DHS
Science and Technology Directorate
FY 2006 Budget Brief

1 March 2005

Dr. Parney Albright
Assistant Secretary, Science and Technology

Homeland Security

Mission and Roles

MISSION:

The Science and Technology Directorate will create enduring homeland security capabilities through research, development, testing, evaluation, and transitioning of revolutionary and existing technologies to detect, prevent, and mitigate chemical, biological, radiological, nuclear, and explosive threats; assess and analyze threats and vulnerabilities; provide technical solutions to Federal, state, and local emergency responders in accordance with operational requirements; and secure the nation's borders and critical infrastructure.

ROLES:

- Partner with operational end-users to identify requirements, develop and field capabilities to counter threats and enhance mission operations;
- Engage government, academic, and private sectors in innovative research, development, rapid prototyping, and systems engineering and development;
- Provide a rapid, efficient, and disciplined process for systems engineering and development; and
- Provide the Department with an enduring research and development complex dedicated to homeland security.

Homeland Security

S&T Budget Activities

- Biological Countermeasures
- Chemical Countermeasures
- Explosives Countermeasures
- Radiological and Nuclear Countermeasures
- Domestic Nuclear Detection Office
- Support of DHS Components
- Threat and Vulnerability, Testing and Assessment
- Salaries and Expenses
- University and Fellowship Programs
- Emerging Threats
- Office of Interoperability and Compatibility
- Critical Infrastructure Protection
- Research and Development Consolidation
- Rapid Prototyping
- Counter MANPADS
- SAFETY Act
- Cyber Security
- Standards

S&T Budget Activities and FY 2006 Requests**

*** Dollars in Thousands*

BUDGET ACTIVITY	FY 2006 REQUEST	BUDGET ACTIVITY	FY 2006 REQUEST
Biological Countermeasures	362,300	University and Fellowship Programs	63,600
Chemical Countermeasures	102,000	Cyber Security	16,700
Explosives Countermeasures	14,700	Critical Infrastructure Protection	20,800
Radiological and Nuclear Countermeasures	19,086	Research and Development Consolidation	116,897
Domestic Nuclear Detection Office	227,314	Rapid Prototyping	20,900
Support of DHS Components	93,650	Counter-MANPADS	110,000
Threat and Vulnerability, Testing and Assessment	47,000	Office of Interoperability and Compatibility	20,500
Emerging Threats	10,500	SAFETY Act	5,600
Standards	35,500	Salaries and Expenses	81,399
		TOTAL REQUEST: 1,368,446	

Homeland Security

Biological Countermeasures - $362.3M

- **Major Sub-activities:**
  - **Systems Studies and Decision Support Tool–** supports HSPD-10 directives for analysis and also provides an integrated analysis and strategy for national biomonitoring.
  - **Threat Awareness and Characterization –** a capability that provides facilities and expertise to support systematic biothreat risk assessments with the involvement of government, university, and industry resources.
  - **Surveillance and Detection Operation–** provides operational fixed and field deployable bioaerosol detection systems.
  - **Surveillance and Detection R&D –** develops new technologies including those leading to totally automated sample collection and analysis,and high-throughput sample analysis. It also supports efforts to integrate military and civilian systems to ultimately integrate environmental data, health surveillance information, intelligence, and threat data to detect and to respond to an event.
  - **Forensics ($28.5M) –** establishes a lead national facility for technical analysis of forensics samples from biologic events.
  - **Response and Restoration –** develops pre-approved protocols and decontamination agents for facilities.
  - **Agriculture–** focuses on addressing operational issues at the Plum Island Animal Disease Center. Has also initiated programs to develop animal vaccines and next generation diagnostics for foreign animal diseases.

Biological Countermeasures – cont'd

- **Major FY 2004 - FY 2005 Accomplishments :**
  - Widely deployed the BioWatch sensor system to provide day-to-day protection in over 30 of our nation's cities - conducting over a million assays with no false alarms. BioWatch also provided field and lab support to many high profile events including the Super Bowl, the G8, and both National Conventions.
  - Provided major contributions to the end-to-end study that culminated in HSPD-10, aimed developing the requirements for an integrated national bio-defense architecture. Conducted analyses on four reference cases: a large outdoor anthrax release; a large indoor release of smallpox; contamination of a bulk food supply; and two highly virulent agricultural attacks, one on livestock and the other on plants.
  - Established the Biodefense Knowledge Center, a 24/7 operational hub enabling collaboration and communication within the homeland security complex to meet the operational and planning requirements of government decision-makers and program planners, the intelligence community, law enforcement officers, public health practitioners, and scientists.
  - Established an interim capability for the National BioForensics Analysis Center (NBFAC) at USAMRIID that is already handling some 1500 samples.
  - Conducted assessments to support four Material Threat Determinations by the Secretary of DHS.

Biological Countermeasures – cont'd

- **Key FY 2006 Deliverables:**
  - Complete the first formal risk assessment required under HSPD-10.
  - Complete the deployment of Generation 2 BioWatch systems to the top threat cities and complete test and evaluation of laboratory prototypes of the Generation 3 BioWatch detection systems
  - Initiate a High Throughput Diagnostics Demonstration, working with regional and state laboratories to demonstrate the capability to analyze thousands of samples per day in support of response to a suspected case or an outbreak.
  - Complete the development of a coupled epidemiological and economic model for FMD to allow the evaluation of various intervention strategies..
  - Complete the end-to-end systems study for antibiotic resistant threats, multiple small threats and avian influenza.

- **Future Major Capability Goals:**

  Deploy an integrated, end-to-end national biodefense architecture against all high-consequence biological threats – known, emerging, and engineered including:
  - Decision tools to perform system studies against the entire spectrum of threats
  - A Bio-threat Characterization Center that will assess and prioritize current and potential future threat agents
  - A Bio-Defense Knowledge Center providing instantaneous access to experts and libraries Continuous urban monitoring for up to 20 bioagents, with detection times of under 4 hours
  - Integrated detect-to-warn critical facility protection
  - A fully operational, accredited National Bio-forensics Analysis Center
  - A suite of vaccines), therapeutics and diagnostics to control foreign animal diseases

Chemical Countermeasures - $102M

- **Major Sub-activities:**
  - **Chemical Analysis and Infrastructure** – develops a fundamental understanding of toxic chemical threats and assesses risks and vulnerabilities, develops reach-back capabilities for domestic emergencies, and supports a lab capability to rapidly restore chemically contaminated areas, and provides forensic analytic tools for attribution.
  - **Detection** – supports major leap-ahead technology development effort for providing tools to warn and notify responders of chemical threat releases.
  - **Architecture** – conducts systems studies to assess top-level risks and consequences of a broad range of chemical agents to guide program prioritization and to establish functional requirements and performance metrics; conducts operational technology demonstrations
  - **Response and Recovery** – provides operational solutions to chemical agent decontamination

- **Major FY 2004 - FY 2005 Accomplishments:**
  - Conducted preliminary activities toward the development of a Chemical Security Analysis Center (CSAC) that will provide threat awareness and assessment.
  - Initiated system studies around three defining scenarios: indoor chemical agent release, outdoor toxic industrial chemical release, and release of toxin in the water system.
  - Initiated three demonstration projects: the Facility Restoration Demonstration Project, a Water Security Demonstration and a National Security Special Event (NSSE) Deployable Detection System Demonstration.
  - Initiated key development programs targeting leap-ahead advancements in detection capabilities for both monitoring facilities and a responder detection tool. The detectors will provide detection and discrimination of up to 20 different chemical threats, including classical chemical warfare agents (CWAs) and toxic industrial chemicals (TICs) in a single unit across a wide range of concentrations.

Chemical Countermeasures – cont'd

- **Key FY 2006 Deliverables:**
  - Reach full operational status at the CSAC.
  - Complete technology down-select and draft candidate decontamination protocols in concert with the Environmental Protection Agency (EPA) through the Facility Restoration Technology Demonstration. Transition the Water Security Demonstration to EPA for continuation and conduct technology down-select for the next-generation deployable capability through the NSSE Technology Demonstration.
  - Complete the critical design review of technologies for the rapid facility monitor and the first responder detector and conduct a technology down-select supporting prototype selection and build.
  - Transition high throughput mobile laboratory to end user

- **Future Major Capability Goals:**
  - Fully functional interagency resource for chemical threat data
  - Functional lab response capability to conventional agents
  - Capability for simulated operational test of non-traditional agent countermeasures
  - Demonstrated operational solutions for broad-spectrum facility protection and updated deployable systems
  - Demonstrated decontamination solutions for conventional agents
  - Commercially available broad spectrum facility, hand-held detectors, and nontraditional agent sensor
  - Fielded non-traditional agent version of high-throughput mobile lab prototype

Chemical Countermeasures – cont'd

- **Key FY 2006 Deliverables:**
  - Reach full operational status at the CSAC.
  - Complete technology down-select and draft candidate decontamination protocols in concert with the Environmental Protection Agency (EPA) through the Facility Restoration Technology Demonstration. Transition the Water Security Demonstration to EPA for continuation and conduct technology down-select for the next-generation deployable capability through the NSSE Technology Demonstration.
  - Complete the critical design review of technologies for the rapid facility monitor and the first responder detector and conduct a technology down-select supporting prototype selection and build.
  - Transition high throughput mobile laboratory to end user

- **Future Major Capability Goals:**
  - Fully functional interagency resource for chemical threat data
  - Functional lab response capability to conventional agents
  - Capability for simulated operational test of non-traditional agent countermeasures
  - Demonstrated operational solutions for broad-spectrum facility protection and updated deployable systems
  - Demonstrated decontamination solutions for conventional agents
  - Commercially available broad spectrum facility, hand-held detectors, and nontraditional agent sensor
  - Fielded non-traditional agent version of high-throughput mobile lab prototype

Explosive Countermeasures - $14.7M + $109M

- **Major Sub-activities:**
  - **Infrastructure Protection –** assess blast mitigation techniques for critical infrastructure and provides guidance for protection measures.
  - **Suicide Bombers/Leave Behind Improvised Explosive Devices –** complete assessment of currently available technologies while simultaneously developing new technologies to detect suicide bombers at stand-off distances.
  - **Vehicle Bombs –** complete prototype efforts of a vehicle bomb detection system while simultaneously develop vehicle bomb stand-off detection and interdiction capabilities.

- **Major FY 2004 - FY 2005 Accomplishments:**
  - Initiated the development of a prototype explosive detector for vehicle bombs and accelerated development of hardened overhead storage bins for passenger aircraft.
  - Initiated a survey and evaluation of commercial-off-the-shelf equipment to detect, interdict and mitigate the consequences of suicide bombers and vehicle bombs, and a cost-benefit analysis of approaches to aircraft hardening.
  - Funded demonstration of capabilities to detect, interdict, and mitigate the consequences from suicide bombers in the rail environment.

Explosive Countermeasures – cont'd

- **Key FY 2006 Deliverables:**
  - Continue to consolidate explosives management functions.
  - Develop the ability to detect, interdict and mitigate the consequences from suicide bombers and vehicle bombs approaching high profile targets and densely populated areas.
  - Improve the ability to detect, interdict and mitigate the consequences of explosives and weapons on aircraft transporting (domestic and foreign inbound) passengers and their baggage as well as cargo containers/bays.

- **Future Major Capability Goals:**
  - Detect, interdict, and mitigate the consequences of vehicle bombs in transit and approaching critical infrastructure.
  - Detect, interdict, and mitigate the consequences of suicide bombers approaching critical infrastructure or densely populated areas.
  - Detect smuggling of explosives across the US borders.
  - Detect, interdict, and mitigate the consequences of explosives or weapons in aircraft passenger cabins and air cargo.

TSL Plans (1 of 3)

- In FY04 and FY05, TSA RDT&E funds have been appropriated under three major categories, with (>90%) of funded RDT&E for aviation security
  - Applied Research
    - Historically (even pre-9/11) ~ $55M. This budget line has funded FTE's (currently 74 personnel) and explosives countermeasures
    - Some funding (~$5M) for…
      - Biometrics
      - access control, or
      - communications (RFID) technology
  - Next Generation Explosives Technology
    - ~$45M since FY03
      - Historically next generation checked baggage screening programs (Manhattan II and Phoenix)
      - More recently passenger screening explosives detection systems
  - Air Cargo R&D
    - $55M in FY04 and $75M in FY05
    - Next generation explosives detection R&D and pilot studies of existing cargo screening technology

TSL Plans (2 of 3)

- Planned redirection
  - Driven by…
    - Maturity of aviation security explosives countermeasures technology
    - Threat of vehicle and suicide bombs
      - Minimal detection approaches available
  - Aviation
    - Facts
      - In FY06 planned completion of Phoenix prototype development
      - Manhattan program
        - Has changed from a short-term/high pay-off/ revolutionary detection R&D to a long term R&D program of broad applicability
      - Currently available technologies can be used to screen most cargo
    - Thus, in FY06…
      - Prototype an automated carry-on baggage explosives detection screening system, and
      - A fused, automated explosives and weapons detection passenger screening system, and
      - Program to support certification activities and next generation R&D.

TSL Plans (3 of 3)

- Vehicle bomb (VBIED) explosives countermeasures in FY06….
  - Complete prototype of a “checkpoint”/ close-in VBIED detection system and pilot at one location.
  - Initiate a significant R&D program to develop stand-off detection capability.
  - Initiate a program to determine feasibility of marking explosives to detect VBIED further upstream from the target (e.g., at truck scales
  - Complete an infrastructure protection strategy and implement solutions where possible leveraging DoD and DoS efforts
  - Suicide bomb/ leave-behind IED explosives countermeasures in FY06….
    - Complete the rail pilot of COTS technologies
      - primarily checkpoint technologies but perhaps some limited stand-off detection capabilities.
    - Continue R&D efforts to detect suicide bombers at stand-off distances.
    - Initiate R&D to detect the smuggling of military explosives across US borders, emphasis on maritime.
- “Redirection” of funding significant from a threat perspective
  - Not as dramatic from technology approach
  - More emphasis will be placed on a system solution vs. inserting detection technology
  - More emphasis will also be placed on preventing the IED from reaching its target

Radiological and Nuclear Countermeasures - $19.1M

- **Major Sub-activities:**
  - **Attribution and Forensics on Contaminated Evidence** – completes lab improvements to carry out attribution and demonstrate an ability to analyze highly enriched uranium samples
  - **Incident Management and Recovery** – completes field studies in the New York City urban dispersion program and transfer of technology to the New York City Office of Emergency Management
- **Major FY 2004-FY 2005 Accomplishments:**
  - Assumed management of the Port Authority of New York and New Jersey radiation detection test bed. Broadened the project scope beyond testing and evaluating individual pieces of technology to include response protocols and operational concepts.
  - Focused detection technology efforts on the detection of shielded special nuclear material (SNM) in cargo containers.
  - Directed preplanned product improvement efforts toward improvement in two current Customs and Border Protection-deployed radiographic imaging systems.
  - Initiated joint DHS and Department of Defense project focusing incident management and recovery efforts for radiological and nuclear decontamination.
  - Established a test and evaluation capability at the Nevada Test Site (NTS) for testing against SNM.

Radiological and Nuclear Countermeasures – cont'd

- **Key FY 2006 Deliverables:**
  - Redirect all detection related missions and corresponding funding to the establishment of the Domestic Nuclear Detection Office. The remaining, non-detection research and development will continue to be funded through the Radiological/Nuclear Countermeasures portfolio. The two programmatic thrust areas remaining are Incident Management and Recovery, and Attribution and Forensics on Contaminated Evidence (formerly part of the Systems Analysis and Pilot Deployments programmatic area).
  - Conduct the laboratory improvements that are necessary to carry out the attribution mission.
  - Conduct all field studies for the New York City Urban Dispersion Program with a technology transfer following to NYC Office of Emergency Management in late 2006.

- **Future Major Capability Goals:**
  - A national attribution capability for countering nuclear and radiological terrorism as part of the U.S. government incident management capability for both the law enforcement and national security communities.
  - New or enhanced capabilities in the areas of crisis response, consequence management and recovery utilizing emerging technologies to demonstrate and deploy near-term enhancements to responder capabilities, such as improved search and characterization, and render-safe systems.

Domestic Nuclear Detection Office - $227.3M

- **Major FY 2004-FY 2005 Accomplishments:**
  - Detection activities were conducted under the Radiological and Nuclear Countermeasures portfolio.
- **Key FY 2006 Deliverables:**
  - Develop the system architecture, conduct all associated systems engineering, develop technology roadmaps, and develop a strategic plan for the DNDO.
  - Coordinate with other Federal, state, and local R&D organizations.
  - Develop concepts for innovative technologies and coordinate with interagency R&D organizations on all advanced detection technologies, development concepts, and programs.
  - Develop and provide technical standards and protocols for detection systems, reporting systems, and information sharing systems.
  - Design and conduct technical and operational test and evaluation of related detection equipment, technologies, systems, procedures, concepts of operation, and protocols for the domestic nuclear detection system.
  - Prepare and maintain the DNDO Test and Evaluation Master Plan.
  - Oversee the Radiological and Nuclear Countermeasures Test and Evaluation Complex (Rad/NucCTEC) and use other Rad/Nuc test infrastructure as needed to execute the Office's assessment responsibilities.
  - Provide operational support, to include: (1) information collection, coordination, and analysis; (2) coordinated technical reachback; and (3) and the development of standards, protocols, concepts of operations, training, safety and security procedures, and state and local support.
  - Identify technology opportunities and execute programs to dramatically improve the domestic nuclear detection system overall and component-wise performance, especially high-risk, high-payoff technology investments.
- **Future Major Capability Goals:**
  - Integrated interagency operational capability for detection of radiological and nuclear materials using innovative and transformational technologies.

Support to DHS Components - $93.7M

- **Major Sub-activities:**

  Border and Transportation Security

  - **Border Watch** – develops the system of sensors, processes, and people to monitor the status of our land, sea, and air borders to detect an approaching threat
  - **Transportation Watch** – develops the system of sensors, processes, and people to monitor the status five transportation domains – aviation, rail, ship, highways, and pipelines to provide domain awareness.
  - **Border and Transportation and Security Net –** provides a robust information management network between and among the various components of Border Watch and Transportation Watch

- **Major FY 2004 - FY 2005 Accomplishments:**
  - Issued a solicitation for an Advanced Container Security Device to develop and field test (within the Directorate's CounterMeasures Test Bed) the next generation of shipping container security devices.
  - Supported the BTS Directorate in placing technology in the field to support the Arizona Border Control Initiative.
  - Continued development and refinement of BTS technology requirements and planning using a capabilities-based process to ensure that Federal technology planners understood the capabilities that BTS agents and officers view as essential for mission success and to help planners focus technology development on filling the identified gaps in those capabilities.
  - Developed the BTS Technology Vision which included Border Watch, Transportation Watch and Border Net, significantly improving our ability to provide the information necessary to secure our borders. The foundation of the vision is an architecture and a set of technology programs that will gather, process and distribute real-time knowledge of the border and transportation situation and provide decision support tools and labor saving devices for our security forces.

Support to DHS Components – BTS cont'd

- **Key FY 2006 Deliverables:**
  - Build on the sensor trade studies and modeling conducted in FY 2005 to develop and test advanced sensor suites including improved visual and non-visual sensors (video, infrared, seismic, acoustic and radar). These sensors may be deployed on the ground, at sea, and in the air. In addition, evaluate data produced by Ports-of-Entry (POE) inspectors, such as traffic and incident information, along with data produced by border inspection systems will be evaluated as part of the surveillance system.
  - Build on the design and development effort for the next generation of container security and communications systems to detect intrusion, location, contents and tampering.
  - Integrate Transportation Watch capabilities across the transportation domains enabling a Common Operational Picture (COP) across the entire transportation environment. Extensive data sharing, including the ability to discover links in criminal or suspicious activities across domains will be a key requirement to providing an effective Transportation COP.
  - Initiate development and integration of smart portals and sensors for detection of explosive threats to shipping. Utilize rapid prototyping processes, focusing initially on passenger and vehicle ferries.
  - Define system architecture that fully supports the Border Watch Common Operational Picture with multi-modal access to essential databases, remote communications and intelligence fusion.
- **Future Major Capability Goals:**
  - Smart Containers that provide automated detection and targeting of contraband, with connectivity that provides an end-to-end visibility of status, position, alerts, and environmental conditions on contents from time of manufacture through final delivery.
  - Border with depth across the U.S. with high probability of detection and low false alarm rate for detection of persons and contraband.
  - Rapid and integrated screening of people and cargo at Points of Entry, including automated alerting and detection of contraband, rapid determination of intent, identity or deception, and automated intelligence and data fusion with DHS systems.
  - Full border intelligence capability, including total BTS/USCG database access.
  - Detection, containment and reporting systems for reacting to on-board aircraft threats and reduced risk to highest threats.

Support to DHS Components – EP&R

- **Major Sub-activities:**

  Emergency Preparedness and Response

  - **Regional Technology Integration (RTI) Initiative** – implements a demonstration program for incorporating technology and operational solutions directly in existing state and local emergency response infrastructure to assess effectiveness
  - **Interagency Modeling and Atmospheric Analysis Center (IMAAC)** - provides a single near-real time prediction for airborne release of hazardous material
  - **Emergency Responder Personal Protective Equipment** – focuses on developing materials and technologies to be used in multi-hazard environments, by diverse users, and to function as an integral part of a complex system
  - **Unified Incident Command & Decision Support** – develops an information management and sharing architecture that meets the needs of incident commanders and responders to share information, to present decision options, and to coordinate emergency efforts.
  - **Simulation-Based Training and Education** – enables first responder to access important information on technologies, training, and standards through a single electronic portal.

- **Major FY 2004-FY 2005 Accomplishments**
  - Initiated operation of the Interagency Modeling and Atmospheric Assessment Center (IMAAC) and supported the National Exercise Program and special events, such as the Democratic and Republican National Conventions. IMAAC established connectivity to the Department of Homeland Security Operations Center and the FEMA National Emergency Operations Center to provide near real time hazards predictions for airborne releases.
  - Selected four urban areas for the pilot of the Regional Technology Integration (RTI) Initiative. These locations provide an opportunity to evaluate geographic and governance diversity as well as variability in threats and vulnerabilities. Initiated an integrated assessment process in collaboration with these communities.
  - Focused activities on the identification of simulation based training and education requirements through interaction with the responder community. The portfolio leveraged the work initiated by Office of Domestic Preparedness and the Memorial Institute for the Prevention of Terrorism, the National Institute of Justice and the Department of Defense in identifying needs and gaps as well as existing technology development programs that can be utilized for incident management training

Support to DHS Components – EP&R cont'd

- **Key FY 2006 Deliverables:**
  - Leverage Federal resources to provide dynamic venue for collaborative research, development, testing and evaluation of atmospheric transport and dispersion (ATD) models for hazards predictions.
  - Complete implementation of technology systems solutions for the first four pilot locations of the RTI initiative; prepare test and evaluation plans and conduct operational readiness exercises to evaluate the overall system performance.
  - Develop the system requirements that support national, interoperable simulation based training and exercise. This capability will focus on large scale, multi-jurisdictional incidents and will facilitate the implementation of the National Incident Management System and the National Preparedness Goal.
  - Demonstrate several revolutionary and highly innovative materials for emergency personal protective equipment (PPE) applications. Demonstrate prototype material/technologies that can that can be made into functional garments and/or integrated personal protective systems will be demonstrated.
  - Initiate an Advanced Concept Technology Demonstration of a candidate Unified Incident Command (UIC) architecture that will achieve revolutionary advances in Unified Incident Command and Decision Support and bring analytical tools to bear on real-time information in-flows and out-flows for incident commanders and emergency responders. Advanced capability will be applicable to a variety of response paradigms, including single incidents, multiple simultaneous incidents, long duration response and recovery operations, and large-scale public health events.
- **Future Major Capability Goals:**
  - Integrated all-hazard personal protective ensembles
  - Interoperable and scalable regional response networks
  - Modeling capability to address all hazards in all terrain and meteorological conditions
  - Unified Incident Command decision support system enabling full implementation of the National Incident Management System

Support to DHS Components – USSS

- **Major Sub-activities:**

  United States Secret Service (USSS) **Emerging Threats** – assesses emerging threats to dignitaries and USSS assets
  - **Physical Personnel Safety** – develops escape hood technology
  - **Operational Security** – develops a ubiquitous mobile computing system
  - **Loss of Location Fidelity** – develops covert optical and chemical tagging and tracking tags
  - **Cyber Security** – develop a capability to send and receive encrypted image data

- **Major FY 2004-FY 2005 Accomplishments:**
  - Continued comprehensive assessments of emerging threats and evolving technologies that pose a threat to dignitaries and assets protected by USSS personnel.
  - Prototyped and deployed an enhanced law enforcement security-oriented simulation training system for the USSS-specific training and modeling.
  - Continued R&D of network protection systems and procedures designed to mitigate exploitation of site-specific "Very Large Scale Integration" (VLSI) control architectures encountered at an ever increasing number of protective venues.
  - Developed handheld, man-portable, concealable, wireless tracking device for locating operators of wireless communication device(s) in difficult radio frequency environments.
  - Developed, produced and deployed one-hundred (100) imaging stations to positions on or near the nation's borders to allow users real time access to the USSS's documents database to enhance law enforcement's ability to quickly detect counterfeit identification documents.
  - Initiated development of a lightweight, robust, escape hood capable of being carried discreetly within the suit jacket pocket of a USSS Agent during a protective detail.
  - Initiated a proof of concept trial to determine the viability of a ubiquitous mobile computing system that would allow secure wireless networked communication between unlike devices with high fidelity data transmission.
  - Developed a Global Information System project centering on a secure scalable streaming and secure transcoding methodology.

Support to DHS Components – USSS cont'd

- **Key FY 2006 Deliverables:**
  - Continue development of appropriate escape hood technology
  - Begin the development of a mobile platform that will be required to detect, exploit, and defend against covert and overt electronic surveillance systems
  - Continue (given a successful proof of concept in FY 2005) with the development of a ubiquitous mobile computing system that would allow secure wireless networked communication between unlike devices with high fidelity data transmission
  - Initiate an Optical & Chemical Tagging/Tracking Project to develop optical and chemical tags that are robust and covertly deployable.
- **Future Major Capability Goals:**
  - Maintain comprehensive threat awareness relevant to USSS mission.
  - Technical capabilities to defeat potential threats in both the protective and enforcement components of the USSS mission.

Support to DHS Components – USCG

- **Major Sub-activities:**

  United States Coast Guard (USCG)

  - **Situational Awareness for Maritime Domain Awareness** – develops automated classification and prediction capability for vessel intent in a port area
  - **Compel Compliance** – fields new capability to communicate and stop at-sea small prop-driven vessels and in-port swimmers/divers
  - **Boarding Capability** – improves space accountability for non-ferrous vessels
  - **Personnel Alerting and Contraband Detection and Identification** – adapts CBRN-E technologies to maritime environment
  - **Maritime Safety, Security and Mobility, and Protection of Natural Resources** - provides non-invasive treatment of ballast water for nuisance aquatic species, fields new techniques for stand-off detection of oil spills, and improves search and rescue capabilities

- **Major FY 2004 - FY 2005 Accomplishments:**
  - Assumed management of the CAPTAIN OF THE PORT ADVANCED TECHNOLOGIES INSERTION (CATs-I) program, at the USCG Sector Command Center (SCC) in South Florida. The HAWKEYE program provided an operational prototype venue to simultaneously demonstrate innovative maritime related technologies (such as Surveillance, Command & Control, Sensor Fusion, and Communications) and to assess technology performance with respect to its direct impact on mission execution.
  - Design modifications and operational testing of the BOAT TRAP entanglement system will improve Coast Guard's capability to compel compliance of uncooperative small vessels. Completed research on potential alternatives, requirements, and a technology assessment study to determine the applicability and potential for achieving performance goals for compelling compliance of large deep draft vessels.
  - An Integrated Anti-Swimmer prototype system was field tested; underwater imaging systems and an acoustic impulse device were also evaluated to establish performance expectations and to address system integration issues.
  - Completed a technology assessment for Multi-Purpose Tools to support boardings including necessary advances to provide reliable communications among boarding members and between the boarding team and the cutter.

Support to DHS Components – USCG cont'd

- **Key FY 2006 Deliverables:**

  Continuation of HLS mission research in the following areas:

  - Situational Awareness for Maritime Domain Awareness – develop automated classification and prediction capability for vessel intent with a port area.
  - Compel Compliance – field new capability to communicate and stop at-sea small prop-driven vessels and in port swimmers/divers.
  - Boarding Capability – improve space accountability for non-ferrous vessels.
  - Personnel Alerting and Contraband Detection and Identification – adapt breakthrough technologies in CBRNE countermeasures for the maritime environment.
- **Future Major Capability Goals:**
  - Ability to quickly and safely, with high confidence, determine a level of threat against a broad range of targets of interest up to 2000 nautical miles and inland waterways; includes detection of mines and underwater threats.
  - Offensive and defensive capabilities to control vessels and people through continuum of force while minimizing collateral effects and maximizing protection and safety.
  - Multipurpose capability to have space accountability: detect, localize and characterize contraband (CBRNE) at distances of 50 ft. or greater; ID people.
  - Protect boarding teams against hazardous substances and personal attack.

Threat & Vulnerability, Testing & Assessment - $47M

- **Major Sub-activities:**
  - **Knowledge Management Technologies** – develops computationally based tools and methods for assessing information about and creating, applying, and disseminating knowledge on terrorist threats and activities.
  - **Social Behavioral & Economic Analysis** – determines the motives and intents of and identifies terrorists by understanding the socio-political, cultural, economic, and behavioral aspects of terrorism and developing reliable biometric indicators.
  - **Information and Specialized Intelligence Assessment –**provides all WMD capability assessments to the Information Analysis and Infrastructure Protection (IAIP), S&T, and other DHS Directorates.
- **Major FY 2004 - FY 2005 Accomplishments:**
  - Delivered the Threat-Vulnerability Mapper (TVM), to provide the Information Analysis and Infrastructure Protection Directorate analysts with a simple, straightforward way to depict the geographic distribution of threats across the U.S. and to search the underlying databases for information on terrorists and attacks.
  - Created the knowledge management architecture, known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement) to integrate the various information analysis and synthesis, visualization, and knowledge discovery component capabilities.
  - Created the Interagency Center for Applied Homeland Security Technology (ICAHST) to provide detailed technical information and guide research, strategy, and systems design for the broad range of technologies and techniques necessary to identify, understand, and remediate CBRNE threats.
  - Completed an initial set of 120 all-CBRNE capability assessments for 20 terrorist organizations on the five CBRNE plus cyber threat agents. Continued support to the Nuclear Assessment Program (NAP) that judges the credibility of communicated nuclear threats for such clients as the FBI, DOE, and Department of State (DOS).
  - Established the Institute for Discrete Sciences (IDS), to investigate and develop the specialized computing algorithms and hardware architectures necessary to analyze massive amounts of diverse data from multiple, disparate, distributed data sources, and to model terrorist attacks and simulate consequences on a real-time, high-resolution basis.
  - Completed an engineering design for the Enhanced International Travel Security (EITS) system enabling implementation of pilot studies to be implemented with the United Kingdom, Canada, and Australia. EITS allows the validity of travel documents and the identity of travelers to be determined in real-time at U.S. borders and other points of entry.

Threat & Vulnerability, Testing & Assessment – cont'd

- **Key FY 2006 Deliverables:**
  - Enable the development of analytic resources and technologies to characterize terrorist capabilities, detect their activities, predict their intentions based on infrastructure vulnerabilities, strengthen preventive measures, and increase the ability to respond.
  - Provide an enhanced, integrated capability for information synthesis, relying on a foundation of advanced semantic processing and visual analytics and supported by specialized discrete mathematics techniques and technology. This will provide comprehensive knowledge discovery and dissemination capabilities to a diverse set of users – from first responders to intelligence analysts.
  - Develop a capability for information extraction, pattern discovery, group detection, and visualization for unstructured text as well as audio and video information to complement the existing capability for structured data.
  - Continue providing integrated capabilities to multiple DHS components, setting national agendas in visual analytics and discrete sciences, and furthering interagency cooperation.
  - Create a CBRNE threat encyclopedia and integrate with the ADVISE (Analysis, Dissemination, Visualization, Insight, Synthesis, and Enhancement) system.
  - Create a National Homeland Security Support System (NH3S) using the ADVISE architecture and providing quantitative risk analysis and decision support capabilities.
- **Future Major Capability Goals:**
  - A global capability for verifying the identity of travelers and the validity of travel documents.
  - Coherent, standardized capability for precise identification of individuals using multiple biometrics.
  - An interagency facility with direct real-time connections to data sources and response centers and with integrated knowledge management tools allowing information synthesis using advanced semantic processing and visualization in order to allow for information extraction, pattern discovery, and visualization from structured and unstructured data sources.
  - Consolidated formalized threat and capability assessments for internal use.
  - Predictive or prescriptive models of terrorist behaviors, motives, and intentions to enhance awareness of manifold threats and enable quantitative assessment of risk.

Emerging Threats - $10.5M

- **Major Sub-activities:**
  - **Near Term Projects and Future Technologies Solicitation** – funds near-term and breakthrough solutions to emerging threats.
  - **Emerging Threats Analysis** – sponsors all-inclusive analyses to identify previously unrecognized threats and to assess the relative importance of the threat in the context of homeland security.

- **Major FY 2004-FY 2005 Accomplishments:**
  - Established informal partnerships with the intelligence community and with the USSS portfolio to leverage ongoing activities in support of over-the-horizon assessment.
  - Initiated efforts, in combination with Rapid Prototyping, in both near-term and breakthrough solutions to homeland security issues. Near-term projects are funded out of the Rapid Prototyping Portfolio. Breakthrough projects are funded from the Emerging Threats Portfolio.

Emerging Threats – cont'd

- **Key FY 2006 Deliverables:**
  - Sponsor comprehensive assessments to identify and prioritize emerging threats. The outcomes of the assessments lead the strategic programs to integrate multiple disciplines and threat scenarios and comprehensively use intelligence-based information to establish organizational foresight.
  - Fund research dedicated to long-term, undefined threats as a means to exercise technology influence in the marketplace and build infrastructure to incentivize non-requirements driven, high-risk, high-payoff R&D, thereby promoting technology push and collaboration to solve otherwise intractable problems.
  - Complete development of projects initiated in FY 2005, and test and evaluate the products from these projects. Develop technologies and systems against emerging threats identified as a result of FY 2005 emerging threats analysis.
- **Future Major Capability Goals:**
  - Sponsor comprehensive assessments to identify and prioritize emerging threats. The outcomes of the assessments will lead the strategic programs to integrate multiple disciplines and threat scenarios and comprehensively use intelligence-based information to establish organizational foresight.
  - Fund research dedicated to long-term, undefined threats as a means to exercise technology influence in the marketplace and build infrastructure to incentivize non-requirements driven, high-risk, high-payoff R&D, thereby promoting technology push and collaboration to solve otherwise intractable problems.

Standards - $35.5M

- **Major Sub-activities:**
  - **Integrated Standards Process and Infrastructure** –maintains and improves development and promulgation of homeland security standards at the national level
    - **Conformity Assessment**– develops a systematic approach for adding conformity assessment programs for critical equipment, system, and personnel credentialing
  - **Standards for CBRNE and Cyber Countermeasures** –develops standards and test protocols for emerging CBRNE and Cyber countermeasure technologies
  - **Standards for Border and Transportation Security** – develops standards for biometrics, human factors,
  - **Standards for Emergency Preparedness and Response** – develops standard guides for preparedness and response planning, drills and exercises, incident management, and decontamination
    - **Standards for Personal Protective and Operational Equipment Standards for Geospatial Information**
    - **Standards for Training -** develops standard curricula for CBRNE topics
    - **Standards for Interoperable Communications** – develops a portal as a one-stop-shop for public safety agencies
  - **Standards for Informational Analysis and Infrastructure Protection** – develops standards for performance-based building codes, standards for technologies to clear up after CBRN releases in facilities, and standards for SCADA and industrial control systems.

Standards – cont'd

- **Major FY 2004-FY 2005 Accomplishments:**
  - Composed three management directives to establish DHS policy regarding the adoption and development of national standards.
  - Formed an interagency task force to address the controversy over the effectiveness and use of immunoassays for the detection of anthrax by emergency responders.
  - Evaluated a five step method to pre-screen suspicious white powders to look at the effectiveness of biological agent simulants, and the establishment of a program to address both chemical and biological decontamination standards for the first responder community.
  - Supported efforts to coordinate the development of a draft standard for hospital preparedness and to develop a multi-disciplinary Mission Essential Task List (METL) based on Emergency Responder Guidelines developed by the Office of Domestic Preparedness.
  - Supported development of a number of respiratory standards including three National Institute for Occupation Safety and Health (NIOSH) standards and one National Fire Protection Association (NFPA) standard.

Standards – cont'd

- **Key FY 2006 Deliverables:**
  - Continue to maintain and improve the process by which homeland security standards are developed and promulgated at the Federal level. Incorporate the appropriate conformity assessment program development into the standards development process. Maintain and update the homeland security standards database available to the homeland security community.
  - Continue to utilize interagency working groups to reevaluate requirements and prioritize needs for CBRNE countermeasures standards. Focus on developing sampling protocols and guidelines and standardized sample triage methods for CBRNE countermeasures. Focus on standards for emerging CBRNE countermeasures technologies including CBRNE point detectors; CBRNE stand off detectors and urban surveillance technologies such as BioWatch, CBRNE facility monitors, and water distribution monitors. Continue programs to address multimodal biometrics, latent fingerprints, rapid biometric evaluations, and biometric image and feature quality. Also explore and evaluate ergonomics, human factors, and usability issues of biometric sensors, software, and systems.
  - Continue with the completion of a standard guide for building event dispersion and health assessment preparedness and response planning and the standard guide for conducting emergency preparedness drills and exercises.
  - Continue current CBRNE personal protective and operational equipment specifically focusing on completing the suite of respiratory protection equipment standards to include powered air purifying respirators, closed-circuit self contained breathing apparatus, supplied air respirators and combination respirators.
  - Support the development of comprehensive standards related to the development, testing, and certification of effective robotic technologies for urban search and rescue (US&R). These US&R robotics standards include sensing, mobility, navigation, planning, integration, and operator interaction with search and rescue robot systems, as well as ensuring that the robots can meet operational requirements.
- **Future Major Capability Goals:**
  - Develop, adopt, and implement an integrated suite of standards for ensuring the effectiveness of all scientific and technological tools essential for homeland security.
  - Set metrics for products, services, guidelines, performance specifications, testing and evaluation protocols, training, and certification of equipment and personnel.
  - Provide programs to ensure compliance with established standards.
  - Implement a conformity assessment program to fulfill DHS needs for certification and accreditation.

University and Fellowship Programs - $63.6M

- **Major Sub-activities:**
  - **Scholars and Fellows**
  - **Centers of Excellence**
- **Major FY 2004-FY 2005 Accomplishments:**
  - Established four university Centers of Excellence:
    - The Center for Risk and Economic Analysis of Terrorism Events, at the University of Southern California and its partners will receive $12 million over three years to evaluate the risks, costs and consequences of terrorism and to guide economically viable investments in countermeasures.
    - The National Center for Foreign Animal and Zoonotic Disease Defense at Texas A&M and its partners will receive $18 million over three years to address potential threats to animal agriculture including Foot and Mouth Disease, Rift Valley fever, Avian influenza and Brucellosis. In addition to working closely with industry and government, they will work with DHS's Plum Island Animal Disease Center.
    - The National Center for Food Protection and Defense at the University of Minnesota and its partners will receive $15 million over three years to establish best practices and attract new researchers to manage and respond to food contamination events, both intentional and naturally occurring.
    - The University of Maryland (UMD) and its partners as the Center for Behavioral and Social Research on Terrorism and Counter-Terrorism. This Center will be funded at $12 million for three years following contract award.
  - Selected approximately 200 students for the DHS Scholars and Fellows from 93 institutions (including Historically Black Colleges and Universities/Minority Serving Institutions) in 38 states and the District of Columbia.

University and Fellowship Programs – cont'd

- **Key FY 2006 Deliverables:**
  - Establish at least three additional Centers of Excellence.
  - Maximize collaboration with other Federal agencies, by collaborating with EPA's Science to Achieve Results (STAR) Program on microbial risk assessment. The DHS-EPA cooperative Center on Microbial Risk Assessment will result in one five-year grant to a university-based consortium and will be jointly funded by both agencies for a total of $10 million.
  - Conduct an additional cycle of the Fellows and Scholars Program.
- **Future Major Capability Goals:**
  - A new generation of scientists and engineers are educated in scientific and technology issues related to homeland security.
  - A suite of academic institutions, in partnership with private industry and public sector research enterprises, are applied to research topics to solve broad-based homeland security problems.

Cyber Security - $16.7M

- **Major Sub-activities:**
  - **Cyber Security R&D Center** – A "virtual" R&D center with a significant focus on outreach to university, private sector, and venture capital communities.
  - **Internet Infrastructure Security** – Development of models, tools, reference implementations and guidelines associated with more secure versions of key Internet communication protocols.
  - **Next-Generation Cyber Security Technologies** – Emphasis on development, testing, evaluation, and piloting of new generations of cyber security technologies.
  - **Cyber Security Testbed** – Development of a large scale cyber security testbed network and associated software testing infrastructure.
  - **Large-Scale Network Data Sets** – Continue ongoing collection, refreshing and sharing of data sets.
- **Major FY 2004 - FY 2005 Accomplishments:**
  - Completion and operational use of the full-scale cyber security testbed network.
  - Developing a roadmap, in partnership with Federal researchers and officials and the private sector, to accelerate the development and deployment of a secure domain name infrastructure. Current work also includes the identification of technology requirements and development of models to aid in assessing the performance impact of utilizing Domain Name System Security Extensions (DNSSEC) in operational environments.
  - Initiated an effort to address different facets of the need for improved methods for cyber security testing and assessment, with emphasis on economic assessment, in order to provide a foundation for the long term goal of economically-informed risk-based cyber security decision making.
  - Initiated dialog aimed at international collaboration on cyber security R&D with Canada, the United Kingdom, and Japan.
  - Providing technical support for cyber security program execution through the "virtual" Cyber Security R&D Center, supporting pre-research activities (such as developing roadmaps, organizing workshops and meetings, aiding in drafting research solicitations and proposal review), as well as post-research activities (such as facilitating pilot tests and exercises, venture capital community outreach, private sector outreach, and interfacing with non-government R&D communities).

Cyber Security – cont'd

- **Key FY 2006 Deliverables:**
  - Continue to provide support to the Directorate in pre-research activities and post-research activities through the "virtual" Cyber Security R&D Center.
  - Initiate a new multi-year next-generation technologies R&D program phase.
  - Complete full-scale operational test bed, acquisition and generation of network data sets, enhancement of remote management and configuration capabilities, and a final project report.
  - Developing software reference implementations of the Domain Name System Security Extensions (DNSSEC) for servers and client applications, and planning for pilot deployments of DNSSEC. Direct investments in the area of routing protocol security at the development of a modeling and simulation framework for impact assessment of secure routing protocols on the Internet performance.
- **Future Major Capability Goals:**
  - Creation of secure routing protocol (i.e., a secure equivalent to the Border Gateway Protocol), with Internet infrastructure providers moving out with deployments.
  - Significant deployment of DNSSEC into the Internet with emphasis on critical information infrastructure.
  - Interactions between DHS/NSF-funded DETER testbed and other separately-funded testbed activities.
  - Economically informed risk-based cyber security decision making capability.
  - Technology for automated scanning of code for vulnerabilities.
  - Tools and techniques to detect, respond to, and recover from large scale cyber attacks.
  - Tools for network forensics and attribution.
  - Secure wireless technology that can be reliably used.

Critical Infrastructure Protection (CIP) - $20.8M

- **Major Sub-activities:**
  - **Modeling, Simulation and Analysis** - develop tools to simulate and assess the structures and interdependencies of interrelated critical infrastructure components in order to identify and prioritize key vulnerabilities and mitigation solutions.
  - **Protective Security Technologies** – conduct vulnerability studies and develop key enabling technologies for physical protection of critical infrastructure and resources
  - **National CIP R&D Plan** – develop the annual plan required by HSPD-7

- **Major FY 2004 - FY 2005 Accomplishments:**
  - Developed a CIP Decision Support System (DSS) focused on prioritizing investment, protection, mitigation, response, and recovery strategies related to Critical Infrastructure Protection. The prototype model includes representation of all critical infrastructure sectors, as well as their interdependencies. Preliminary test cases have been used to develop consequence estimation features of the CIP-DSS at both national and metropolitan scales.
  - Initiated a system study to find potential solutions for personnel surety for security guards that protect our Nation's Critical Infrastructure, as well as insiders with access to sensitive areas of, or information about the infrastructure.
  - Supported a System Study for Municipal Domestic Water Security.
  - Initiated interagency development of the first annual National Critical Infrastructure Protection R&D Plan using the Infrastructure Subcommittee of the National Science and Technology Council.
  - Initiated cooperative and collaborative research and development project with the Kentucky Homeland Security University Consortium.

Critical Infrastructure Protection (CIP) –cont'd

- **Key FY 2006 Deliverables:**
  - Incorporate a metropolitan area modeling capability, adversary-defender constraint and information dynamics models, and an enhanced threat spectrum capability into the CIP-DSS.
  - Complete pilot tests of the CIP-DSS in several state and regional areas.
  - Publish the National Academy Study on Security of the Electrical Industry.
  - Complete the quick-look system studies of all Critical Infrastructures and Key Resources, and the end-to-end System Study for Municipal Domestic Water Security.
  - Deliver improved closed circuit TV (CCTV) components for object identification and behavior recognition. Deliver an enhanced threat detection CCTV system based on video image understanding architecture, including the improved CCTV components.
  - Deliver the second annual National CIP R&D Plan with agency budget information and a roadmap for deliverables. Incorporate relevant inputs from: a) federal agencies including activities, and levels of effort; b) critical infrastructure sector owners and operators; and c) private and public research institutions and universities.
- **Future Major Capability Goals:**
  - Secure electronic and digital Critical Infrastructure control systems including sensing and control systems.
  - Real time decision support modeling for decision makers in emergencies including prioritization strategies, as well as protection, mitigation, and response strategies.
  - Integrated, layered perimeter defense for high-value targets and cost efficient self-healing materials to withstand projectiles and small arms munitions.
  - Facility protection measures including embedded sensors and blast hardened material and designs and a secure HVAC detection and response system.
  - Low-cost, high performance intelligent and integrated monitoring systems with low dependence on operators.

Research and Development Consolidation - $116.9M

Purpose:

To align with the guidance from Congress to functionally integrate the RDT&E activities within the Department. This action will: bring under a single accountable authority the scientific and engineering personnel and other RDT&E resources of the Department; maximize the efficiency and effectiveness of the RDT&E capacity; develop and expand synergistic RDT&E programs that cut across the Department's activities; create an opportunity for a world-class RDT&E capabilities; allow other Directorates and organizational elements to focus on their operational missions, and eliminate within them the specialized management infrastructure required to manage organic RDT&E. S&T will have Line Management Authority of the following:

- Transportation Security Laboratory
- Applied Technology Division (ATD) Research, Development & Evaluation Branch
- Control System Security Test Center
- Institute for Information Infrastructure Protection
- New Mexico Institute of Mining & Technology Energetic Materials Research & Testing Center (EMRTC)

Rapid Prototyping - $20.9M

- **Major FY 2004-FY 2005 Accomplishments:**
  - Initiated efforts to address chemical and biological threats, explosive detection, training technology tools, improvised nuclear device defeat, and investigative and forensic support topics.
  - Developed a joint port and coastal surveillance prototype designated HAWKEYE with the United States Coast Guard (USCG) that provides an integrated maritime surveillance system covering Port Everglades, Miami, and Key West, Florida.
  - Initiated the implementation of the Technology Clearinghouse as required in the Homeland Security Act of 2002.
  - Continued to fund projects initiated under the *Near Term Projects and Future Technologies Solicitation,* and the *Support to State and Local Responders* and *Rapid Prototyping Support to Federal DHS Missions* programs.
- **Key FY 2006 Deliverables:**
  - Transition mature programs from the development phase to operational testing and evaluation.
  - Continue to support the Technology Clearinghouse
  - Continue to fund projects initiated under the *Near Term and Future Technologies* solicitation released in FY 2004, and complete the development of projects initiated in FY 2005 under *Support to State and Local Responders* and *Rapid Prototyping Support to Federal DHS Missions,* and test and evaluate the products from these projects.
- **Future Major Capability Goals:**
  - Continue to Identify new technology candidates and capabilities to meet the existing and emergent technical requirements of the Department.
  - Continue to meet the requirements of Section 313 of the Homeland Security Act of 2002.

Counter-MANPADS - $110M

- **Major Sub-activities:**
  - **System Development and Demonstration (SD&D), Phase II** – conducts independent testing of contractor systems via flight tests on selected commercial aircraft
  - **Report SD&D Findings System SD&D, Phase III** – installation, if approved, of pre-production Counter-MANPADS equipment on aircraft for operational testing and evaluation, including live fire tests.
- **Major FY 2004 - FY 2005 Accomplishments:**
  - Initiated and completed Phase I following a competitive bidding process for a two-year System Development and Demonstration (SD&D) effort. The focus was on proving the feasibility of migrating existing DoD technology into the commercial sector and exploring other technology as appropriate. Following Preliminary Design Reviews, the Phase I portion of the twenty-four month SD&D effort concluded and DHS initiated a selection evaluation process to determine which companies would be selected to further mature their preliminary designs, build representative prototypes, install them on aircraft, and conduct formal testing during the Phase II eighteen month effort.
  - Hosted a Stakeholders' Meeting, attended by representatives of the airlines, the equipment manufacturers, and other affected sectors, including representatives of multiple Federal government Departments and Agencies.
  - During Phase II, the contractors will complete redesigns and undergo Critical Design Review. The contractors will fabricate, install, and test their prototypes on commercial aircraft. Each will deliver two complete units to demonstrate performance, integrate products onto aircraft, and conduct studies to emphasize operational suitability and to validate costs. The FAA will certify aircraft safety and airworthiness of the integrated countermeasures. DHS performance tests will include operational effectiveness testing in commercial aircraft environments, wind tunnel tests, reliability testing, missile detection, track accuracy and maintainability demonstrations.

Counter-MANPADS – cont'd

- **Key FY 2006 Deliverables:**
  - Build, deliver, install, and fly pre-production counter-MANPADS equipment on commercially-operated aircraft by US cargo carriers similar to those aircraft used for the Civil Reserve Air Fleet (CRAF) operations.
  - Conduct operational testing and evaluation and data collection on multiple aircraft types to capture operational and maintenance costs as well as technical performance and reliability data in a commercial operational environment.
  - Modify Phase II systems to incorporate new design requirements including reliability, technology protection, and emergency ground notification improvements based on test and evaluation results.
  - Examine maintaining two contractors in Phase III to foster competition, and to promote manufacturing should a full-rate decision be made.
  - Conduct an aggressive reliability growth effort to increase system reliability to 3000 hours and reduce recurring support costs.
  - During CY 2006, conduct Live-Fire Test and Evaluation assessment
  - Continue on-going dialogues with Original Equipment Manufacturers (OEM) such as Boeing and Airbus and conduct studies to scope the effort required to include provisions for Counter-MANPADS systems on future production aircraft.
  - Pursue Federal Aviation Administration certification for additional aircraft types/models/series not addressed in Phase II.
- **Future Major Capability Goals:**
  - A very reliable system to protect commercial aircraft from the threat of shoulder-fired missiles with virtually no export restrictions designed into aircraft on the production line.

Office of Interoperability and Compatibility - $20.5M

- **Major Sub-activities:**
  - Communications – Will incorporate SAFECOM activities and add technical assistance, pilot interoperability programs, a national interoperability baseline, identification of emergency responder spectrum needs, update the Interoperability Statement of Requirements, and update common grant guidance.
    - SAFECOM – SAFECOM will continue development of a national communications architecture, interoperability standards, and coordination of Federal programs.
  - Equipment – Inventory first responder equipment programs to identify duplication and overlap and identify interoperability/compatibility needs, ensure standards development to support interoperability, create a Federal coordinating structure, and develop common grant guidance.
  - Training- Inventory first responder training programs to identify duplication and overlap and identify interoperability/compatibility needs, ensure standards development to support interoperability, create a Federal coordinating structure, and develop common grant guidance
- **Major FY 2004 - FY 2005 Accomplishments:**
  - Established credibility with first responder community
  - National Statement of Requirements
  - Interoperability Continuum
  - RAPIDCOM
  - Common Grant Guidance
  - Interoperability information portal
  - Inventory of program
  - Federal Interagency Coordination

Office of Interoperability and Compatibility – cont'd

- **Key FY 2006 Deliverables:**
  - National interoperability baseline
  - Updated Statement of Requirements
  - Standardization of architectural framework
  - Implementation of architectural framework
  - Accelerated interoperability standards process
- **Future Major Capability Goals:**
  - Coordinated Federal, state, and local approach for communications interoperability and compatibility
  - Consistent and standardized operational test and evaluation programs for emergency responder technologies

SAFETY Act - $5.6M

- **Major Sub-activities:**
  - **SAFETY Act Implementation** – evaluates technologies to advise DHS on the appropriateness of granting protections under the SAFETY Act to sellers of qualified technologies.
- **Major FY 2004 - FY 2005 Accomplishments:**
  - Created the Office and the mechanisms to implement the SAFETY Act.
  - Drafted, responded to comments, and implemented a draft regulation and revised the Interim Rule.
  - Designed and implemented a web-based application kit and interactive help process.
  - Conducted one-day outreach seminars across the country.
  - Received and acted upon 30 full applications and 120 pre-applications.
- **Key FY 2006 Deliverables**
  - Implement a process to support federal procurement officials.
  - Complete the Final Rule.
  - Continue to improve SAFETY Act implementation and outreach approaches.

Summary of Budget Estimates

	FY 2004 Enacted	FY 2005 Enacted	FY 2006 CJ Budget Estimate	INCREASE (+) OR DECREASE (-) FOR FY 2006 Total Changes	Pr
Total Salary and Expense (Discretionary)	44.2	68.6	81.4	12.8	
Bio Countermeasures (includes NBACC)	285.0	397.7	362.3	-35.4	
Chemical Countermeasures	52.0	53.0	102.0	49.0	
High-Explosives Countermeasures	9.5	19.7	14.7	-5.0	
Radiological and Nuclear Countermeasures	126.3	122.6	19.1	-103.5	
Domestic Nuclear Detection Office (DNDO)	0.0	0.0	227.3	227.3	
Threat and Vulnerability, Testing and Assessments	67.2	65.8	47.0	-18.8	
Standards	39.0	39.7	35.5	-4.2	
Support of Department of Homeland Security Components	34.0	54.7	93.7	39.0	
University and Fellowship Programs	68.8	70.0	63.6	-6.4	
Emerging Threats	21.0	10.8	10.5	-0.3	
Rapid Prototyping	73.0	76.0	20.9	-55.1	
Counter MANPADS	60.0	61.0	110.0	49.0	
SAFETY Act		10.0	5.6	-4.4	
Office of Interoperability and Compatibility		21.0	20.5	-0.5	
Critical Infrastructure Protection	14.8	27.0	20.8	-6.2	
Cyber Security	18.0	18.0	16.7	-1.3	
Research and Development Consolidation	0.0	0.0	116.9	116.9	
Subtotal, Budget Authority (All Sources)	868.6	1,046.9	1,287.0	240.2	
Total enacted appropriations and budget estimates	912.8	1,115.5	1,368.4	253.0	

Homeland Security

Estimated FY 2005 Budget Splits

Performer	FY 2005 Projected
Private Sector	$650M
National Laboratories	$250M
University Programs	$72M
Other Public Sector Government	$80M

S&T Executing Directorates	FY 2005 Projected
Homeland Security Advanced Research and Development Agency (HSARPA)	$289M
Office of Research and Development	$424M
Systems Engineering and Development (SED)	$199M

Homeland Security

Homeland Security