Fielded (DoD or other Agency)
- Adaptable to current JCID and JMAS software
- Configurable to support Fixed Site (e.g. AF Base); Mobile/Dismounted applications
- Criteria includes Cost, Performance and schedule
- Solution can be ready for MOT&E (Oct-Dec ’07)
  - Implies DT/OA, Environment Tested, plus SSAA/IATO/C&A by NSA
  - Supports Wireless capability for MS/C (17 Jul 07) decision

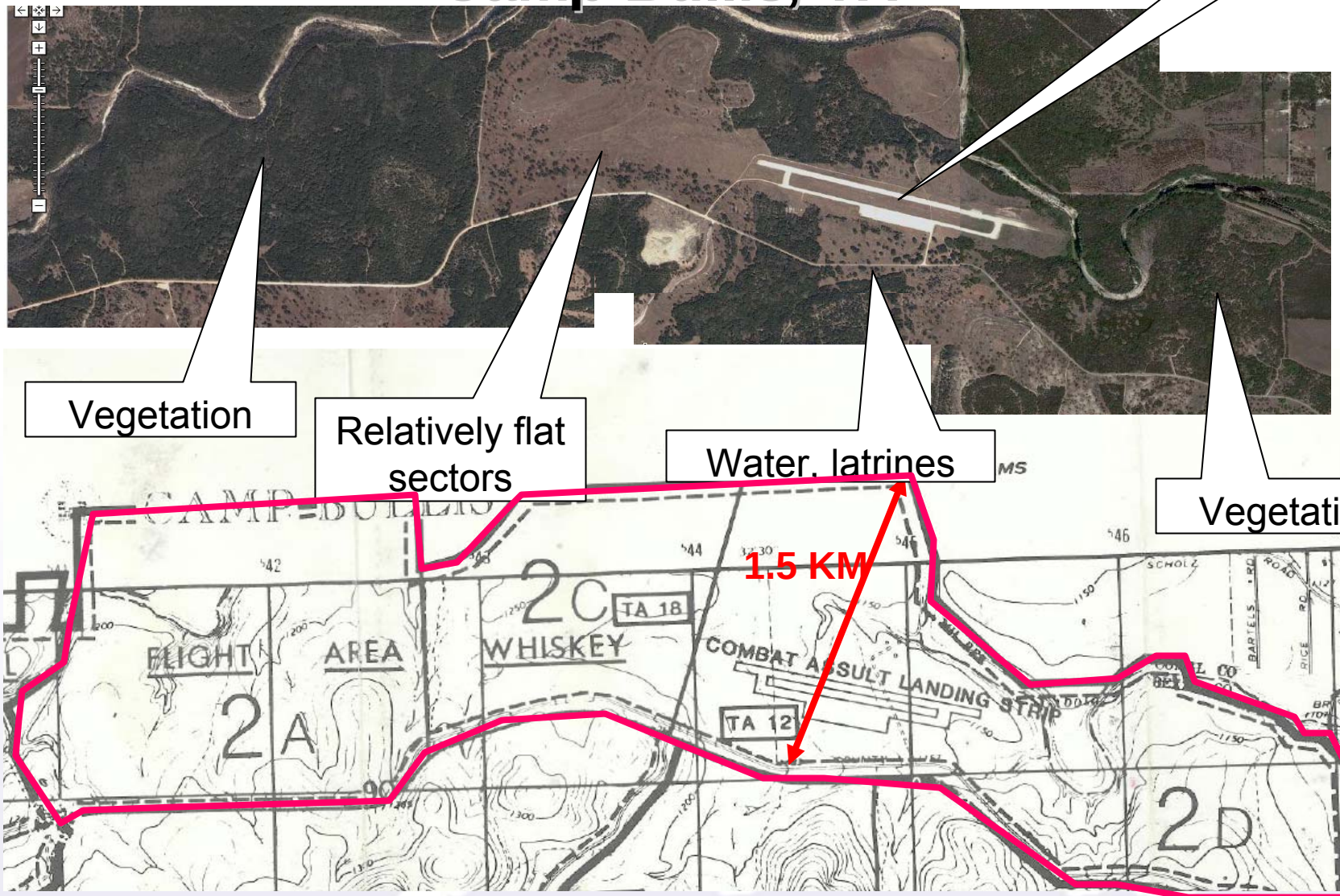
CBRN Sensor to C2 Evolution



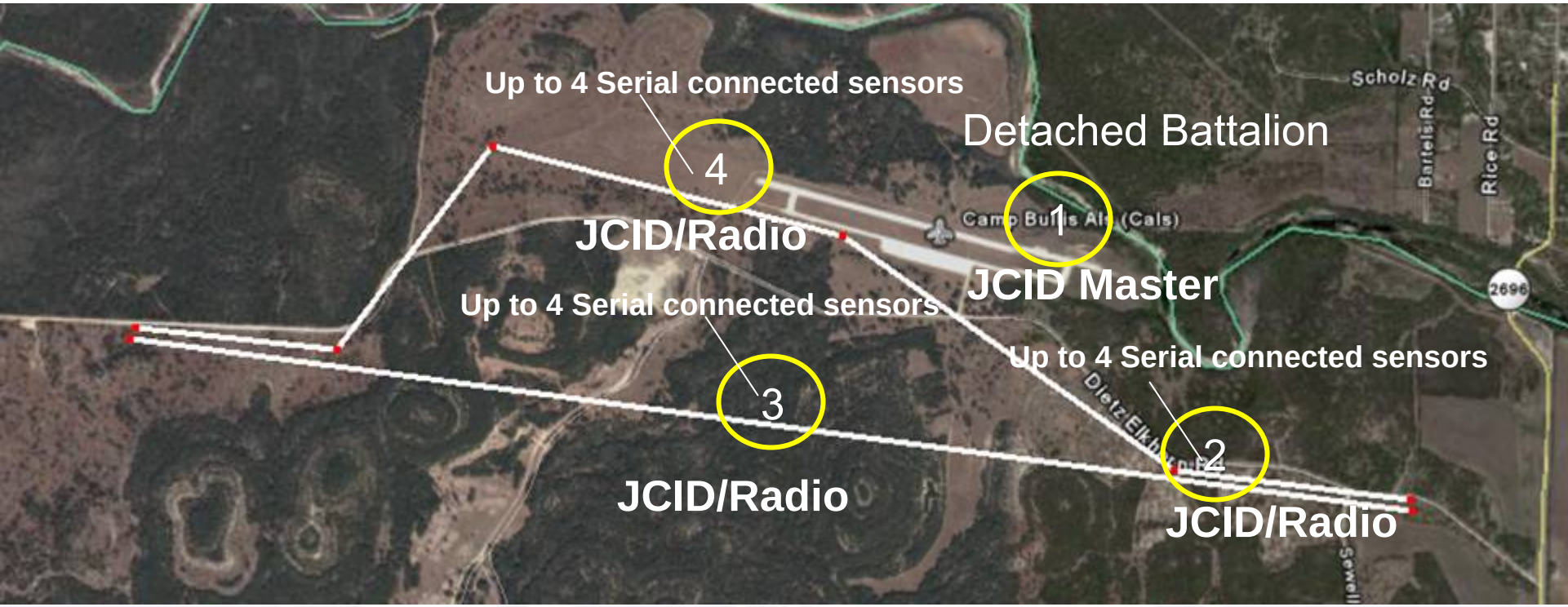
Initial System Architecture



Wireless Assessment
Camp Bullis, TX



Wireless Mesh Network Deployment



Circles indicate hardware placement

Wireless Path Forward

- Evaluate and procure COTS-based interim wireless solution to support MOT&E and IOC
- Assess prototype system by mid-October 06
- Conduct Wireless DT (Q3 07)
- Seek NSA certification for Cross Domain solution
- Procure sufficient numbers of wireless JCIDs to support MOT&E and IOC

Technology Transition Agreements (TTA)

Current Initiatives

- **TTA IS 008 - Sensor Alert Verification for Incident Operational Response (SAVIOR)**
- **TTA IS 015 - Shared Common Operational Picture (COP)**
- **TTA IS 016 – JCID Thin Client Server**
- **TTA IS 017 – InterLAN Service Connection Manager (ILSCM)**
- **TTA IS 021 – JCID on a Chip**

Sensor Alert Verification for Incident Operational Response (SAVIOR)

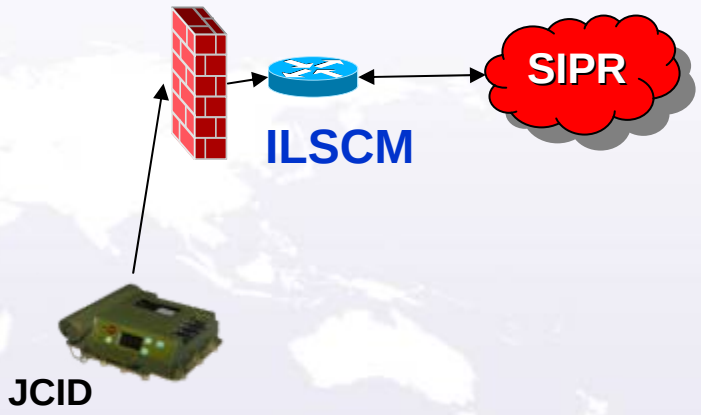
- **Description:** Develop information fusion algorithms and software to reduce chemical point sensor false alarms when used for fixed site protection.
- **S&T Goals:** Algorithms will be developed for jointly processing multi-sensor data from multiple sensor nodes as well as contextual information regarding sensor health and known activities that may affect air quality. Attempt to distinguish attacks from normal events by comparing the temporal response across a network of sensors to everyday occurrences to various attacks.
- **Transition Year:** 2008

JCID Thin Client Server

- **Description:** Develop a JCID thin client server that responds by sending files over a TCP-IP link (either wired or wireless) and communicating with the sensor in its proprietary protocol. Supported formats include HTML and XML as well as standard file encryption. Allow the incorporation of new detectors by modifying external spreadsheets. Simple tables (editable in a spreadsheet) are modified to define the parsing of the digital sensor information into elements of a sensor XML schema and HTML page.
- **S&T Goals:** The objective is to take an existing sensor interface device, developed for chemical sensor fusion, enhance its capabilities to meet JCID compliance and demonstrate this capability for JWARN within 12 months. Deliver 25 units in one year.
- **Transition Year:** 2008

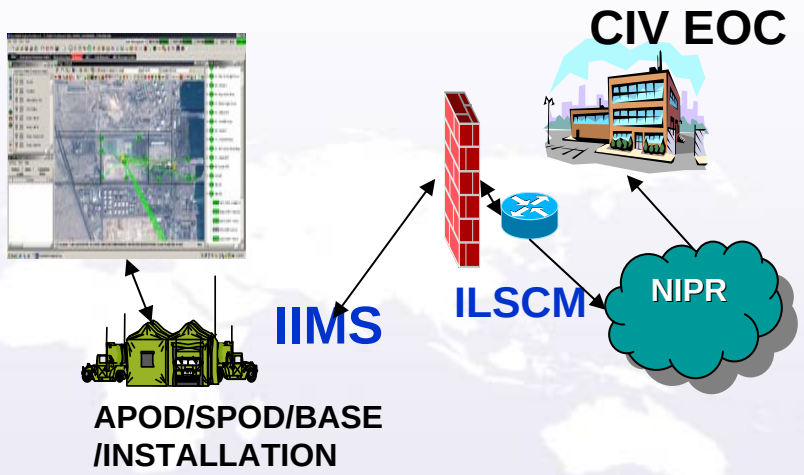
InterLAN Socket Connection Manager (ILSCM)

- **Description:** Employ a bi-directional data guard to provide secure data between unclassified networks and classified networks.
- **S&T Goals:** Adapt existing technology from the Tomahawk program to build a data guard between a sensor network and a C4I system. Process the solution all the way through the DITSCAP process and get an IATO.
- **Transition Year:** 2008



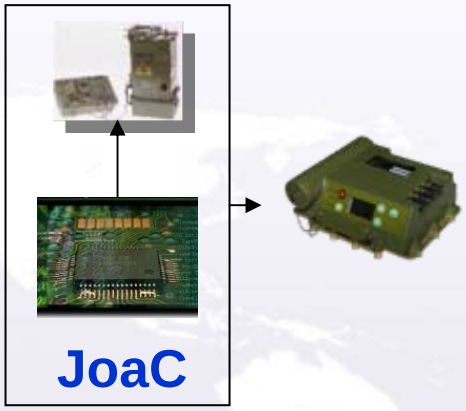
Shared COP

- **Description:** Shared COP explores issues related to sharing information between .mil and .gov networks. Investigate cross enclave information sharing issues.
- **S&T Goals:** Data sharing, messaging standards, cross domain guard solutions, information presentation, accessibility issues, data relevancy
- **Transition Year:** 2007

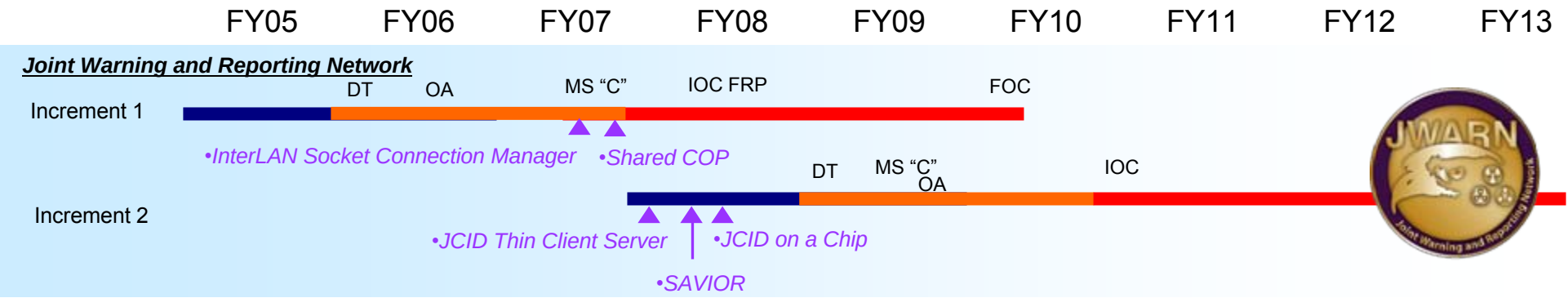


JCID-on-a-chip (JoaC)

- **Description:** This effort proposes a software-defined sensor concept, architecture and approach to developing Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) sensors and CBRNE sensor capability that is hardware independent and can support the ability to load to key supported hardware sensor system technologies, e.g. Field Programmable Gate-Array's (FPGA).
- **S&T Goals:** Build software and/or firmware solution for embedding within future detectors. Work with JPM CA and JPM IS and others in the CBRN COI to develop standards. Collaborate with developers of Holster
- **Transition Year:** 2008



Acquisition Pull: The Technology Transition Paradigm



Backup Slides

What is a Mesh Network

- **Mesh Networks are an advancement in the 802.11x technology.**
  - **A mesh network is a self forming self healing network that forms multiple connection paths between access points by creating a routing table of available access points, thus providing redundancy by rerouting communications.**
  - **A high performance mesh access point contains at least two radios, one which forms the connection point for end users, and the other radio forms the backhaul connection or relay point between the access points in the network.**
    - **In a single radio mesh, the client traffic and mesh traffic share the same radio link, putting traffic on the same channels. This effectively cuts the mesh network performance by two-thirds at a minimum.**
  - **The NSA has approved the usage of 802.11x networks and set the requirements for security for the usage of 802.11x. These guidelines are laid out in the 8100.2, the security requirements dictated in this instruction are being enforced within the Mesh network deployments.**