Counter-IED Program

Joe Foster
Explosives Division
Science and Technology Directorate
Department of Homeland Security

"Putting First Responders First"

Homeland Security
Science & Technology

Mission Need Statement

- To protect the U.S. population and critical infrastructure from Improvised Explosive Devices (IEDs)
    - Suicide Bombers (SBIED)
    - Leave-Behind (LBIED)
    - Vehicle Borne (VBIED)
- Utilize security processes that allow for the free flow of people and commerce.
- No practical, effective capabilities currently exist within the public domain. Military (DOD) solutions conflict with domestic privacy laws or are unsuitable for maintaining open civilian commerce.
- Mission authorized by Homeland Security Presidential Directive #19 (HSPD-19), HSPD-7, National Infrastructure Protection Plan, and Homeland Security Act of 2002.

Homeland Security

Homeland Security Presidential Directive-19

On February 12, 2007, President Bush signed HSPD-19, which addresses the threat of terrorist use of explosives and IEDs in the United States

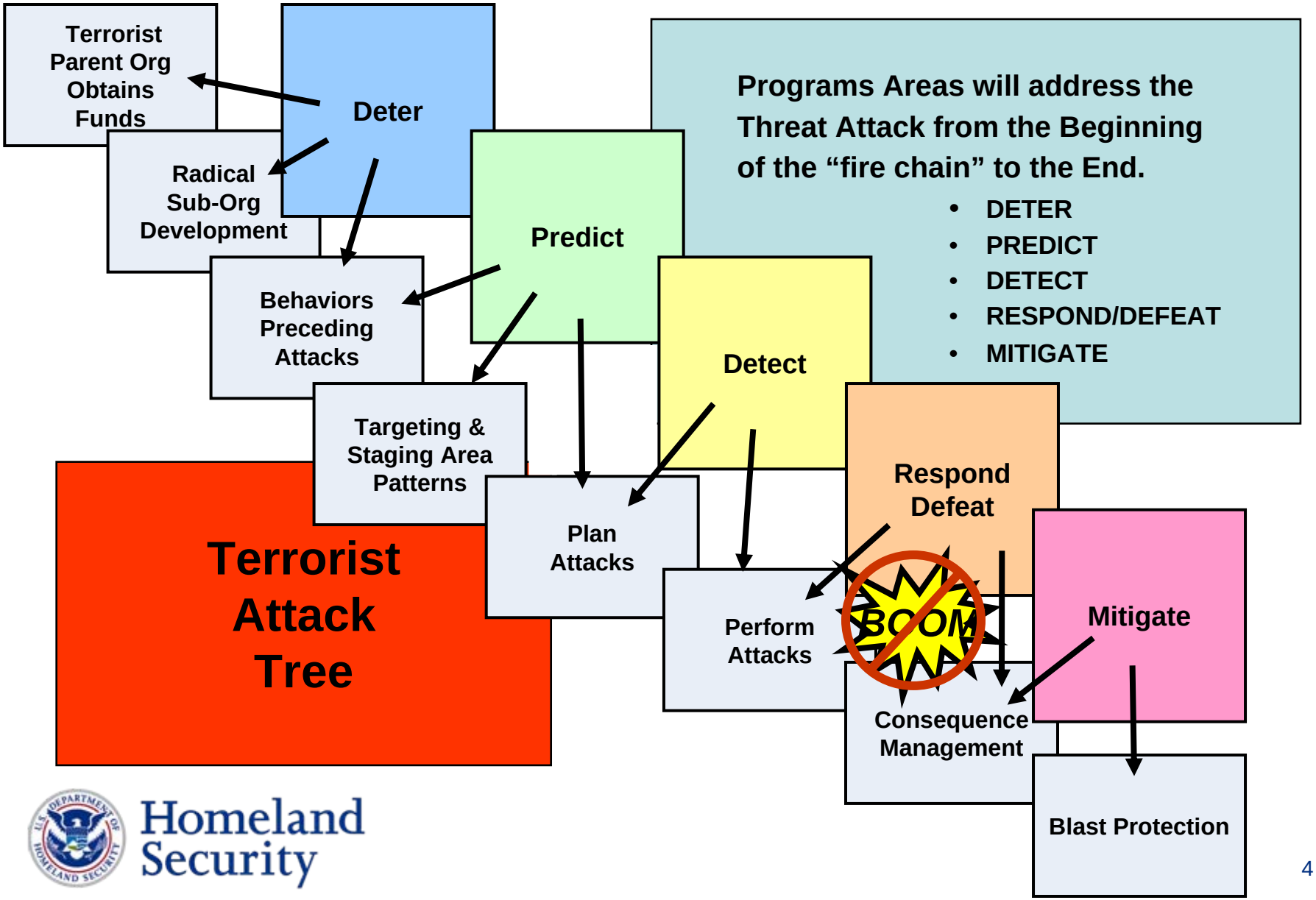
- Establishes a national policy on the prevention and detection of, protection against, and response to terrorist use of explosives (and IEDs) in the United States
- Calls for the development of a National Strategy for IEDs including recommendations

Need technologies to protect against domestic IED threats

- "…Deter, Prevent, Detect, Protect Against, and Respond to Explosive Attacks"

Homeland Security

Preventing IED Attacks



Homeland Security

Counter-IED Programs

Human Factors		Explosives		Infrastructure
Deter	**Predict**	**Detect**	**Respond / Defeat**	**Mitigate**
Within Guidance	**Within Guidance**	**Within Guidance** Explosives • Suicide Bomb Detection • Vehicle Borne IED Detection • Canine Detection R & D	**Within Guidance** Explosives • Bomb Assessment Technology • Render Safe / Neutralize Tools	**Within Guidance** Infrastructure & Geophysical • Infrastructure Blast Mitigation • Advanced Surveillance
Over Guidance Human Factors • Motivation & Intent-Based Deterrence	**Over Guidance** Human Factors • Predictive Screening Project • Risk Prediction Project	**Over Guidance** Explosives • Suicide Bomb Detection • Technology Demonstration/ System Integration • Vehicle Borne IED Detection • Tagging R & D • Standards	**Over Guidance** Explosives • Electronic Countermeasures • Robotics Project • Directed Energy • Render Safe / Diagnostics • Post Blast (Forensics) • Bomb Components • Outreach	**Over Guidance** Infrastructure & Geophysical • Infrastructure Blast Mitigation • Advanced Surveillance • Body Armor (EXD Lead) • Inerting (EXD lead) • Marking (EXD Lead)

Homeland Security

Motivation & Intent-Based Deterrence (Human Factors)

Technology Goals –

- Actionable indication and warnings that support the effective use of intervention and deterrence options
- Increased confidence and accuracy of the intelligence and law enforcement community in identification of the threat and ability to prevent an attack

Approach – Using surveys, case study analysis, and field work, as well as classified and unclassified data, this program will:

- Identify the pathways to radicalization as well as the role of communities in supporting or preventing terrorist violence
- Analyze indicators of groups and individuals moving towards IED use and identify points of intervention by law enforcement and the intelligence community
- Identify effective interventions to reduce the intent of persons and groups to carry out IED attacks against the U.S. homeland.
- Integrate motivation- and intent-based indicators and tools to augment existing indication and warning systems.

Customers –

- Office of Intelligence and Analysis, USSS, TSA, CBP, and state and local governments and law enforcement

Homeland Security

Predictive Screening (Human Factors)

Technology Goals –

- Increased probability of identifying suicide bombing behaviors pre-attack
- Significant expansion of the active surveillance area to include the entire airport, mass transit portal, and special event venue
- Increased deterrence of travelers carrying illegal weapons and false documents

Approach –

- Develop technologies that leverage existing suspicious behavior indicators that are statistically related to possession of illegal weapons and false documents, existing video tracking algorithms, and maturing video-based behavior identification algorithms to automatically identify, alert authorities to, and track suspicious behaviors that precede a suicide bombing attack.
- This technology will be tested at ports of entry, transit portals and special events

Customers –

- Office of Intelligence and Analysis, USSS, TSA, CBP, and state and local governments and law enforcement

Homeland Security

Risk Prediction (Human Factors)

Technology Goals –

- Support for interdiction decisions and indication and warning assessments
- Support for prioritization of intelligence, surveillance, and reconnaissance assets
- Support of real-time hypothesis testing

Approach –

- Leverage existing geo-behavioral pattern discovery algorithms to identify and prioritize the risk of likely potential targets of attack within the United States.
- Combine infrastructure, terrorist tactics, and demographics data to translate the targeting patterns of overseas attacks to U.S. cities

Customers –

- Office of Intelligence and Analysis, USSS, TSA, CBP, and state and local governments and law enforcement

Homeland Security

Suicide Bomber IED Detection (Explosives)

Technology Goals –

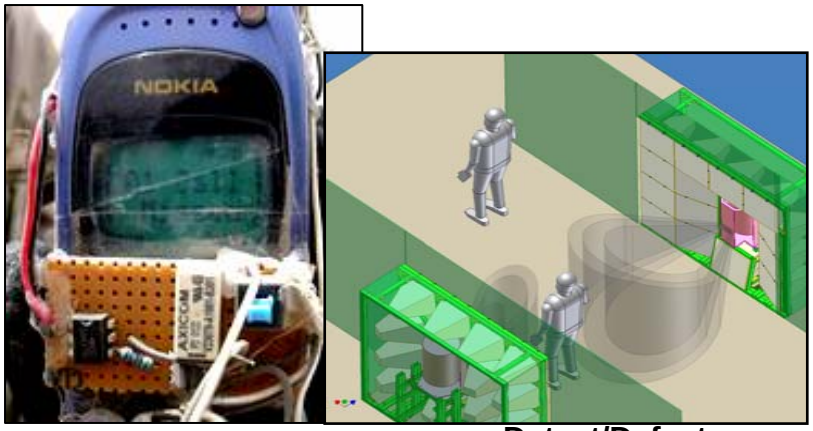
- Increase standoff distance for detection
- Decrease false alarm rates
- Improve person screening automation; e.g. threat configuration on the person (where is the threat located), and threat material composition

Approach –

- Develop and integrate detection technologies (e.g. millimeter wave, backscatter x-ray, THz imaging, spectroscopic and trace detection technologies)
- Improve understanding of the threat to best determine where materials are most likely to be located on a suicide bomber
- Use explosive threat data on characterization and configuration to better understand threats to develop better detection systems
- Develop standalone imaging/spectroscopic prototypes for real-time screening of suicide bombers

Customers –

- TSA, USSS, USCG, CBP, OBP



Detect/Defeat

Homeland Security

Vehicle Borne IED Detection (Explosives)

Technology Goals –

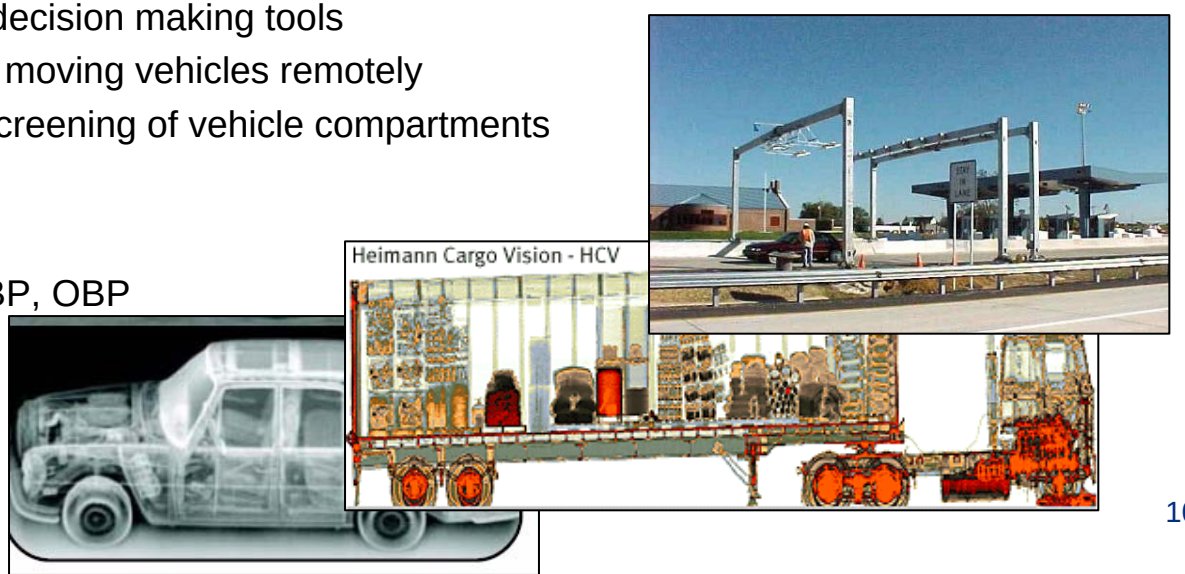
- Increase standoff distance for detection
- Decrease false alarm rates
- Mature vehicle screening automation; e.g. material detection, screening automation, threat configuration on the vehicle (where is the threat located), and threat material composition

Approach –

- Develop and integrate imaging technologies (e.g. Raman, LIBS, Lidar, THz/GHz)
- Improve threat understanding to best determine the most likely locations of threat materials in a vehicle
- Develop automated screening technologies for threat detection
- Improve threat signatures and configurations with explosive threat characterization data
- Improve digital tactical decision making tools
- Prototype for screening moving vehicles remotely
- Prototype for external screening of vehicle compartments

Customers –

- TSA, USSS, USCG, CBP, OBP



Homeland Security

Standards (Explosives)

Technology Goals –

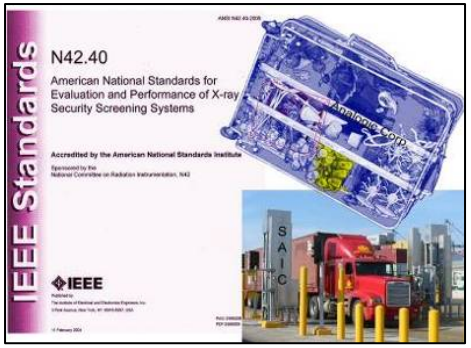
- Develop user validated and industry recognized standards, performance metrics, and application guides
- Develop performance standards, application guides, and Test & Evaluation (T&E) protocols for IED detection and defeating technologies. This includes comprehensive performance standards, acquisition guides for users, as well as guides, practices & test methods for robotics applications
- Development in parallel with technologies
- Leverage NIST partnership with DoD IED DEFEAT program

Approach –

- Minimum performance standards for Portable X-Ray and 3D imaging systems
- Operational holographic imager & standoff detection performance metric tests
- Preliminary performance standards for industry review
- Guides, practices & test methods for using robots to detect and defeat IEDs
- User-validated standards performance metrics, T&E protocol (test bed) development

Customers –

- USSS, TSA, USCG, Preparedness, State/Local Bomb Squads



Homeland Security

Render Safe/Diagnostics (Explosives)

Technology Goals –

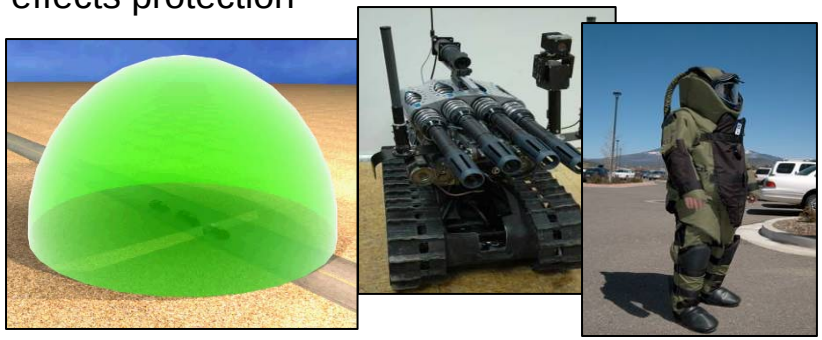
- Increase standoff distance for detection and precision disruption capability
- Reduce collateral damage & explosive content
- Reduce cost, weight, footprint, power requirement, and battery size of current counter-measure devices

Approach –

- Develop fast, light-weight robotics platforms with a suite of tools necessary to deal with emerging threats
- Mature and field a radio frequency (RF) jamming system that will not interfere with the bomb squad robotic RF system
- Develop a multi-shot disruptor that can attack multiple IEDs
- Develop post-blast forensics technologies to speed the process of collection and investigation
- Develop body armor that is climate controlled, wearable and comfortable and provides adequate blast, fragmentation and thermal effects protection

Customers –

- USSS, TSA, USCG, Preparedness, State/Local Bomb Squads



Radio Controlled IED Electronic Countermeasures

Homeland Security

Inerting (Explosives)

Technology Goals –

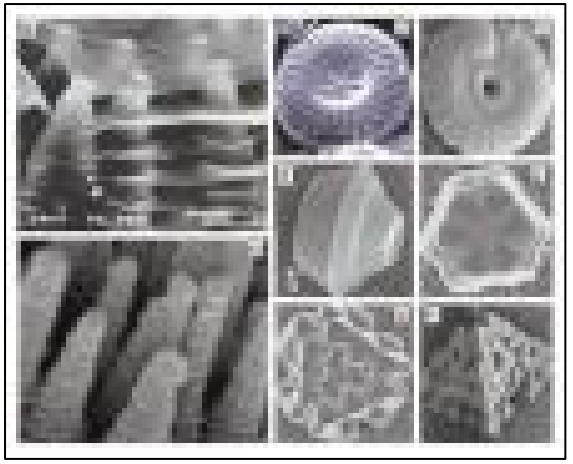
- Identify, define, and develop methods, materials and technologies to render common explosives inert or less explosive
- Reduce the number of commercially available compounds and products with explosive characteristics
- Develop a method to defeat explosives by either adding an ingredient or removing an ingredient to render the compound inert

Approach –

- Proof of Concept Study
- User's Manual

Customers –

- USSS, TSA, USCG, Preparedness, State/Local Bomb Squads



Explosive Inerting Compounds

Homeland Security

Infrastructure Blast Mitigation (Infrastructure)

Technology Goals –

- Identify and mature materials in order to design mitigation measures and 3-dimensional direct and reflected blast effect technologies
- Reduce consequences of an event when prevention has failed
- Lower casualties, increase survivability, decrease severity and extent of economic and property damage, reduce risks to first responders in life saving phase, inform police and fire locations for safely establishing perimeters, reduce time to restore critical services

Approach –

- Active & Passive Systems to protect infrastructure against blast pressure, impulse, fire, dust, fragmentation
- Internal and External Hardening
- Disrupt blast load front
- Disrupt flame front
- Rapidly cool/suppress flame front
- Deflect or absorb wave front
- Counter-wave
- Capture or deflect fragments, dust
- Self-healing materials
- Redundant structural members

Customers –

- TSA, USCG, CBP, OBP and other elements of NPPD, FBI, Infrastructure owners/operators, First Responders, FEMA, State & Local Security Offices

Homeland Security

Advanced Surveillance (Infrastructure)

Technology Goals –

- Provides forensics (identifies where the suspects and their resources came from) and situational awareness for emergency response forces
- Provides key forensics information to law enforcement, provides superior situational awareness to law enforcement and Emergency Services post-event

Approach –

- Develop survivable, integrated system of sensors, connectivity, and deployment for review and assessment of post event conditions
- Integrate data collection and fusion across multiple wave forms and sensor types
- Rapid data retrieval and play-back
- Data hand-off across multiple sensors

Customers –

- TSA, USCG, CBP, OBP and other elements of NPPD, FBI, First Responders, FEMA, State & Local Security Offices

Homeland Security

Field Demonstrations & Technology Roadmaps

Field demonstrations will play a major role in establishing and demonstrating the capabilities of technologies for stand-off detection and defeat of SBIEDs, LBIEDs and VBIEDs.

- Technologies leveraged from inter-agency groups and project outputs are candidates for demonstration
- Demonstrations will be held on an annual basis to support development of technologies
- Customers — security groups, first responders, etc. — will participate in ConOps development, data analysis, and technology evaluations
- FY2008 demonstrations will focus on test and evaluation of commercial off-the-shelf (COTS) and near-COTS technologies. Out-year efforts will demonstrate systems integration and multi-layered architectures

Homeland Security

Common System Architecture

Standardization of Interfaces, Data Formats, and Communication Protocols

- Will improve effectiveness, provide configuration flexibility, control operating costs, and support multi-vendor environments
- Will support effective and efficient decision-making
- Community of security stakeholders must come together to establish hardware interfaces and communications standards
- Similar initiative: Joint Architecture for Unmanned Systems (JAUS), a DoD mandate for use by the Joint Ground Robotics Enterprise

Common System Architecture

Leverage Technology Activities, Programs, and Outputs from Inter-agency R&D Organizations

Authorized by HSPD-19: (4) It is the policy of the United States to counter the threat of explosive attacks aggressively by coordinating Federal, State, local, territorial, and tribal government efforts and collaborating with the owners and operators of critical infrastructure and key resources to deter, prevent, detect, protect against, and respond to explosive attacks […]

Authorized by HSPD-7: (21) Federal departments and agencies shall cooperate with the Department in implementing this directive, consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

RDT&E of technologies to deter, predict, detect, defeat, and mitigate IEDs are conducted by agencies across the federal government. These inter-agency organizations have potential to share:

- Technology Breakthroughs
- Demonstrated Capabilities
- Modeling and Analysis Tools
- Experimental Test Data
- Assessments and Studies
- Subject Matter Experts

Homeland Security

Homeland Security

Science and Technology