

# Joint Capability Technology Demonstration (JCTD) Proposed FY08 Start



## *Joint Force Protection Advanced Security System (JFPASS)*

*24 October 2007*

*Mr. Carlos “Kiko” Lama  
JFPASS JCTD Technical Manager  
carlos.lama@navy.mil  
540-653-3306*



# Joint Warfighting Problem



- **Current Force Protection technologies and CONOPS do not provide a comprehensive, effective, and sustainable Joint FP capability**
- **Fielded FP systems do not provide comprehensive situational awareness**
- **Fielded FP technologies absorb too much manpower**
- **Fielded FP systems are too costly, there are too many variants and redundancies**

*Force Protection systems are DISJOINTED and INEFFICIENT*



# Joint Warfighting Problem



**Burden / risk on warfighter**



**Ineffective FP C2**



**Costly**



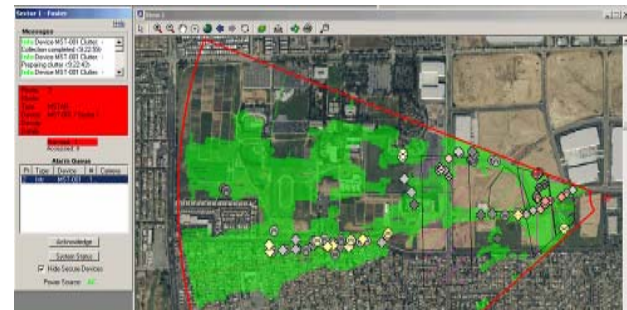
# JFPASS Capabilities



**Non-intrusive Inspections**



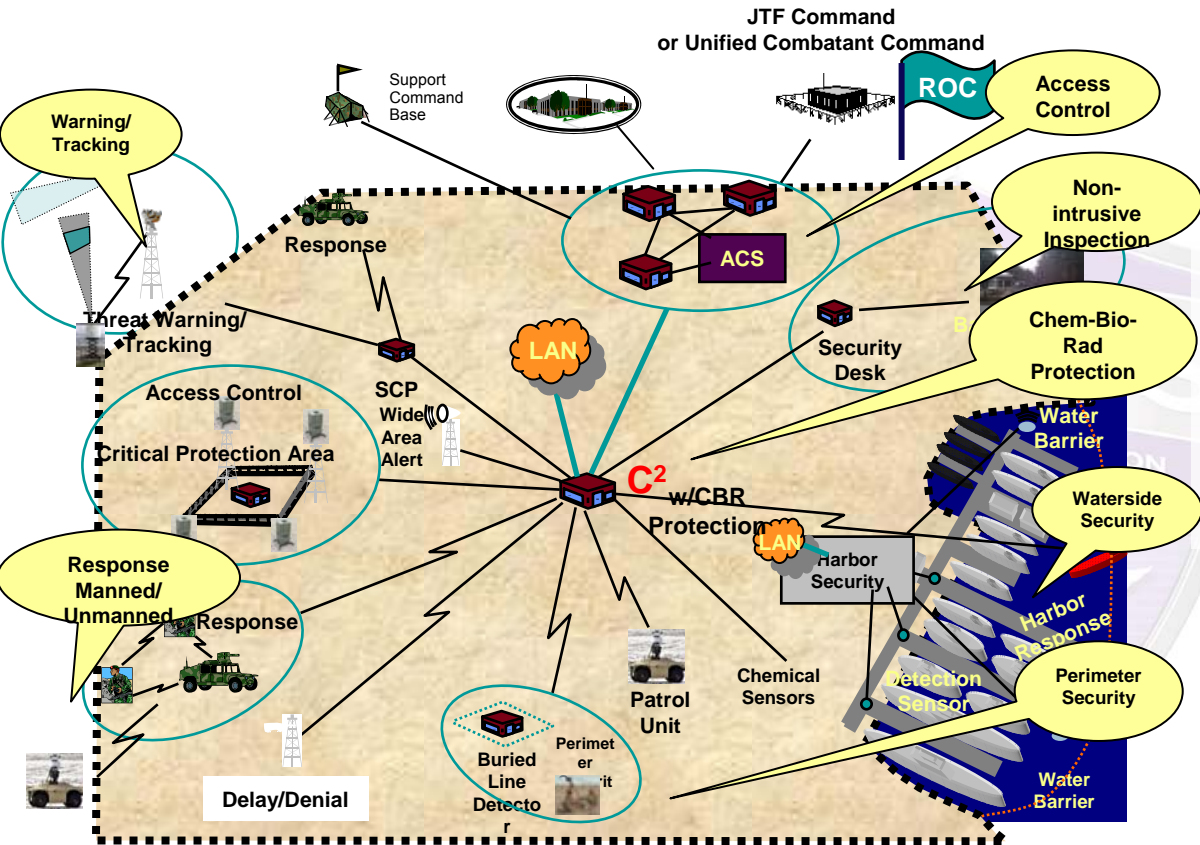
**Unmanned Systems**



**Common Operational Picture**



# JFPASS Operational View



- Demonstrate, assess, and transition an integrated Joint FP capability
- Demonstrate integration via C2 Architecture
- Field the Joint FP capability at OCONUS installation, leave-behind system with sustainment
- Develop CONOPS and architecture (blue prints) for future Program-of-Record for an integrated Joint FP capability

*Technology & CONOPS,  
Architecture (Blue Prints)  
Accelerated Capability  
Informed Requirements*

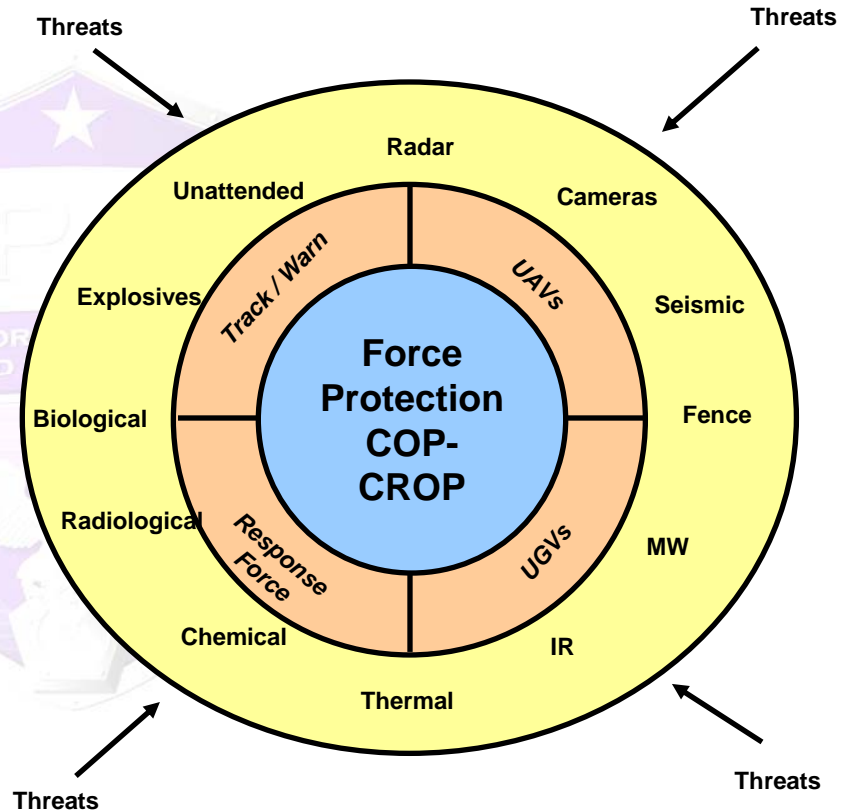
*INTEGRATE ... and ... AUTOMATE  
Leverage benefit of integrated systems for Joint FP*



# JFPASS Technical Approach



- Comprehensive situational awareness will be attained by integrating disparate sensor technologies (new and legacy)
- Effective use of personnel will be attained by maximizing use of unmanned and unattended technologies
- Construction of a common operational picture based on relevant sensor data (via sensor fusion) will provide improved situational awareness
- A common C2 architecture for FP is necessary to provide scalable, tailorable solutions.
- A standard communication protocol will lead to cost reduction by providing interoperability guidance for current and future FP systems.





# Joint Capability Objective

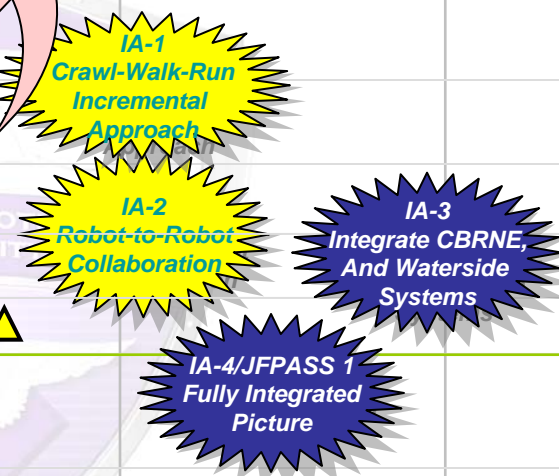
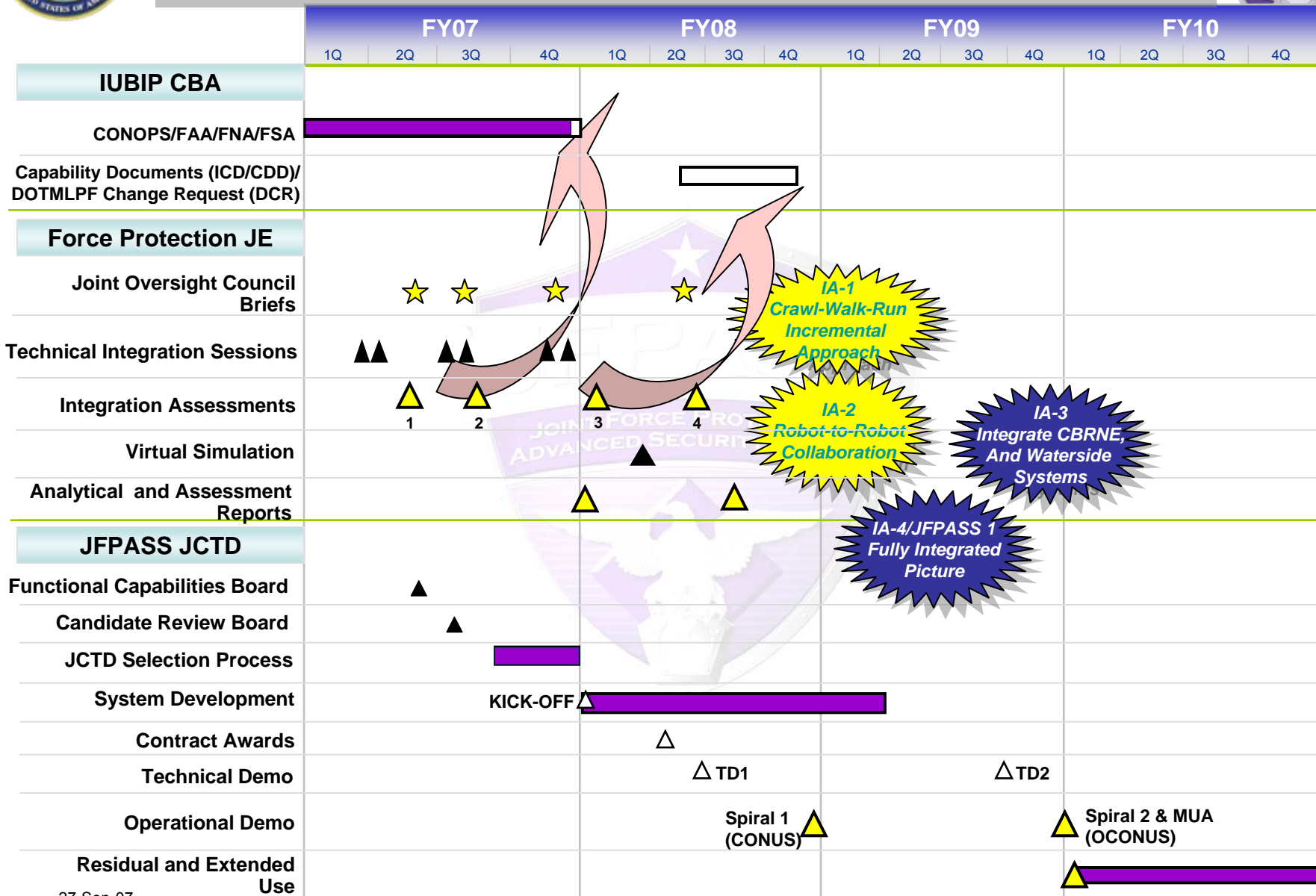


- **Demonstrate, assess, and transition an integrated Joint FP capability, that provides:**
  - Access Control
  - Perimeter Security
  - Non-Intrusive Inspection
  - Waterside Security
  - CBRN sensing and protection
- **Demonstrate integration via C2 architecture, to include:**
  - Standard / scalable connectivity (plug & play)
  - Common and integrated operational picture
  - Decision support system
  - Reduced workload
  - Affordable logistics and maintenance
- **Field the Joint FP capability at OCONUS installation, leave-behind system with sustainment and transition plan**
- **Establish CONOPS and develop integrated architecture (blue prints) for future Program-of-Record (POR) for an integrated Joint FP capability**

*INTEGRATE ... and ... AUTOMATE*  
*Leverage benefit of integrated systems for Joint FP*



# Joint Force Protection Capabilities Schedule







# IUBIP Capabilities Addressed by JFPASS

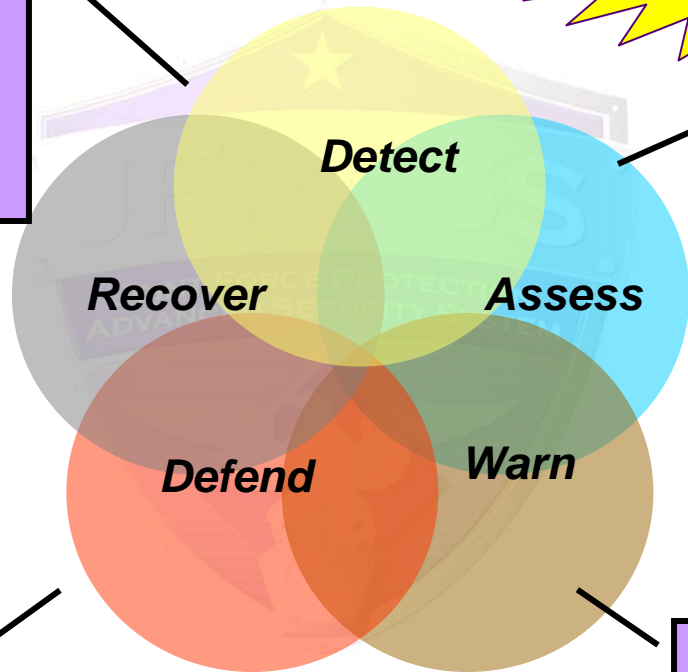


**JFPASS JCTD will address the Capabilities Derived from IUBIP Capability Based Analysis in WHITE text**

**Detect Full Range of Activities**  
Sense / Track Activity  
Conduct Surveillance  
Conduct Reconnaissance  
Collect Information  
Manage Sensor Networks / Capabilities  
Integrate Sensor Capabilities

**Reallocate & Recover Capabilities/ Resources**  
Reallocate Capabilities and Resources  
Recover Capabilities

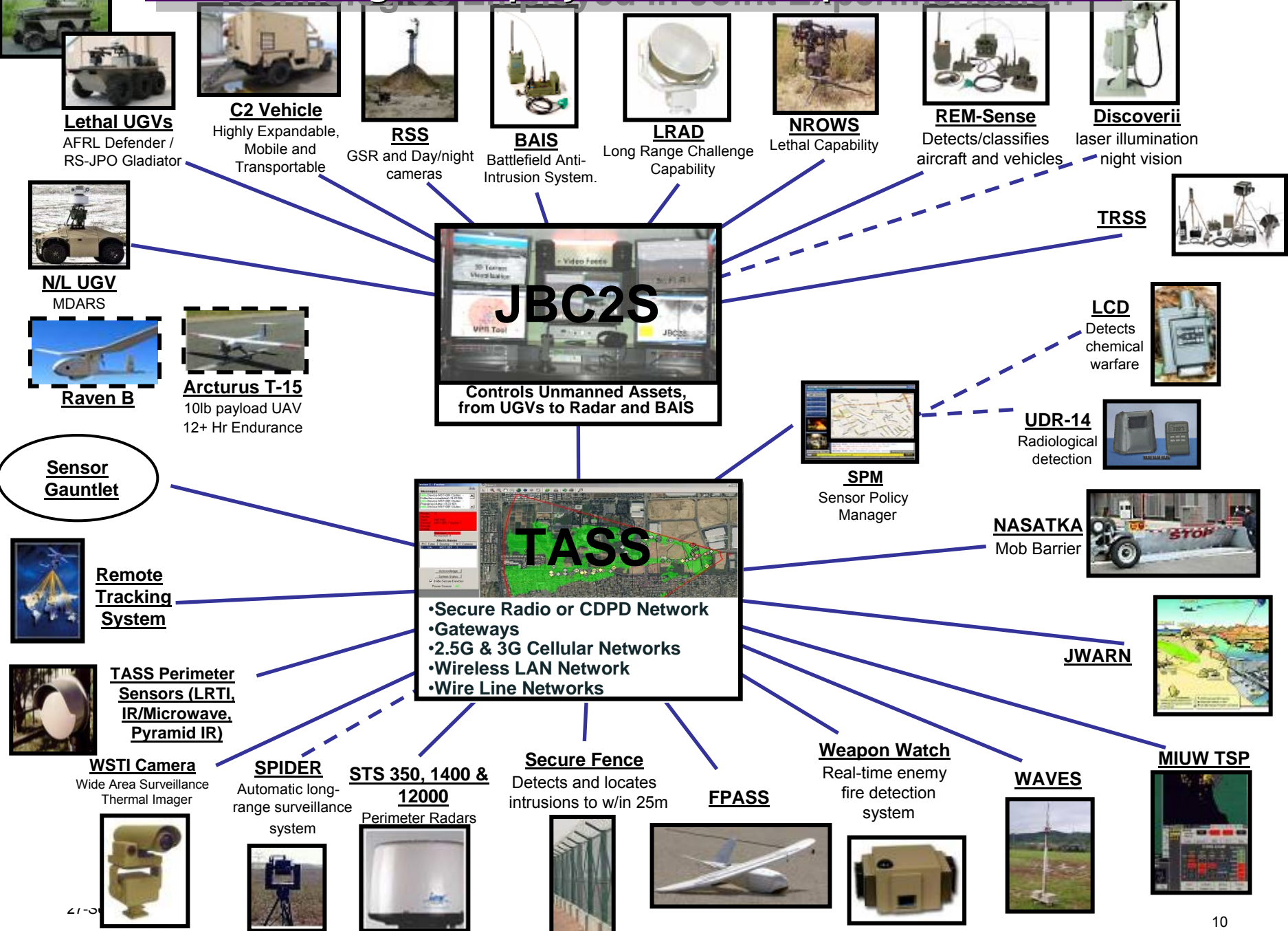
**Prevent, Deter, Restrict, Resist, or Defeat Hostile Actions**  
Integrate C41 Capabilities & Manage Information and Resources  
Execute Passive Measures  
Execute Active Measures  
Mitigate the effects of an Attack



**Recognize, Classify, and Identify Data & Information**  
Evaluate Independent Information  
Integrate Information  
Interpret Information  
Analyze & Synthesize Information  
Develop Intelligence Estimate

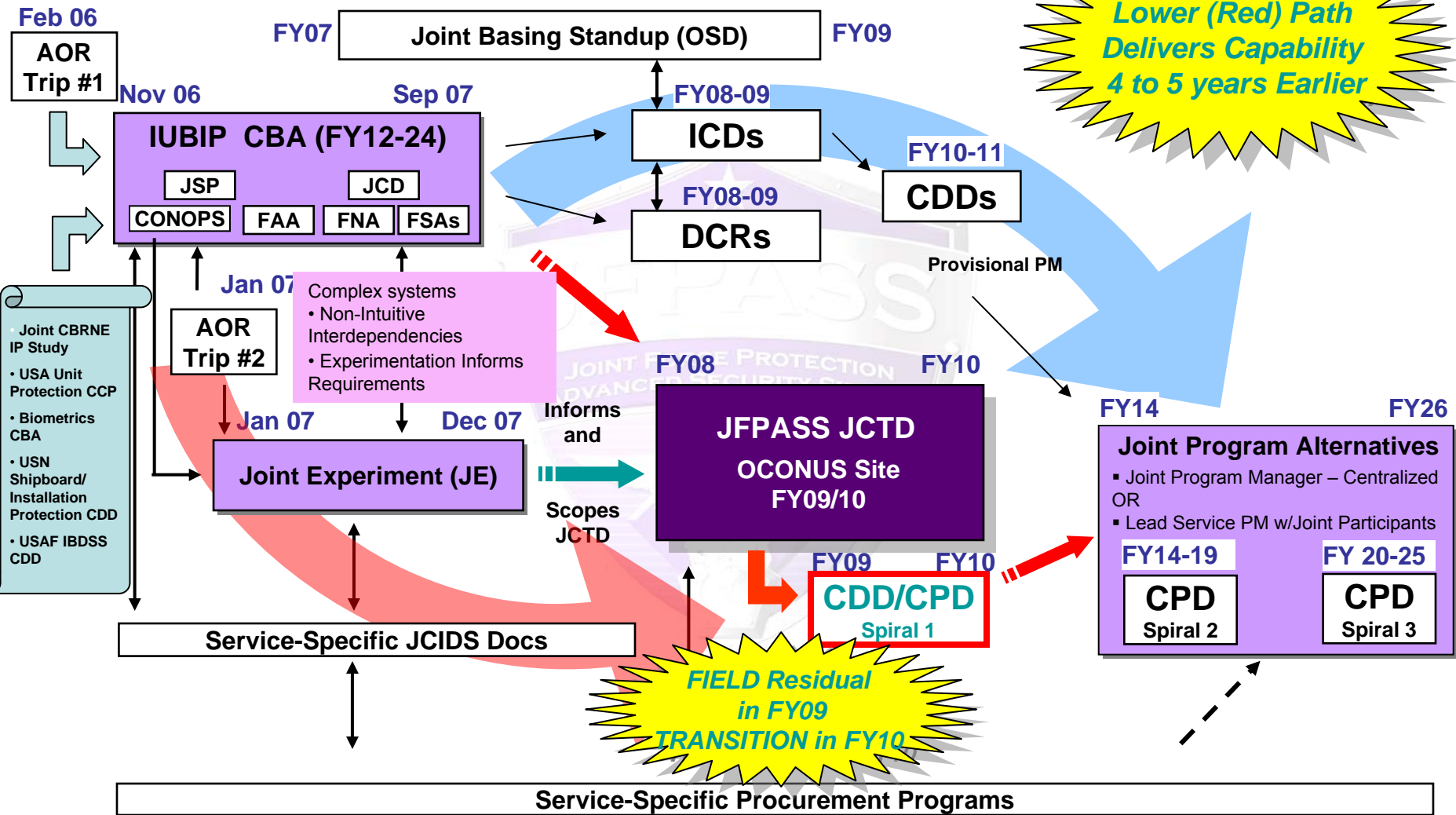
**Disseminate Analyzed Info, Early Warnings, & Decisions**  
Issue Early Warning  
Analyze Mission  
Develop and Prioritize COA  
Make Decision/Issue Orders

# Technologies Employed in Joint Experimentation



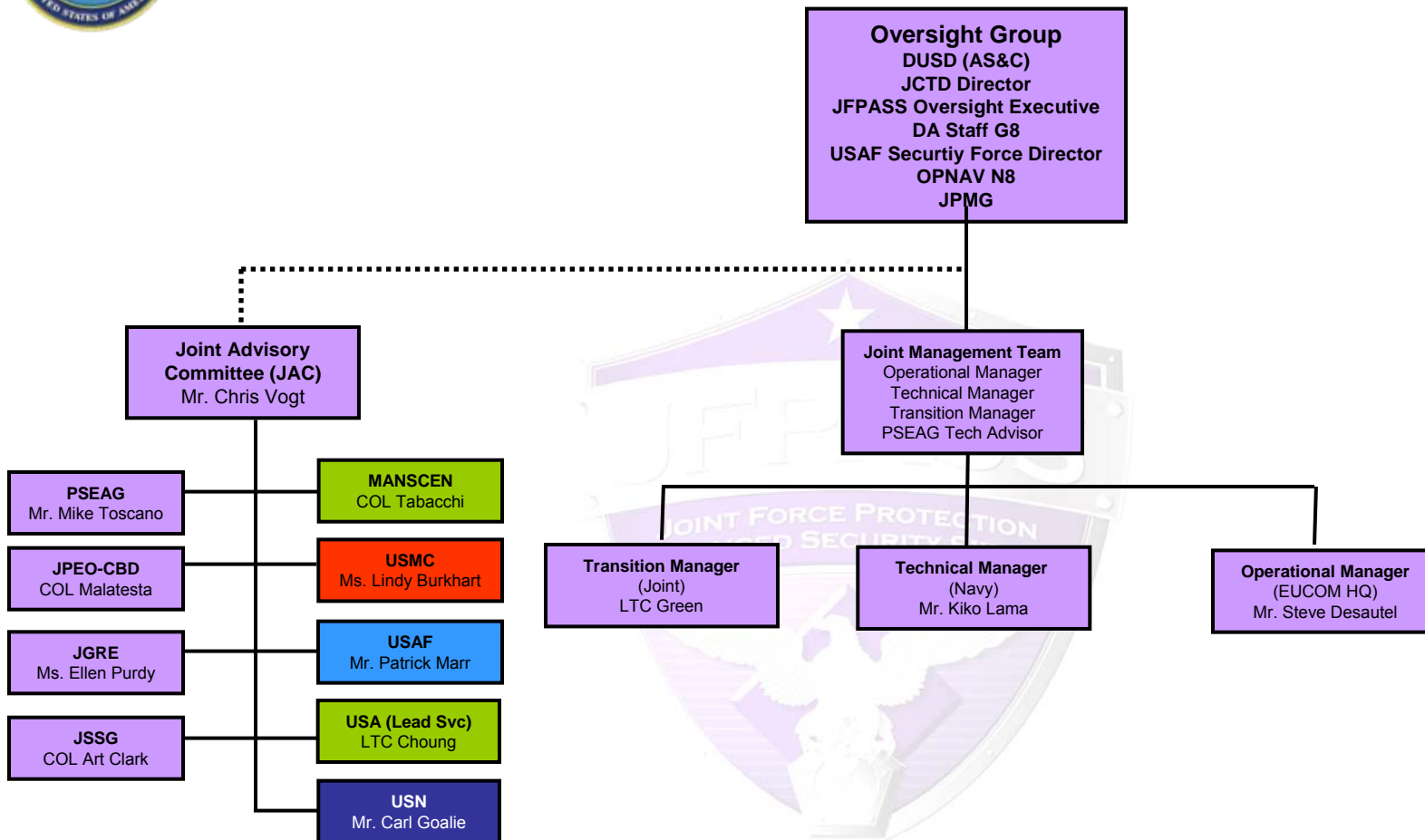


# Joint FP Capability Roadmap





# Oversight and Management Structure





# JFPASS Status



- **Joint Force Protection Advanced Security System (JFPASS) JCTD – Recommended for FY08 “Immediate” Start (OUSD AT&L Report to Congress)**
- **USEUCOM Combatant Command Sponsor and Operational Manager (OM)**
- **Operational Demonstration location – Spangdahlem Air Base, Germany**
- **Kick-off, 10-12 October 2007 (NSWCDD)**
- **Requirements Refinement with USAFE – On-going - 22 Oct – 15 Nov**
- **Planning Tech Demo 1 – March 2008**
- **Spiral 1 Operational Demonstration – Sept 2008 (CONUS)**
- **System Installation July 2009**
- **Spiral 2 Final Operational Demonstration – Sept 2009 (OCONUS)**
- **Extended Operational Use – FY2010**



# Summary



- **JFPASS JCTD is an integral part of a comprehensive DoD effort to improve conventional force protection**
  - Informs concept analysis and future requirements
  - Provides capability to the force 4-5 years earlier
- **JFPASS JCTD will provide a layered, integrated, and automated Base Defense System**
- **US Army is the lead service and is executing with a Joint team**
- **Integration of candidate capabilities demonstrated successfully in FPJE IA-1, -2, and -3**
- **USEUCOM is the Operational Manager (OM)**
- **NSWC Dahlgren provides technical leadership in line with its ATPF mission**