

Department of Homeland Security Science & Technology

Presentation to 6th Annual Network Science Workshop

Dr. Daniel Gerstein
Deputy Under Secretary for Science & Technology

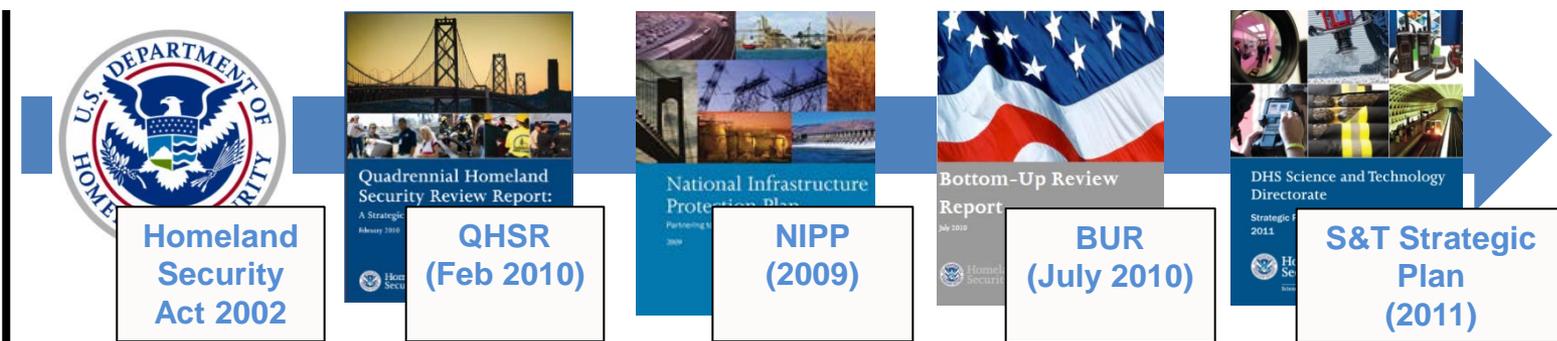
April 23, 2012



Homeland Security

DHS S&T Mission Guidance

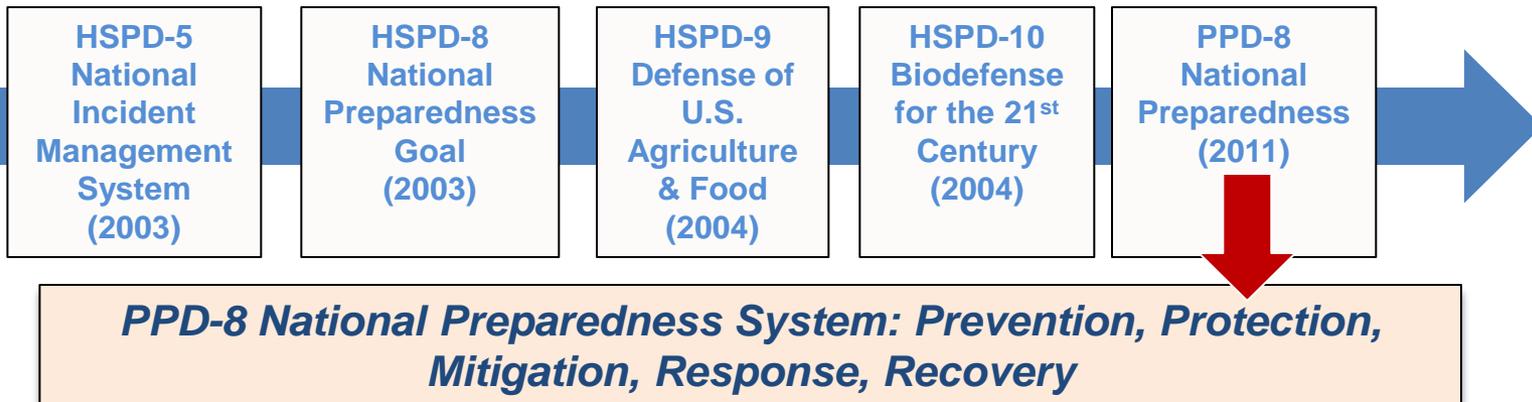
Strategic Guidance



DHS Core Missions

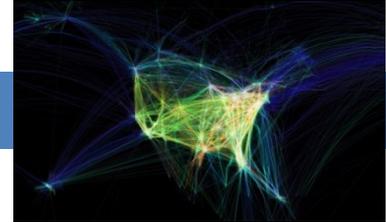
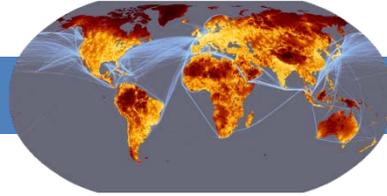
- | | |
|---|--|
| <ol style="list-style-type: none"> 1. Preventing terrorism & enhancing security 2. Securing and managing our borders 3. Enforcing and administering our immigration laws | <ol style="list-style-type: none"> 4. Safeguarding and securing cyberspace 5. Ensuring resilience to disasters 6. Maturing & Strengthening the Homeland Security Enterprise |
|---|--|

Operational Directives



Greater Use of Technology, More Threats

Globalization & Transportation



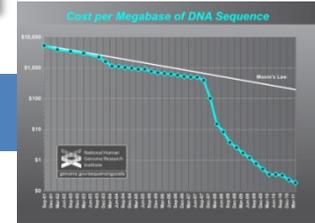
Border Security & Immigration



Violent Extremism



Misuse of Technology



Natural Disasters & Pushing Beyond Design Limits

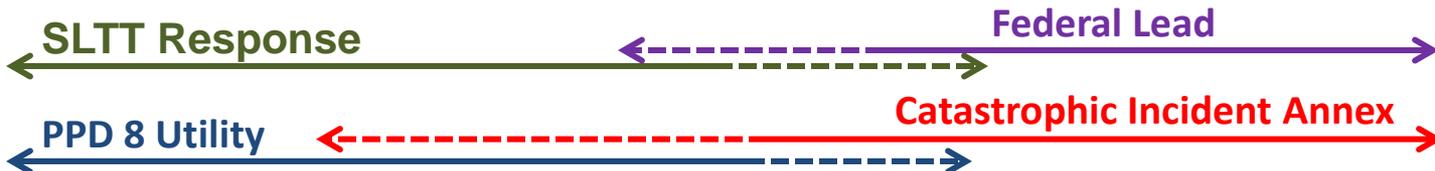
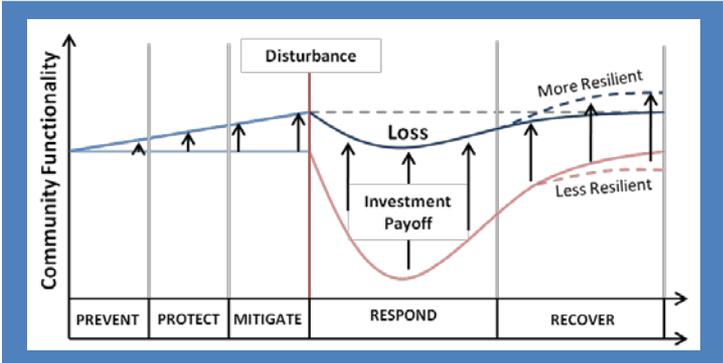
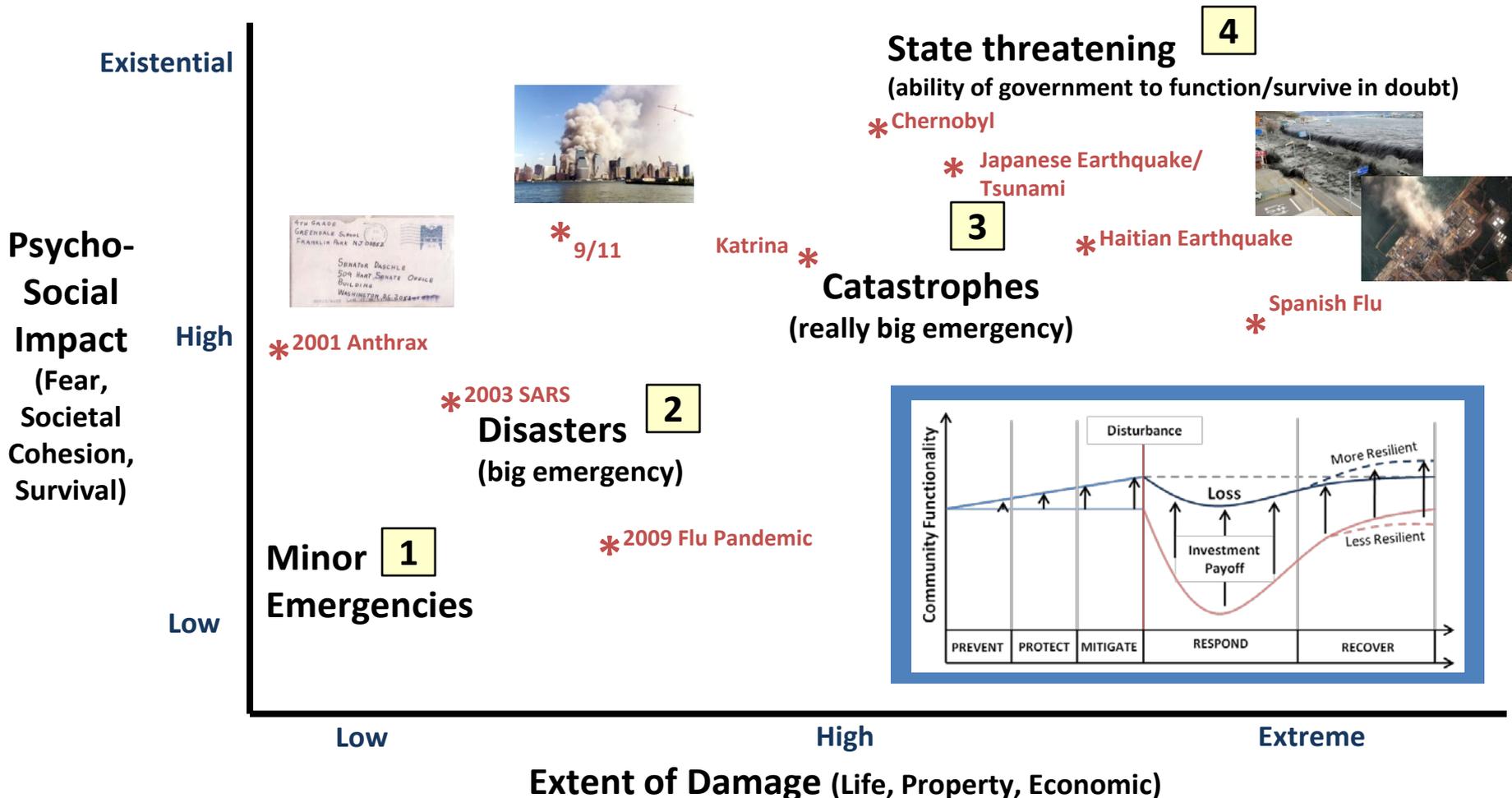


Evolution of Terrorist Attacks in Aviation

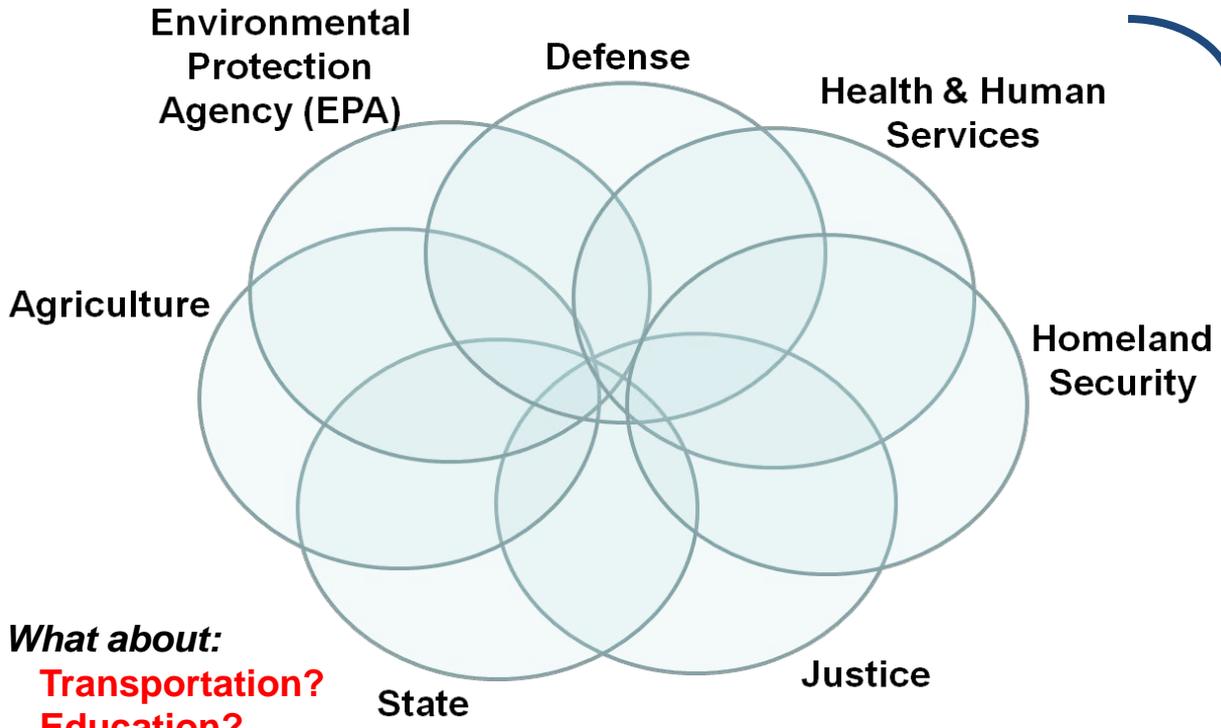
Timeframe	Event/Threat	Vulnerability	Response
1970's	Hostage/Hijacking	Guns, weapons	Magnetometers
1988	Pan Am 103, Lockerbie	Bomb in baggage	Baggage scans
Sept 2001	World Trade Center (WTC), Pennsylvania, Pentagon	Box cutters, etc	Transportation Security Administration (TSA)
Dec 2001	Richard Reid	Shoe bomb	Shoes removed
2004	Chechen suicide attacks	Vests	Pat downs, backscatter
2006	Heathrow liquids plot	Novel liquid bomb	Liquids ban
2009	Non-metallic body bomb	Body bomb in sensitive area	Explosive Trace Detection (EDT), Whole Body Imaging (WBI), Pat down
2010	Printer cartridge bombs	Explosives packed in cargo	Trace detection for cargo



Complicating Factor #1: Dimension of Emergencies

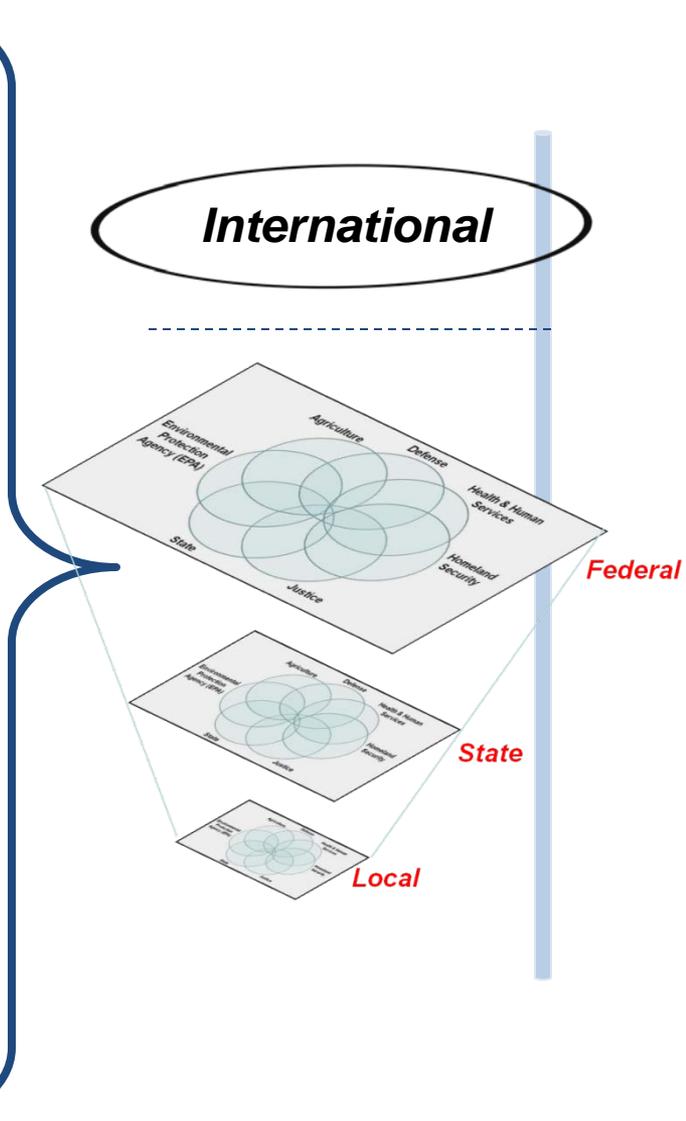


Complicating Factor #2: Number & Diversity of Key Actors



What about:
Transportation?
Education?
Commerce?
Others ...

Must develop common understanding of the threat, lexicon, plans, procedures, communications, etc.



Complicating Factor #3: DoD Versus DHS

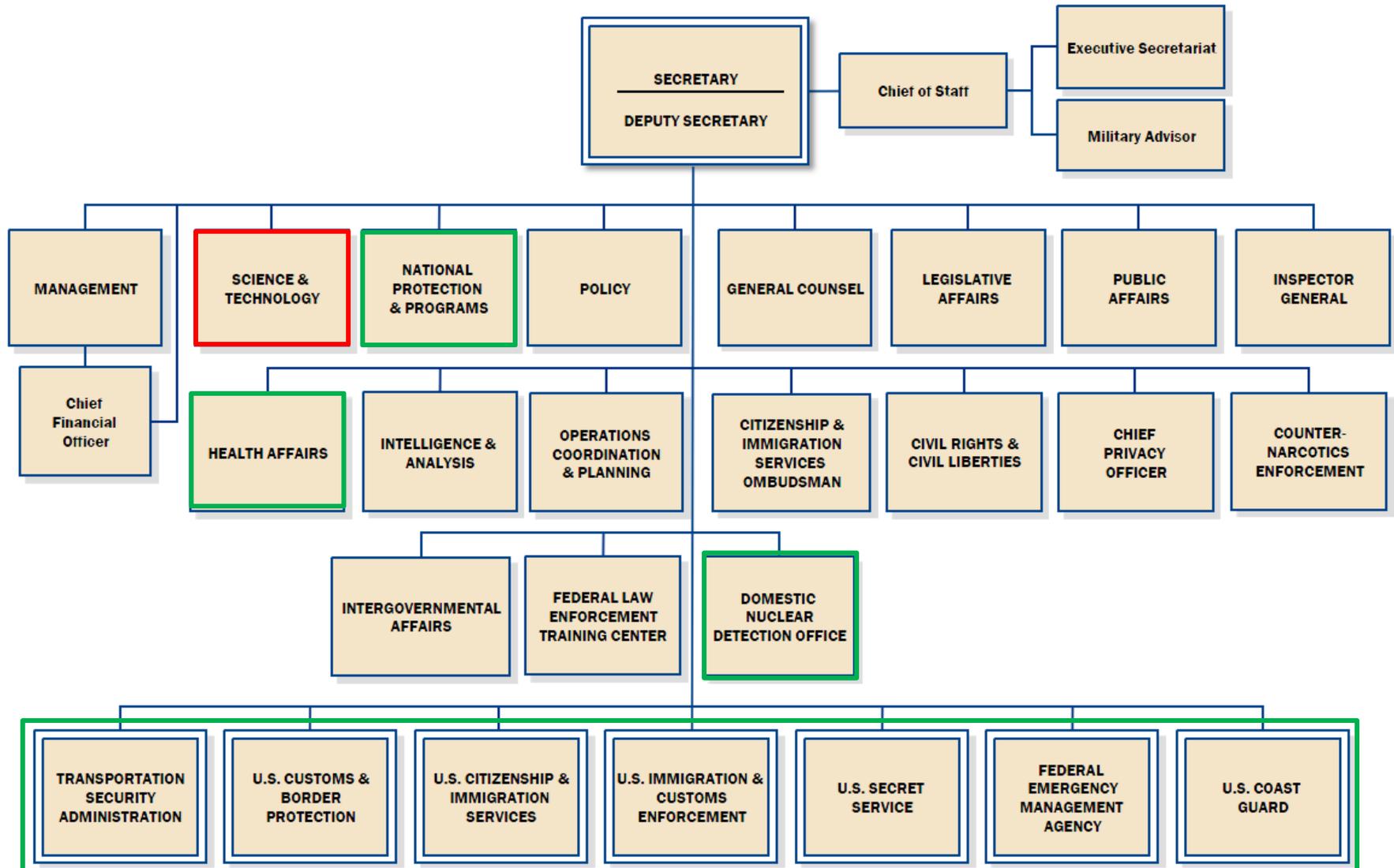
DoD

DHS



Can result in difficulty directly infusing military technology and equipment into the operational work of DHS Components and first responders ...

Department of Homeland Security



How to Achieve the S&T Mission in this Challenging Environment?

- ❑ Organization of S&T aligned with missions
- ❑ Maximizing Technology Returns in Challenging Fiscal Times
- ❑ Developing a “systems” approach to S&T
- ❑ Building a balanced portfolio
- ❑ Technology Foraging
- ❑ Supporting the Homeland Security Enterprise (HSE)



How to Achieve the S&T Mission in this Challenging Environment?

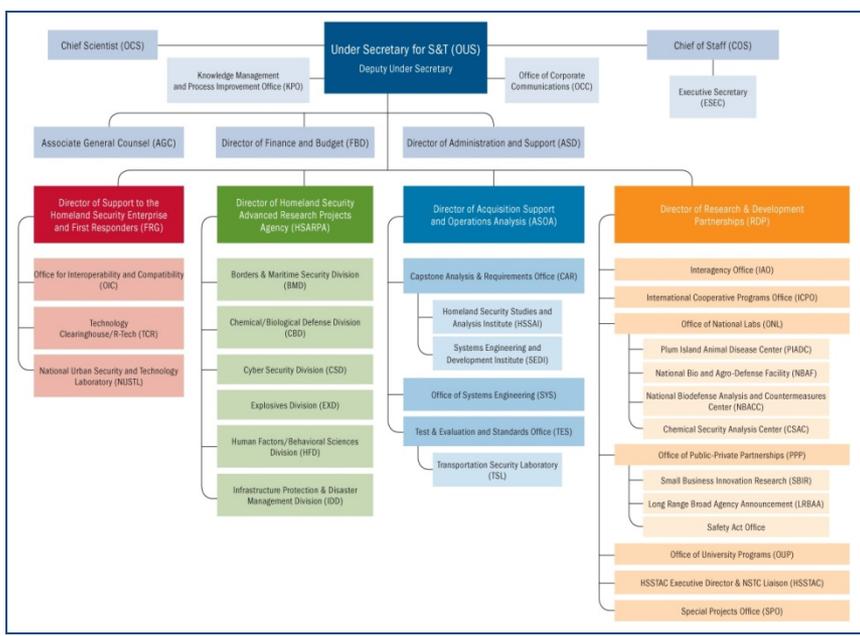
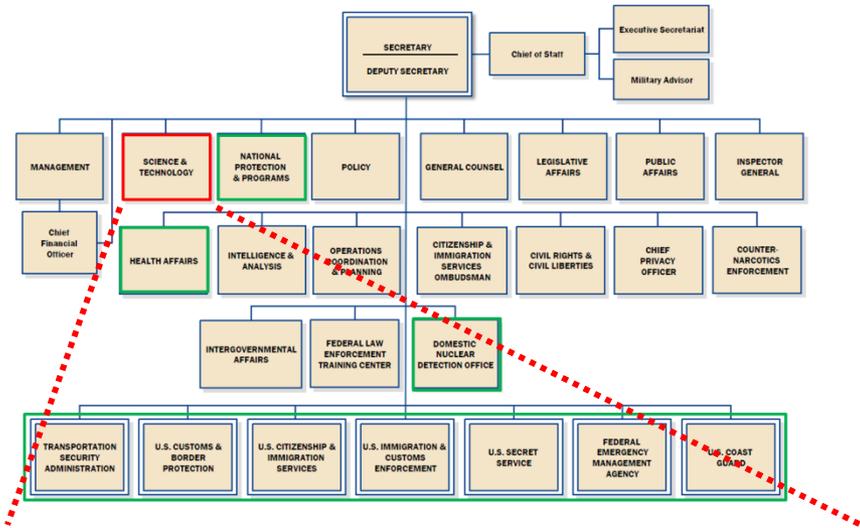
□ S&T Mission

- Strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise (HSE)

□ Achieving the S&T Mission in this Challenging Environment

- **Operationally focused** ... S&T provides the HSE with strategic and focused technology options and operational process enhancements
- **Innovative** ... S&T seeks innovative, systems-based solutions to complex homeland security problems
- **Partnerships** ... S&T has the technical depth and reach to discover, adapt and leverage technology solutions developed by federal agencies and laboratories, state, local and tribal governments, universities, and the private sector - across the US and internationally

Department of Homeland Security Support to Critical Infrastructure



18 Critical Infrastructure Areas

		
Agriculture & Food	Banking & Finance	Chemical Sector
		
Comms Sector	Commercial Facilities	Critical Manufacturing
		
Dams	Information Technology	Energy
		
Government Facilities	Healthcare and Public Health	Water
		
Nuclear Reactors, Materials and Waste	Postal and Shipping	Defense Industrial Base
		
Transportation Systems	National Monuments Icons	Emergency Services

HSARPA Technical Divisions Example Projects



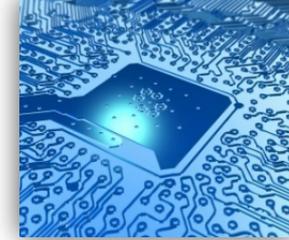
Borders & Maritime

- Buried tripwires
- Mobile surveillance systems
- Tunnel detection and monitoring
- Air-based sensor technologies
- Maritime security of surface and underwater contraband threats



Chem-Bio

- Understanding and analyses of chem-bio threats
- Point-of-care diagnostics
- Enhance the capability to inform attribution of attacks
- Develop countermeasures against foreign animal disease



Cyber

- Decrease vulnerability to malicious and natural events
- Develop protocols essential to trustworthy cyber systems
- Attract next generation cyber security warriors
- Provide tools cyber criminal and terrorist investigations



Explosives

- Passenger and cargo safety at airports & checkpoints
- Protect national infrastructure from explosive threats
- Protect people & facilities in high volume, fast-paced systems
- Support TSA, USSS, First Responders, CBP



Human Factors

- Target and screen people, land vehicles, and sea containers
- Biometric Identity management
- Verify identities, assess intent, & authenticate documentation
- Understand operational threats, improve operator performance, improve sensor technologies

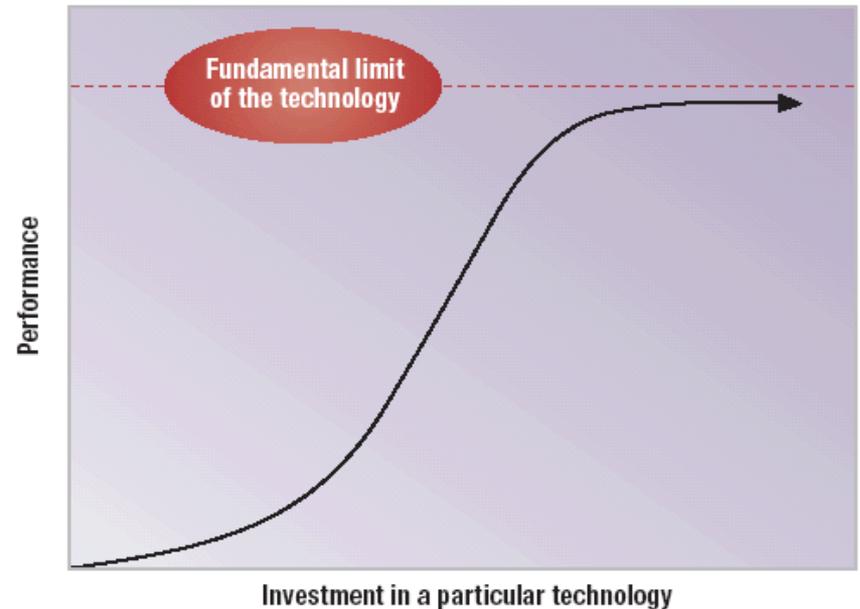


Infrastructure Protection & Disaster

- Evacuation modeling & simulation
- Incident management
- Overhead imagery for disasters
- Location of first responders in challenged environments
- Electric grid resilience
- Levee & tunnel breach mitigation

Maximizing Technology Returns in Challenging Fiscal Times

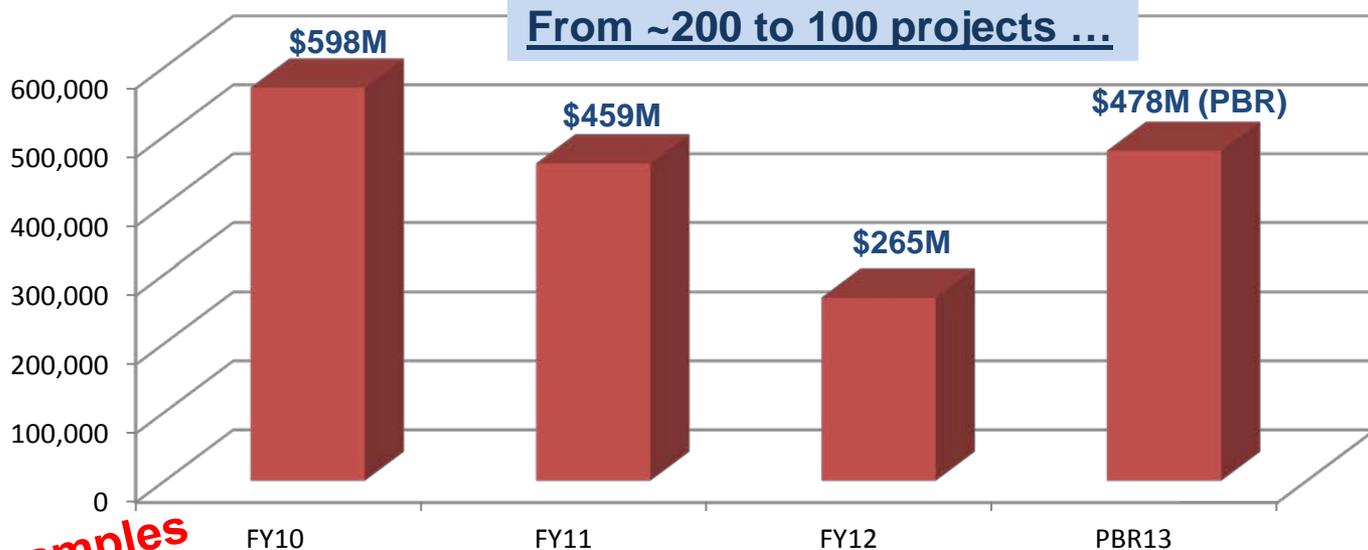
- ❑ **Going from R&D to r&D**
 - Reduced basic and applied research
 - Emphasize near-term development, transition to use
- ❑ **Focus on developing operational and innovative solutions for the HSE**
 - Portfolio balanced towards finding high payoff areas & game changing solutions
 - Partner focus
- ❑ **Preserve investments in uniquely S&T arenas**
 - Biodefense; explosives detection in aviation; cybersecurity for .gov and .com; first responder support
- ❑ **Greater reliance on:**
 - Interagency
 - International
 - Industry
 - Partnerships, in general
- ❑ **Leverage others' investments**
 - Learning from others
 - Serve as a tech clearinghouse
 - Collaboration with interagency and internationally
 - Tech foraging



Maximizing Technology Returns in Challenging Fiscal Times

S&T Discretionary R&D

(\$ in Thousands)



Current Priorities

- Cybersecurity
- Biodefense
- Home Made Explosives (HME)
- First Responders

Examples

Divested (FY12) & Resumed (FY13)	Increases	New Starts
<ul style="list-style-type: none"> <input type="checkbox"/> Small Dark Aircrafts <input type="checkbox"/> Tunnel Detection <input type="checkbox"/> Joint Agro Defense Office (JADO) <input type="checkbox"/> System Studies <input type="checkbox"/> Passive Methods for Precision Behavioral Screening <input type="checkbox"/> Biometrics <input type="checkbox"/> Chem-Bio Event Characterization <input type="checkbox"/> Community Resilience <input type="checkbox"/> IP Communications Test & Eval 	<ul style="list-style-type: none"> <input type="checkbox"/> Border Security--\$16M <input type="checkbox"/> Bio-Security--\$58M <input type="checkbox"/> Chem-Security--\$5M <input type="checkbox"/> Cyber Security--\$23M <input type="checkbox"/> Explosives--\$39M <input type="checkbox"/> First Responder s--\$12M <input type="checkbox"/> Identity Management--\$15M <input type="checkbox"/> Info Sharing & Interoperability--\$17M <input type="checkbox"/> Natural Disaster Resiliency--\$13M 	<ul style="list-style-type: none"> <input type="checkbox"/> Security in Cloud-Based Systems (sCBS) <input type="checkbox"/> Rad/Nuc Response/Recovery <input type="checkbox"/> Biometric Data Interoperability <input type="checkbox"/> Social Media Disaster Resilience <input type="checkbox"/> Integrated Passenger Screening <input type="checkbox"/> PB Threat Imaging Sensor Development <input type="checkbox"/> Portable Detection <input type="checkbox"/> Safe Bulk Detection

A Systems Approach: Strategy to Action

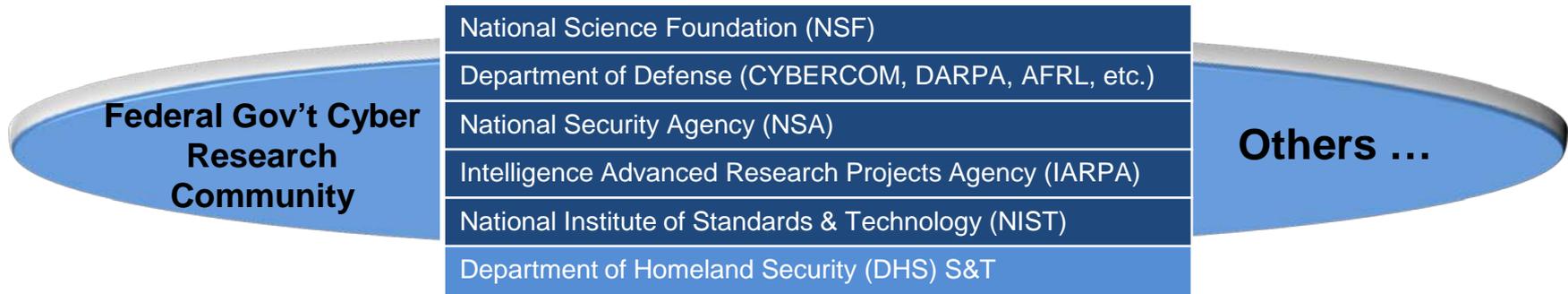
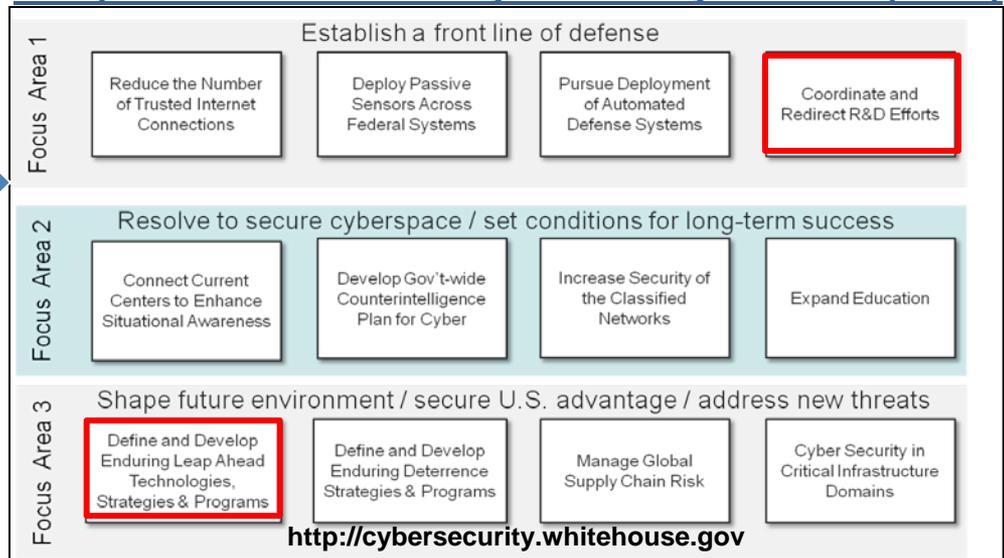
The Cyber Threat Spectrum



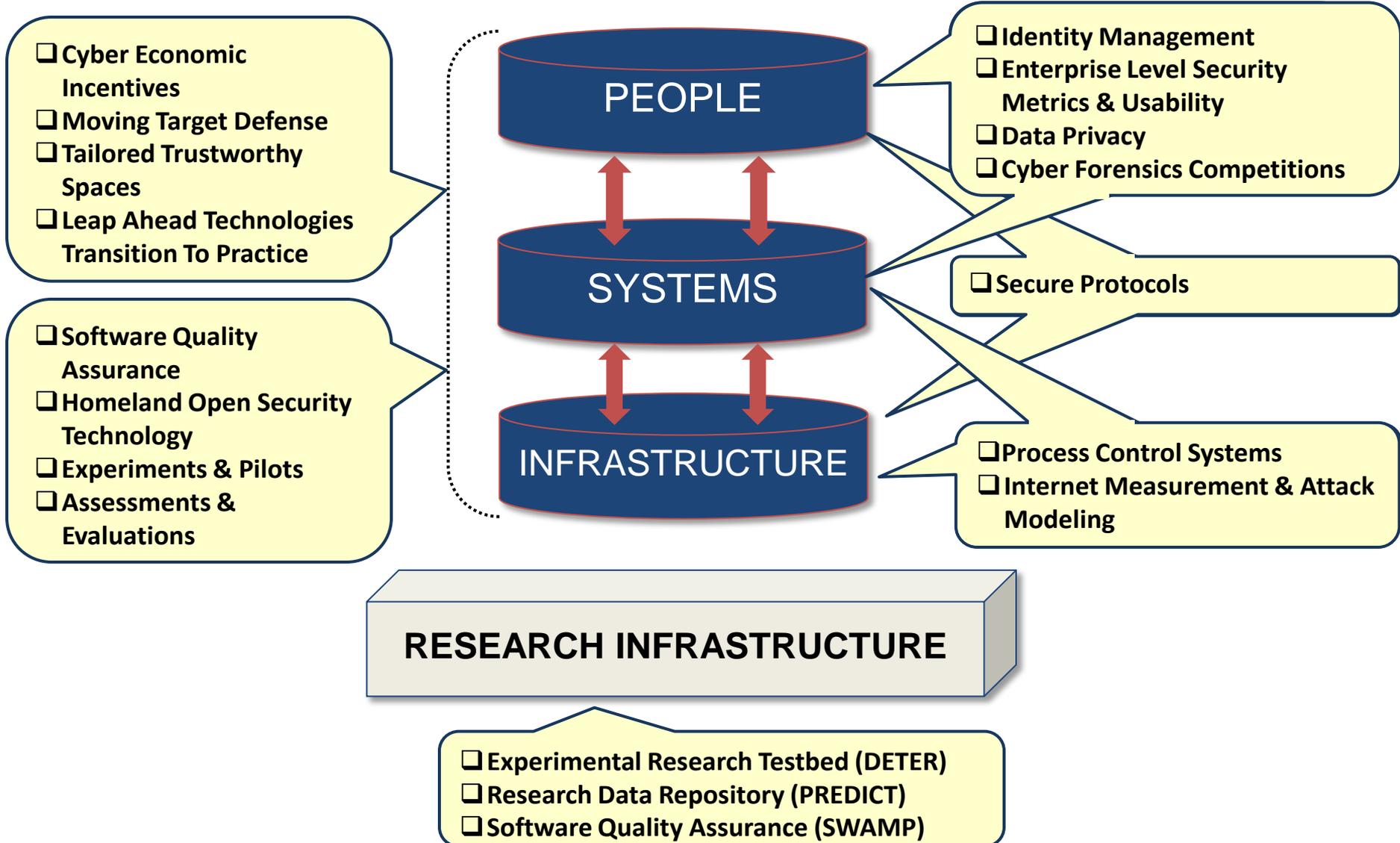
Cyber Security as a Strategic Issue ...

- ❑ National INFOSEC Research Council published “Hard Problem” research agenda in 1999 and 2005
- ❑ In Jan 2008 NSPD 54 / HSPD 23 formalized the Comprehensive National Cybersecurity Initiative (CNCI) ... 3 focus areas, 12 elements
- ❑ In November 2009, DHS published an interagency “Roadmap for Cybersecurity Research,” bringing together CNCI R&D direction with a revised Hard Problem agenda
- ❑ DHS co-chaired the National Science & Technology Council development of a Strategic Plan for the Federal Cybersecurity R&D Program (published December 2011)

Comprehensive National Cybersecurity Initiative (CNCI)



Building a Balanced Portfolio: DHS S&T Cybersecurity Program



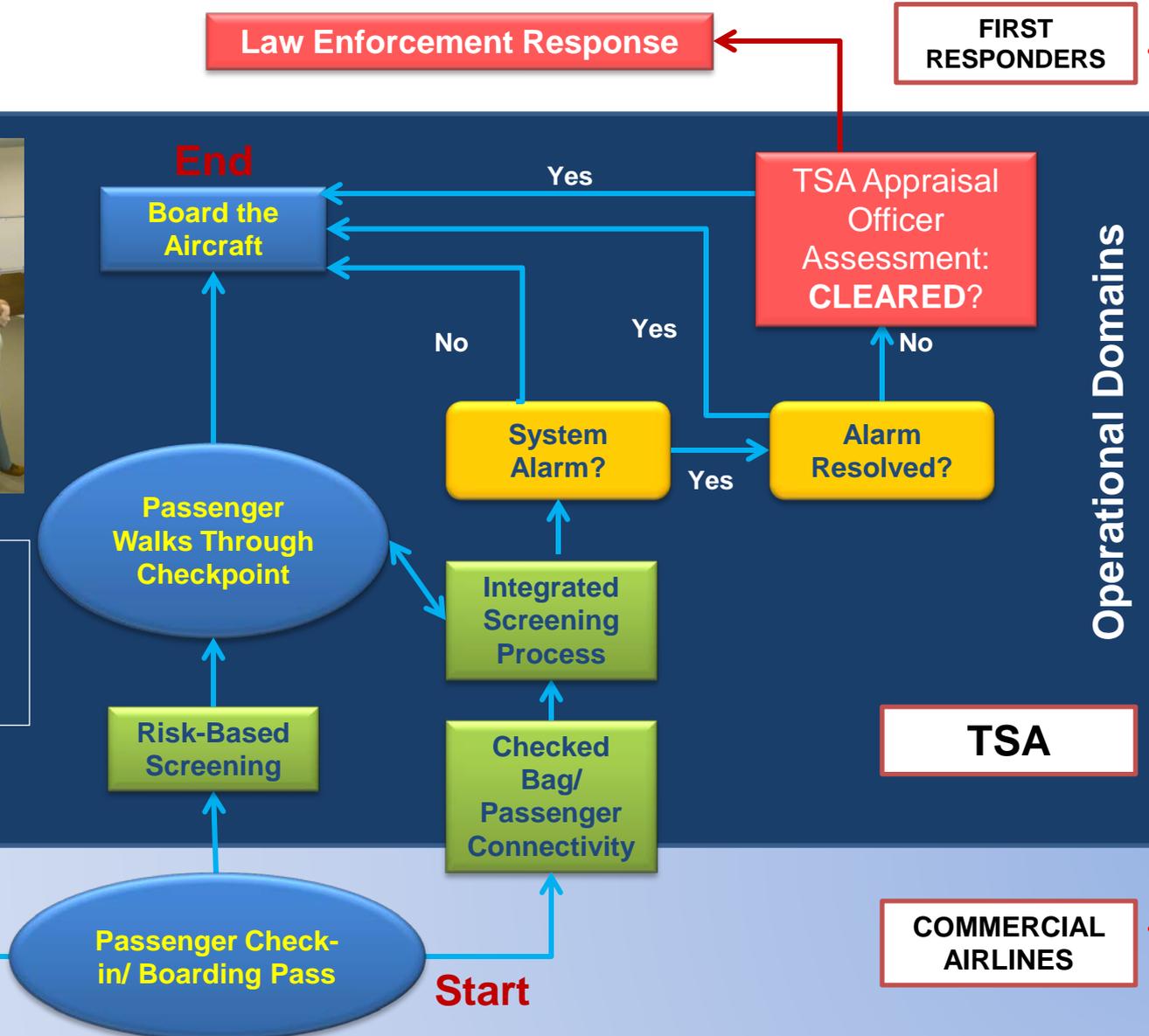
Developing a Systems Approach to S&T (Integrated Checkpoint Operations)



Integrated Checkpoint

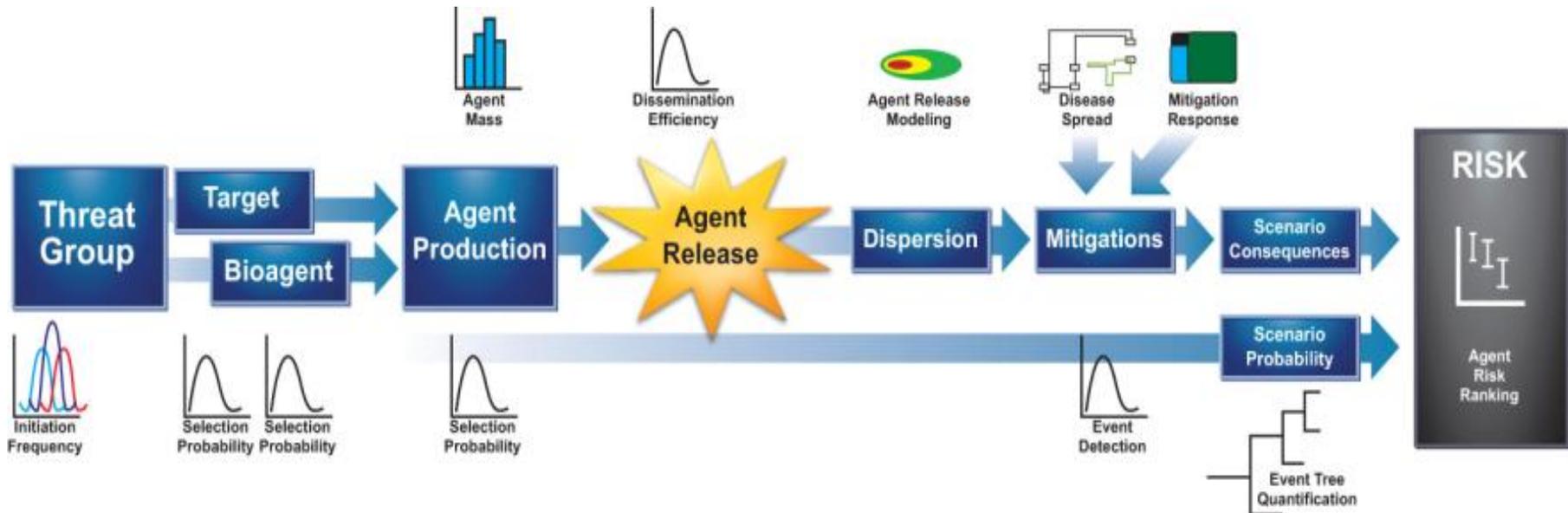
- Reduced FTE required
- Increased Security
- Improved Passenger Experience

ID Check
No Fly List



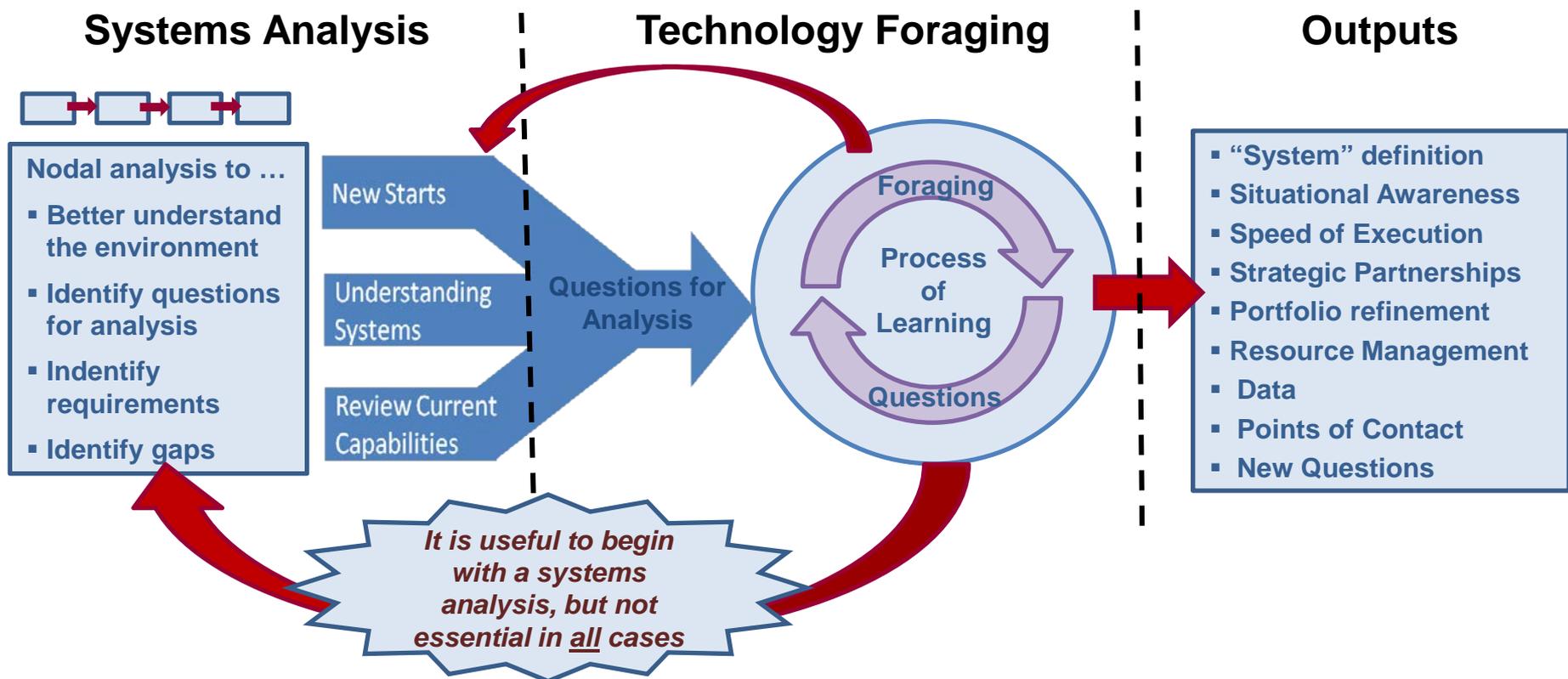
Developing a Systems Approach to S&T (Bioterror)

- ❑ The system of developing a bioterror attack can be decomposed into component parts
 - A successful attack only results from accomplishing each step successfully
 - Each step has a discrete probability of success
- ❑ This methodology has been incorporated into the Bioterrorism Risk Assessment (BTRA) which assists in developing priorities



This same methodology applies to other DHS S&T applications ...

Technology Foraging & Building Partnerships

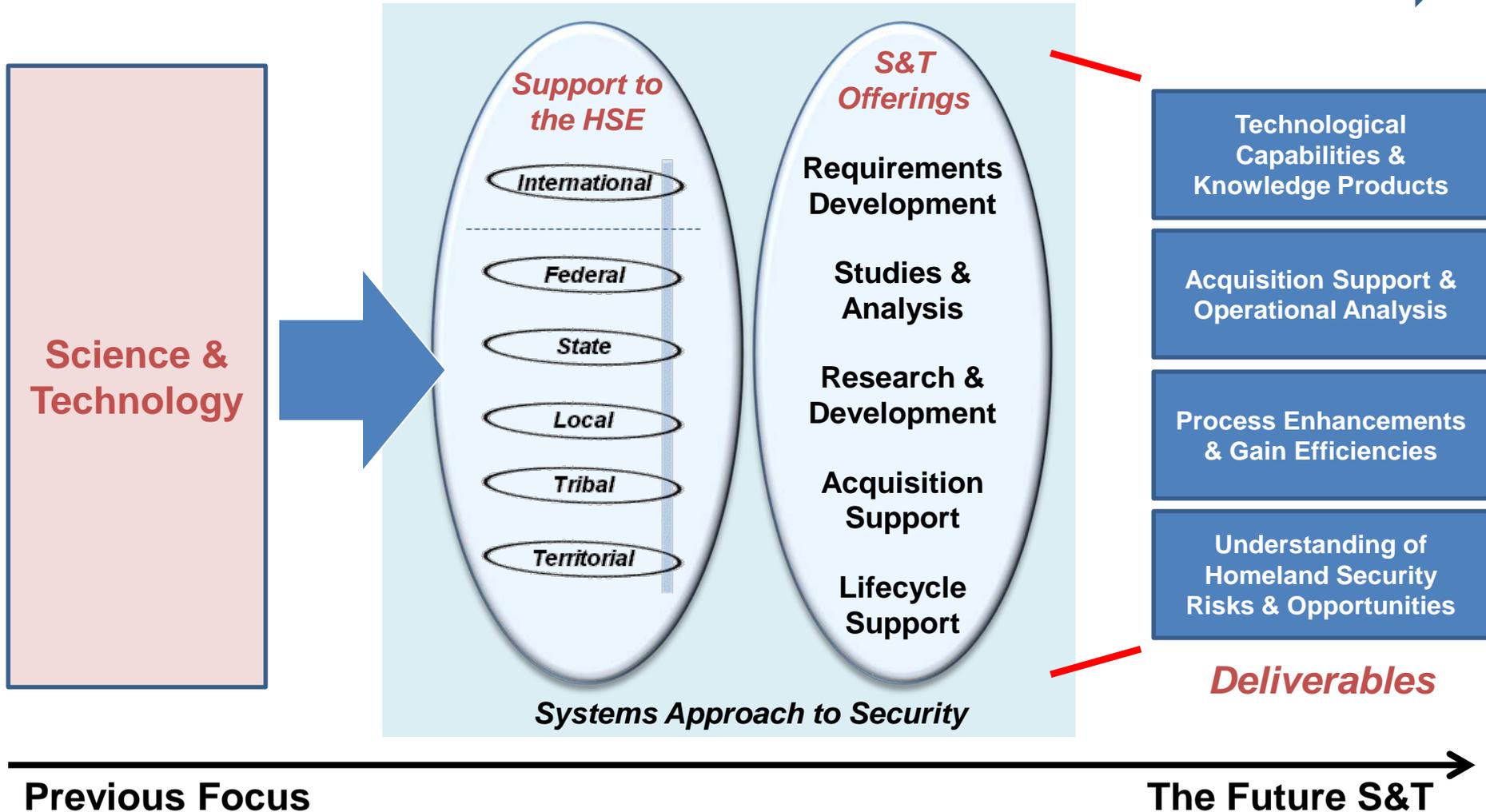


Examples

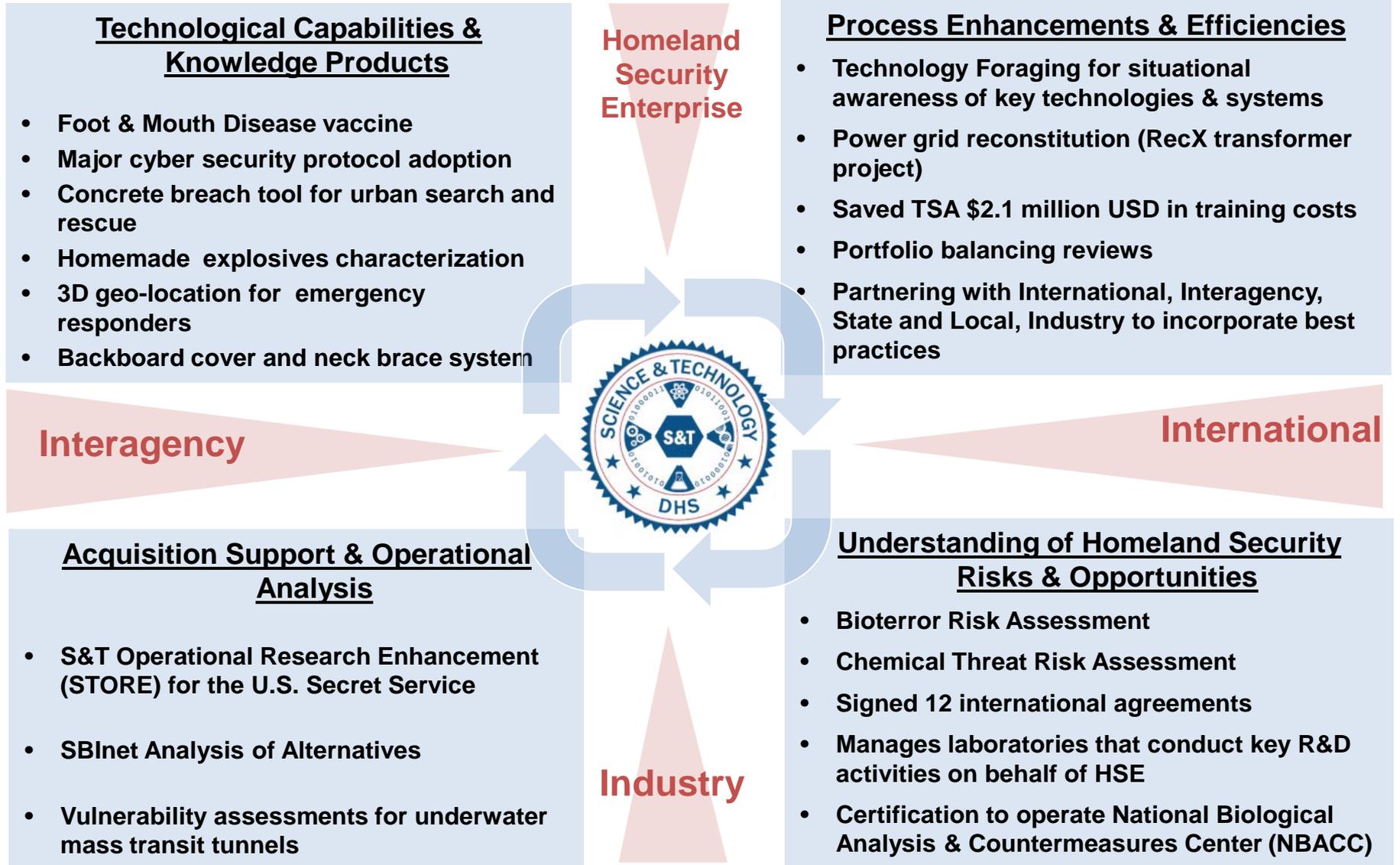
- | | |
|---|--|
| <ul style="list-style-type: none"> ❑ Automated Pollen Recognition ❑ Seized Information Exploitation ❑ Stand-off Detection of Trapped Victims | <ul style="list-style-type: none"> ❑ Rapid Bio-Diagnostics ❑ Next-Gen Textiles for PPE ❑ Virtual Gaming to Aid First Responder Training |
|---|--|

Support to the Homeland Security Enterprise (HSE)

New Approach to Delivering Operationally Relevant Support



DHS S&T In Review



Department of Homeland Security Science & Technology

Presentation to the U.S. Army Armament
Research, Development, & Engineering Center

Dr. Daniel Carstein
Deputy Under Secretary for Science & Technology

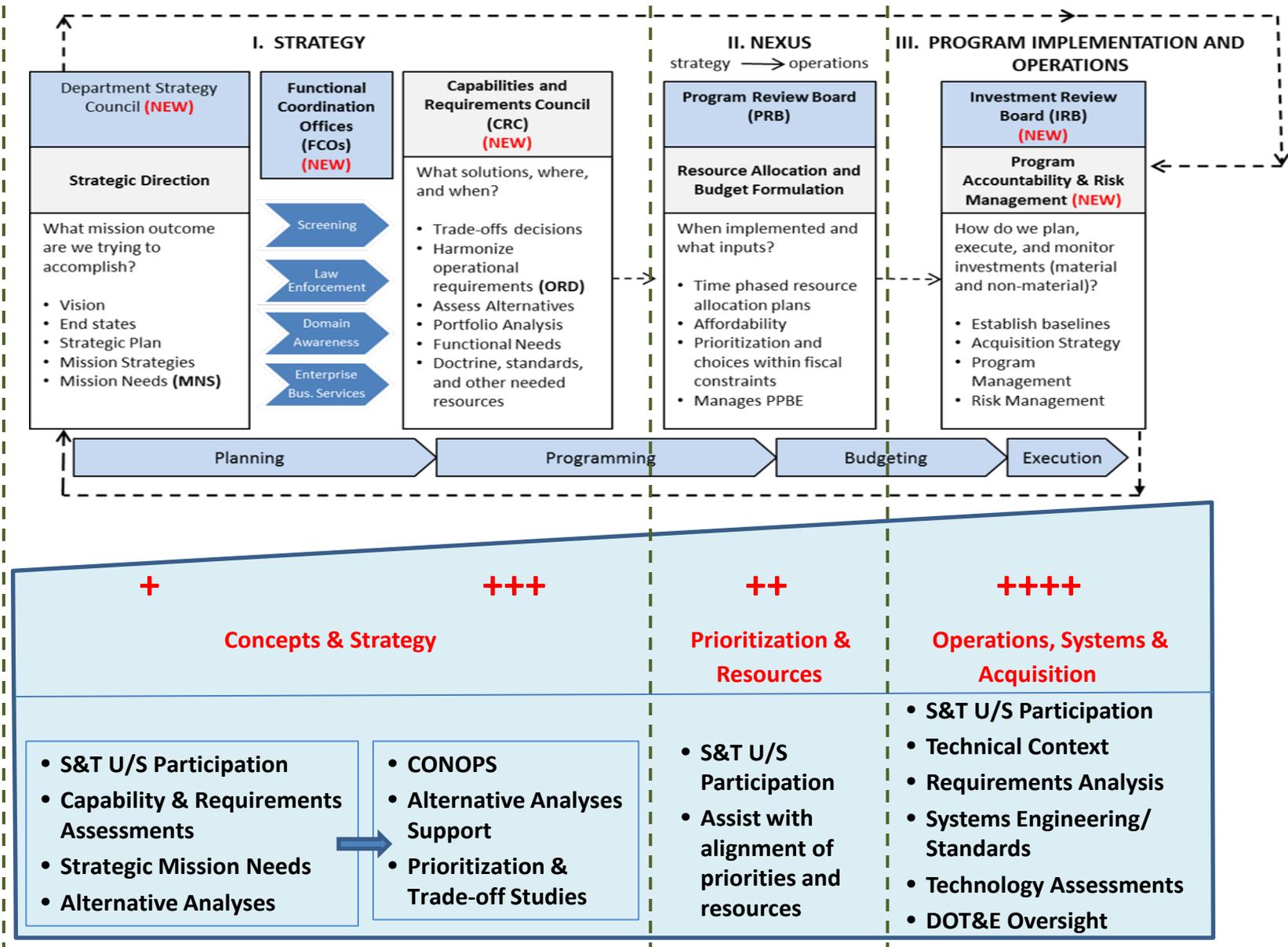
March 7, 2012

BACK UP



Homeland
Security

Proposed Integrated Investment Lifecycle Model (IILCM) S&T Role



How to Reach DHS

Type I (New Technologies)

- ✓ Applied Research Phase
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ \$3M & 36 mos.

Type II (Prototype Technologies)

- ✓ More Mature Prototypes
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ \$2M & 24 mos.

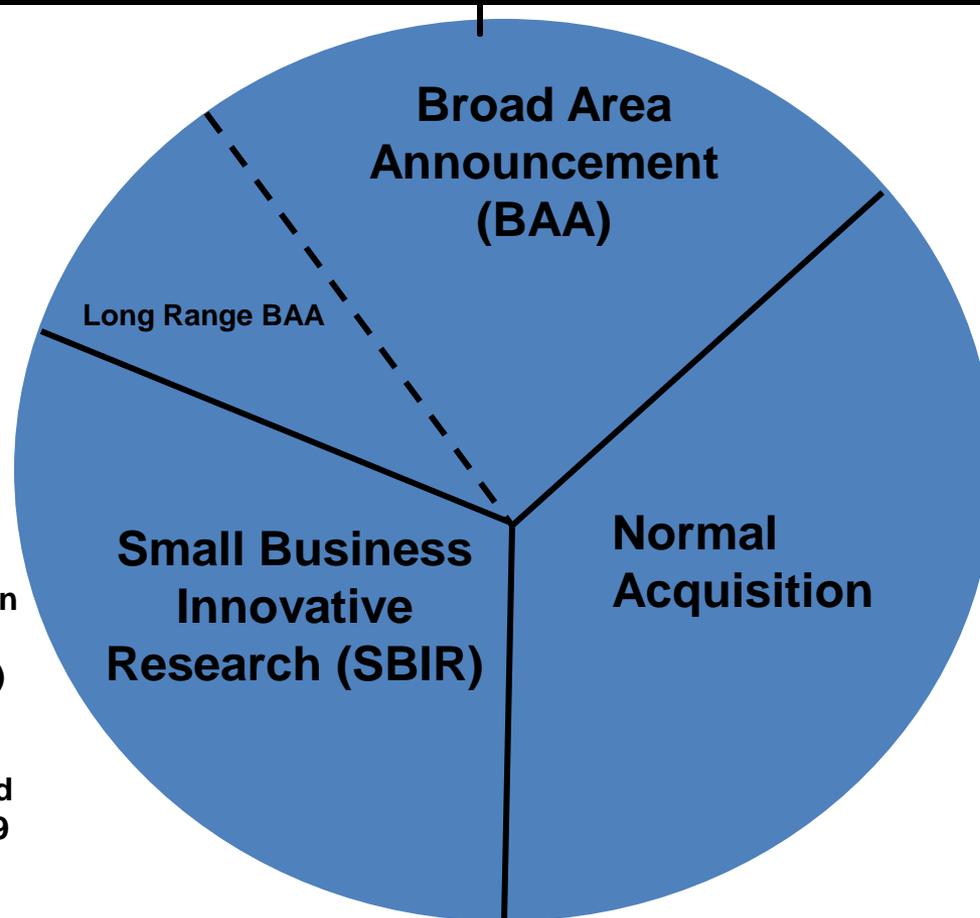
Type III (Mature Technologies)

- ✓ Mature Technology
- ✓ Demo Only in Op Environ.
- ✓ Funding ≤ \$750K & 12 mos.

SBIR

Since 2004, DHS S&T Cyber Security has had:

- 60 Phase I efforts
- 27 Phase II efforts
- 4 Phase II efforts currently in progress
- 9 commercial/open source products available
- Three acquisitions
 - Komoku, Inc. (MD) acquired by Microsoft in March 2008
 - Endeavor Systems (VA) acquired by McAfee in January 2009
 - Solidcore (CA) acquired by McAfee in June 2009



18 Critical Infrastructure Sectors



Agriculture & Food



Banking & Finance



Chemical Sector



Comms Sector



Commercial Facilities



Critical Manufacturing



Dams



Information Technology



Energy



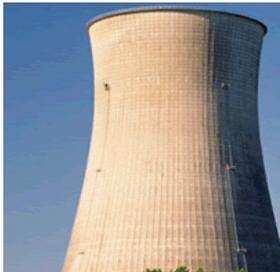
Government Facilities



Healthcare and Public Health



Water



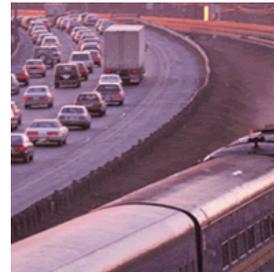
Nuclear Reactors, Materials and Waste



Postal and Shipping



Defense Industrial Base



Transportation Systems



National Monuments Icons



Emergency Services

Infrastructure Sectors



Agriculture & Food



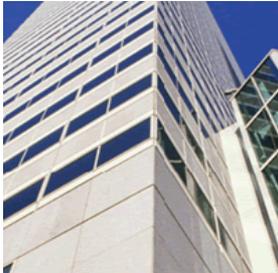
Banking & Finance



Chemical Sector



Comms Sector



Commercial Facilities



Critical Manufacturing



Dams



Information Technology



Energy



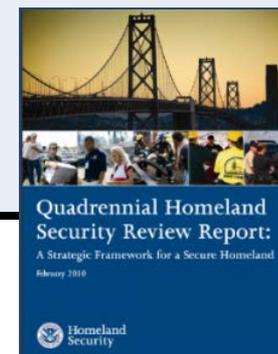
Building a Balanced Portfolio (Example: Bioterror)

PPD-8 Mission Area Bioterror Steps	<u>Preventing</u> , avoiding, or stopping a threatened or an actual act of terrorism	<u>Protecting</u> our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive	<u>Mitigating</u> the loss of life and property by lessening the impact of future disasters	<u>Responding</u> quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic event	<u>Recovering</u> through a focus on the timely restoration, strengthening, and revitalization of infrastructure; housing; sustainable economy; and health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic disaster
Acquire					
Process					
Weaponize					
Scenario Development					
Deployment					

- What capabilities are already fielded in each area?*
- Where are the capabilities gaps?*
- Who else is working in this mission space?*
- Where should S&T invest?*
- Others?*

Quadrennial Homeland Security Review (QHSR)

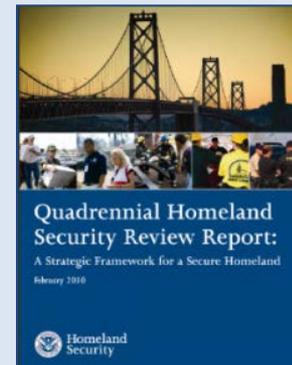
Threats & Hazards	Global Challenges & Trends
<ul style="list-style-type: none"> <input type="checkbox"/> High-consequence weapons of mass destruction <input type="checkbox"/> Al-Qaeda and global violent extremism <input type="checkbox"/> High-consequence and/or wide-scale cyber attacks, intrusions, disruptions, and exploitations <input type="checkbox"/> Pandemics, major accidents, and natural hazards <input type="checkbox"/> Illicit trafficking and related transnational crime <input type="checkbox"/> Smaller scale terrorism 	<ul style="list-style-type: none"> <input type="checkbox"/> Economic and financial instability <input type="checkbox"/> Dependence on fossil fuels and the threats of global climate change <input type="checkbox"/> Nations unwilling to abide by international norms <input type="checkbox"/> Sophisticated and broadly available technology <input type="checkbox"/> Other drivers of illicit, dangerous, or uncontrolled movement of people and goods



Quadrennial Homeland Security Review (QHSR)

The Core Missions

1. Preventing terrorism and enhancing security;
2. Securing and managing our borders;
3. Enforcing and administering our immigration laws;
4. Safeguarding and securing cyberspace; and
5. Ensuring resilience to disasters



Mission 6: Maturing and Strengthening the Homeland Security Enterprise

Foster Innovative Solutions Through Science and Technology

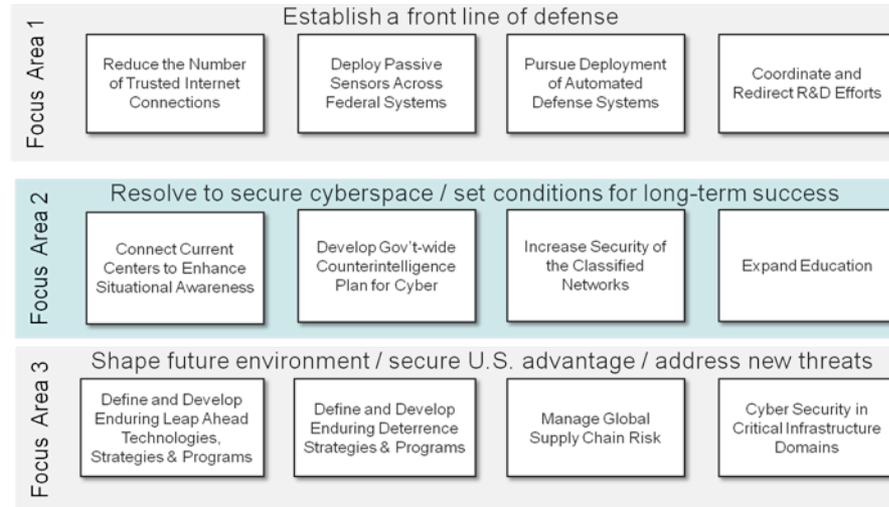
- Ensure scientifically informed analyses and decisions are coupled to effective technological solutions
- Conduct scientific assessments of threats and vulnerabilities
- Foster collaborative efforts involving government, academia, and the private sector to create innovative approaches to key homeland security challenges



- Preserve investments in uniquely S&T arenas**
 - **Biodefense; explosives detection in aviation; cybersecurity for .gov and .com; first responder support**
- Emphasize near-term development, transition to use**
 - **Tech foraging; fund fewer projects but fund for success**
- Leverage others' investments**
 - **Tech foraging; IQT; collaboration with interagency and internationally; tech clearinghouse**
- Clear understanding of problem to be solved and emphasis on systems solutions**
- Strong emphasis on partnerships with customers**

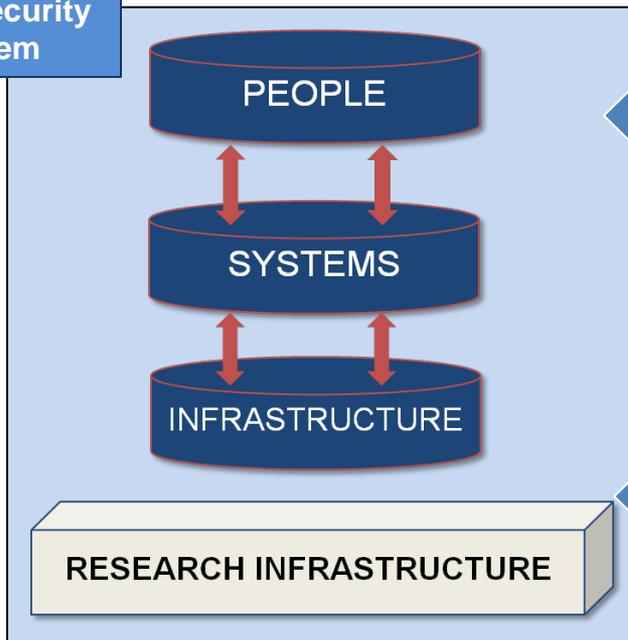
A Systems Approach: Strategy to Action

Comprehensive National Cybersecurity Initiative (CNCI)



<http://cybersecurity.whitehouse.gov>

Cybersecurity System



Technical Areas (BAA)

- TTA-1 Software Assurance**
- TTA-2 Enterprise-level Security Metrics**
- TTA-3 Usable Security**
- TTA-4 Insider Threat**
- TTA-5 Resilient Systems and Networks**
- TTA-6 Modeling of Internet Attacks**
- TTA-7 Network Mapping and Measurement**
- TTA-8 Incident Response Communities**
- TTA-9 Cyber Economics**
- TTA-10 Digital Provenance**
- TTA-11 Hardware-enabled Trust**
- TTA-12 Moving Target Defense**
- TTA-13 Nature-inspired Cyber Health**
- TTA-14 Software Assurance MarketPlace**

Cyber Security Program Areas

- Research Infrastructure to Support Cybersecurity (RISC)**
- Trustworthy Cyber Infrastructure (TCI)**
- Cyber Technology Evaluation and Transition (CTET)**
- Foundational Elements of Cyber Systems (FECS)**
- Cybersecurity User Protection and Education (CUPE)**

Research Infrastructure (RISC)

- ❑ **Experimental Research Testbed (DETER)**
 - Researcher and vendor-neutral experimental infrastructure
 - DETER - <http://www.isi.edu/deter/>

- ❑ **Research Data Repository (PREDICT)**
 - Repository of network data for use by the U.S.- based cyber security research community
 - PREDICT – <https://www.predict.org>

- ❑ **Software Quality Assurance (SWAMP)**
 - A software assurance testing and evaluation facility and the associated research infrastructure services

Trustworthy Cyber Infrastructure (TCI)

Secure Protocols

- **DNSSEC – Domain Name System Security**
- **SPRI – Secure Protocols for Routing Infrastructure**

Process Control Systems

- **LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity**
- **TCIPG – Trustworthy Computing Infrastructure for the Power Grid**

Internet Measurement and Attack Modeling

- **Geographic mapping of Internet resources**
- **Logically and/or physically connected maps of Internet resources**
- **Monitoring and archiving of BGP route information**

Evaluation and Transition (CTET)

Assessment and Evaluations

- Red Teaming of DHS S&T-funded technologies

Experiments and Pilots

- Experimental Deployment of DHS S&T-funded technologies into operational environments

Transition to Practice (CNCI)

- New FY12 Initiative

Foundational Elements (FECS)

- Enterprise Level Security Metrics and Usability**
- Homeland Open Security Technology (HOST)**
- Software Quality Assurance**
- Cyber Economic Incentives (CNCI)**
 - **New FY12 Initiative**
- Leap Ahead Technologies (CNCI)**
- Moving Target Defense (CNCI)**
 - **New FY12 Initiative**
- Tailored Trustworthy Spaces (CNCI)**
 - **New FY12 Initiative**

Cybersecurity Users (CUPE)

❑ Cyber Security Competitions

- National Initiative for Cybersecurity Education (NICE)
- NCCDC (Collegiate); U.S. Cyber Challenge (High School)

❑ Cyber Security Forensics

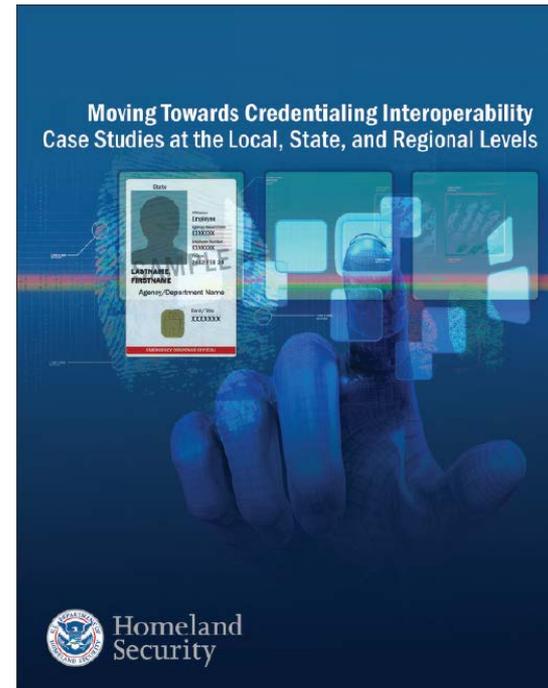
- Support to DHS and other Law Enforcement customers

❑ Identity Management

- National Strategy for Trusted Identities in Cyberspace (NSTIC)

❑ Data Privacy Technologies

- New Start in FY13





HSARPA

Paul Benda
Chief of Staff
Director, HSARPA



HSARPA Focus

▪ Understand the Operational Context

- S&T will conduct a systems analysis to develop better understanding of current missions, systems, and processes
- Identify target operational gaps where S&T can have the most impact
- Facilitate transition plans (Transition = Operational Use + Ownership)

▪ Demonstrate a Return on Investment

- $ROI = f(\text{Efficiency Impact}, \text{Capability Impact}, \text{Transition Cost})$
- Efficiency Impact
 - ✓ Doing current processes faster, with higher throughput, and/or cheaper
- Capability Impact
 - ✓ Enabling a change to current processes by adding techniques or technologies, increasing performance, and/or decreasing risk

HSARPA Technical Divisions



- **Explosives Division** - Detect, prevent and mitigate explosives attacks against people and infrastructure
- **Chemical/Biological Defense Division** - Detect, protect against, respond to, and recover from potential biological or chemical events
- **Cyber Security Division** - Create a safe, secure and resilient cyber environment
- **Borders and Maritime Security Division** - Prevent contraband, criminals and terrorists from entering the U.S. while permitting the lawful flow of commerce and visitors
- **Human Factors/Behavioral Sciences Division** - Identify and analyze threats, enhance societal resilience, and integrate human capabilities in technology development
- **Infrastructure Protection & Disaster Management Division** - Strengthen situational awareness, emergency response capabilities and critical infrastructure protection

Border and Maritime Security



- **Mission:**

Develop, integrate, and evaluate technologies to detect, track, and classify threats crossing air/land/water borders in between Ports of Entry.

- **Research Areas:**

- **Buried tripwires**
- **Mobile surveillance systems**
- **Tunnel detection and monitoring**
- **Air-based sensor technologies**
- **Maritime security of surface and underwater contraband threats**

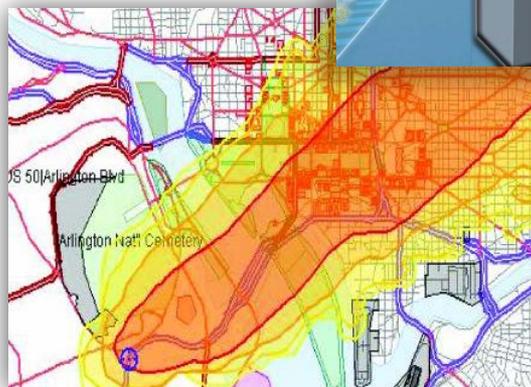
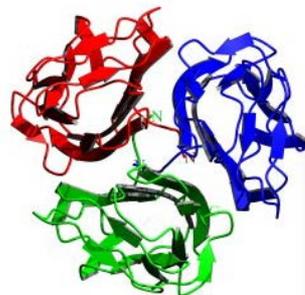
Chemical and Biological Defense

■ Mission:

- Save lives and protect Nation's infrastructure against chemical, biological and agricultural threats and disasters.

■ Research Areas:

- Comprehensive understanding and analyses of chem-bio threats
- Develop pre-event assessment, discovery, and interdiction capabilities
- Develop capability for warning, notification, and timely analysis
- Optimize recovery processes
- Enhance the capability to inform attribution of attacks
- Develop medical countermeasures against foreign animal diseases



Cyber Security

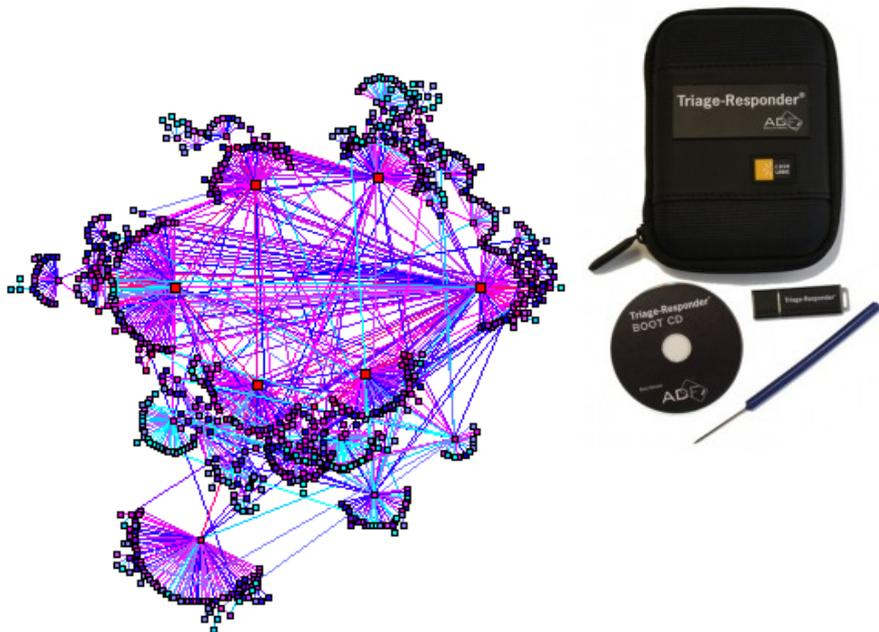


■ Mission:

Secure cyber systems and networks, resilient to cyber threats. Protect users, infrastructure, and the Internet.

■ Research Areas:

- Ensure infrastructure and the Internet are secure and less vulnerable to malicious and natural events
- Develop protocols essential to trustworthy cyber systems
- Provide safe cyber arenas to enable research on discovery, testing, and analysis of tools, technologies and software
- Provide R&D activities for users to attract next generation cyber security warriors, provide tools cyber criminal and terrorist investigations



Explosives

■ Mission:

Develop technical capabilities to detect, respond, defeat, and mitigate non-nuclear explosives terrorism.

■ Research Areas:

- Secure passenger and cargo safety at airports and checkpoints
- Protect national infrastructure and treasures from explosive threats
- Protect people and facilities in high volume, fast-paced environments like trains and subways
- Support TSA, US Secret Service, first responders, Customs and Border Protection



Human Factors and Behavioral Sciences

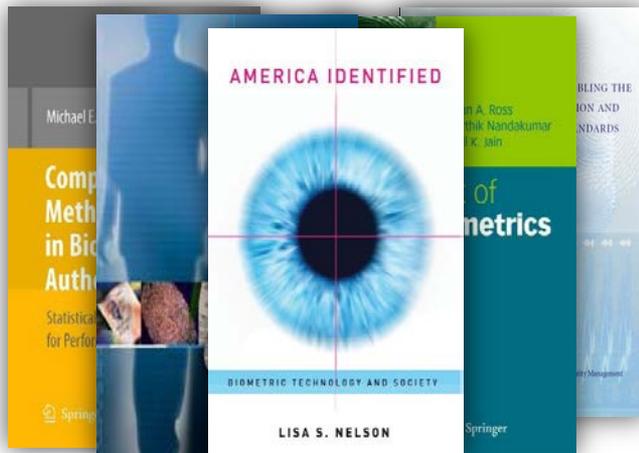


■ Mission:

Develop people-centric technologies, knowledge products, and enhanced human performance to ensure homeland security.

■ Research Areas:

- Target and screen people, land vehicles, and sea containers entering the U.S.
- Biometric Identity management
- Verify identities, assess intent, and authenticate documentation
- Understand operational threats, improve operator performance, improve sensor technologies, perform technology testing and evaluation



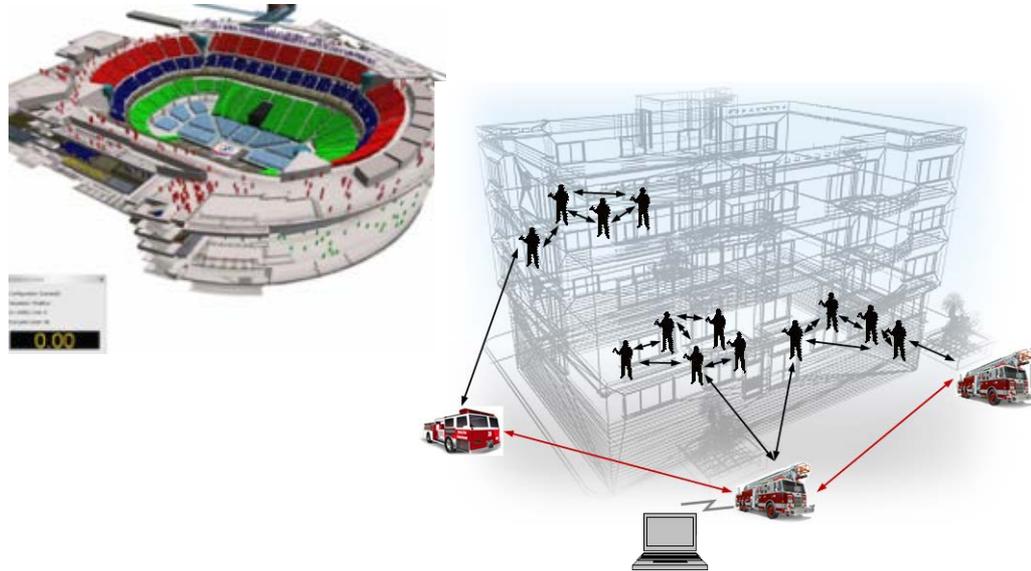
Infrastructure Protection and Disaster Management

■ Mission:

Provide physical and virtual technologies and solutions to protect national infrastructure and manage disaster impact and response.

■ Research Areas:

- Modeling and simulation for evacuation
- Incident management
- Overhead imagery for disaster response
- Location of first responders in GPS challenged environments
- Electric grid resilience
- Levee and tunnel breach mitigation



APEX - STORE

- **USSS and DHS S&T Partnership**
 - **S&T 2 year investment: \$21.5M**
 - **Leveraging \$11.6 additional investment (DoD, IC, and USSS)**
 - **Partnership continues beyond S&T investment period**
- **Shared Objectives:**
 - **Establish a rigorous analysis and acquisition process to fully explain USSS requirements and budget needs**
 - **Implement technology enhancements for the USSS Protective Mission**
 - **Create an annual capability investment cycle to implement future technologies**



APEX – Secure Transit Corridors

■ Objective:

- Demonstrate a rail and truck security device that will monitor unauthorized door openings, anomalies, and events and provide encrypted in-transit tracking for C-TPAT* Tier III, FAST member's supply chain routes originating from Mexico and Canada and ending in the U.S.
- Assist CBP/OFO in integrating a new capability into their existing operational model.

■ Technology Focus:

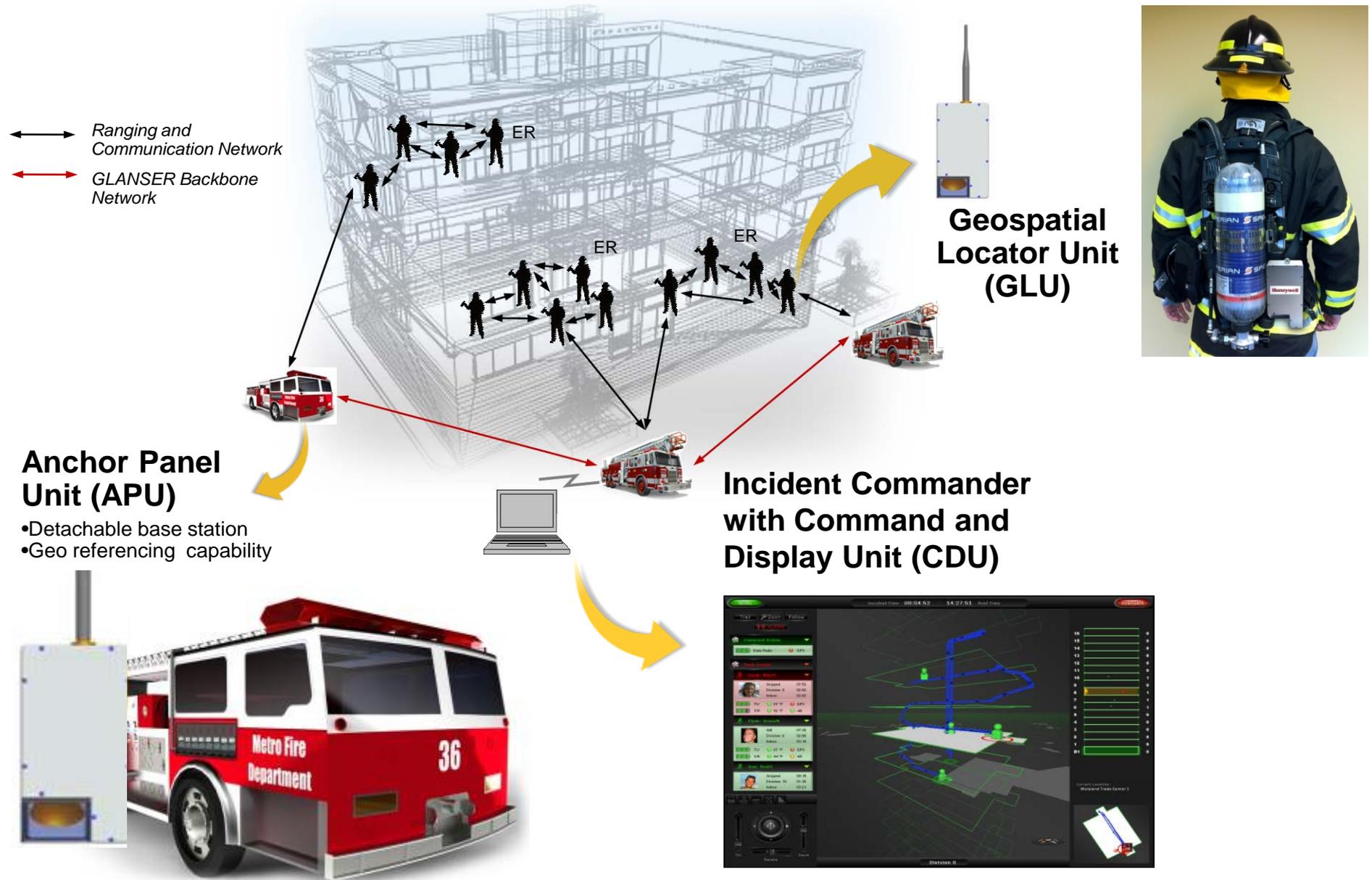
- The Electronic Chain of Custody (ECoC) is a conveyance security device that adds an additional layer of security to truck /rail supply chain routes by providing electronic traceability and accountability of cargo door openings using enroute tracking.

■ Transition Strategy:

- After completion of the Technology Demonstration, the Supply Chain Management System (SCMS) capability will transition to CBP and the technical security device specifications will be delivered to industry to allow for competitive sourcing of security devices.



GLANSER



FY 2013 Budget Summary

- The FY 2013 President's Budget Request for S&T Research, Development, Acquisitions, and Operation (RDA&O) \$693M—returns S&T R&D to the FY 2011 level, which is a 23% decrease in R&D compared to FY 2010.

FY10 - FY13 S&T Budget

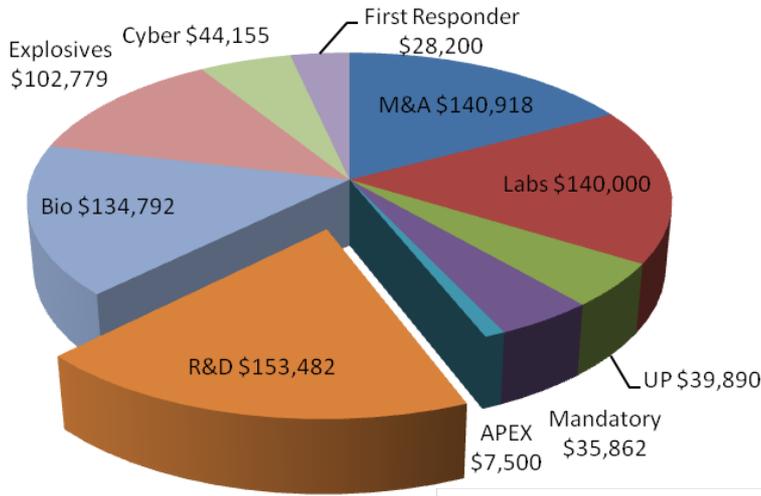
(\$ in thousands)

PPA	Enacted	CR	Enacted	President's Budget
	FY10	FY11	FY12	FY13
Management and Administration	143,200	140,918	135,000	138,008
RDA&O	863,271	686,660	533,000	693,464
Laboratory Facilities	150,188	140,000	176,500	127,432
Acquisition and Operations Support	65,260	47,034	54,154	47,984
University Programs	49,350	39,999	36,563	40,000
Research Development and Innovation	598,473	459,627	265,783	478,048
Total including M&A	1,006,471	827,578	668,000	831,472

S&T Budget

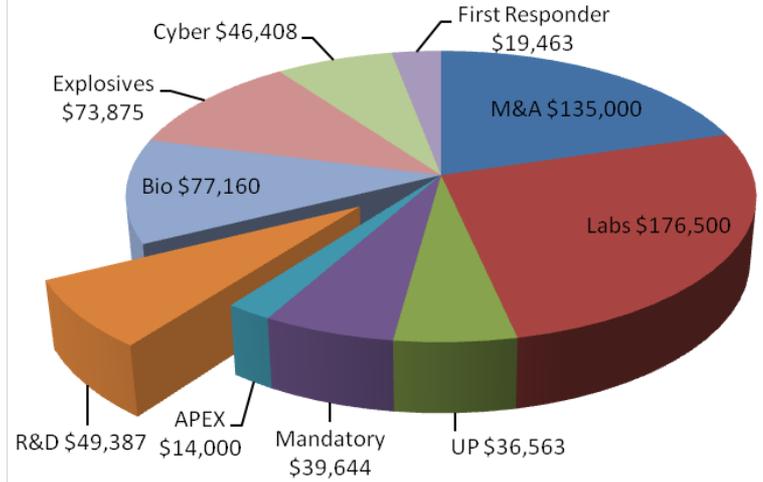
FY 2011 Funding

\$ in Thousands



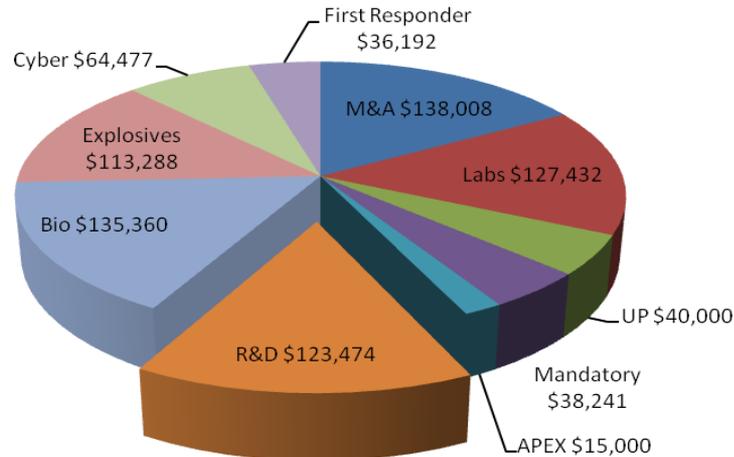
FY 2012 Funding

\$ in Thousands



FY 2013 Funding

\$ in Thousands





**"My science was all wrong. And, like a fool,
I said, 'So sue me.' "**