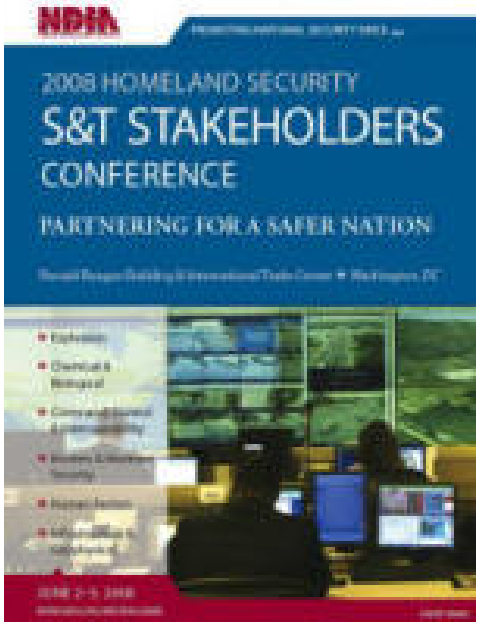
Partnering for a Safer Nation

2008 Homeland Security S&T Stakeholders Conference

Kevin "Spanky" Kirsch
Science and Technology Directorate
Department of Homeland Security
Director, Office of Special Programs

June 2, 2008



Homeland Security

Definition of Homeland Security

"Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."

The National Strategy for Homeland Security

July 2002

Homeland Security

Components of Technology Integration

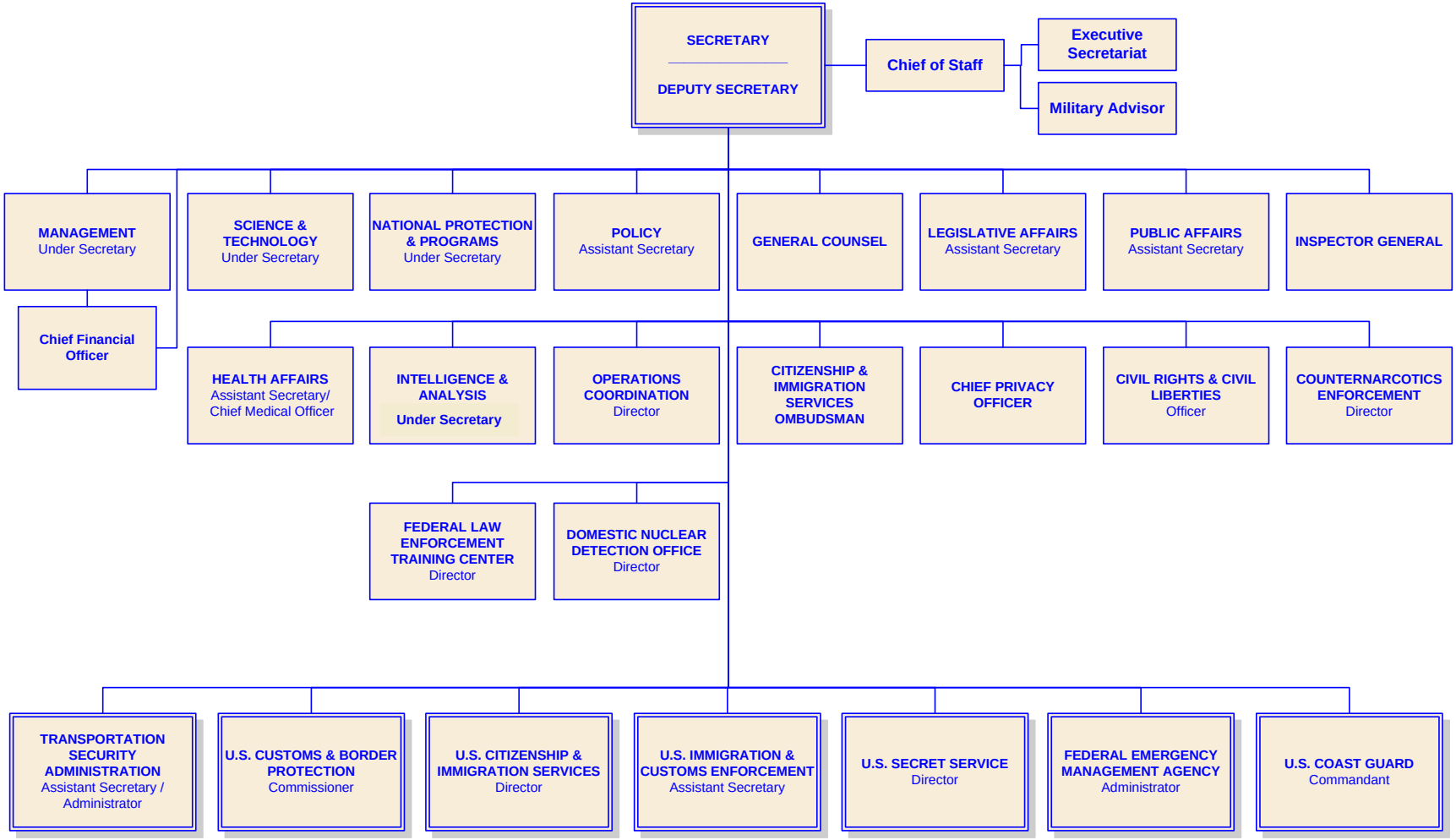
Five major components of effective integration of technology:

- Equipment/Infrastructure
- Socialization
- Regulatory/Legal, Political, Doctrinal, Ethical, Cultural
- Training
- Funding

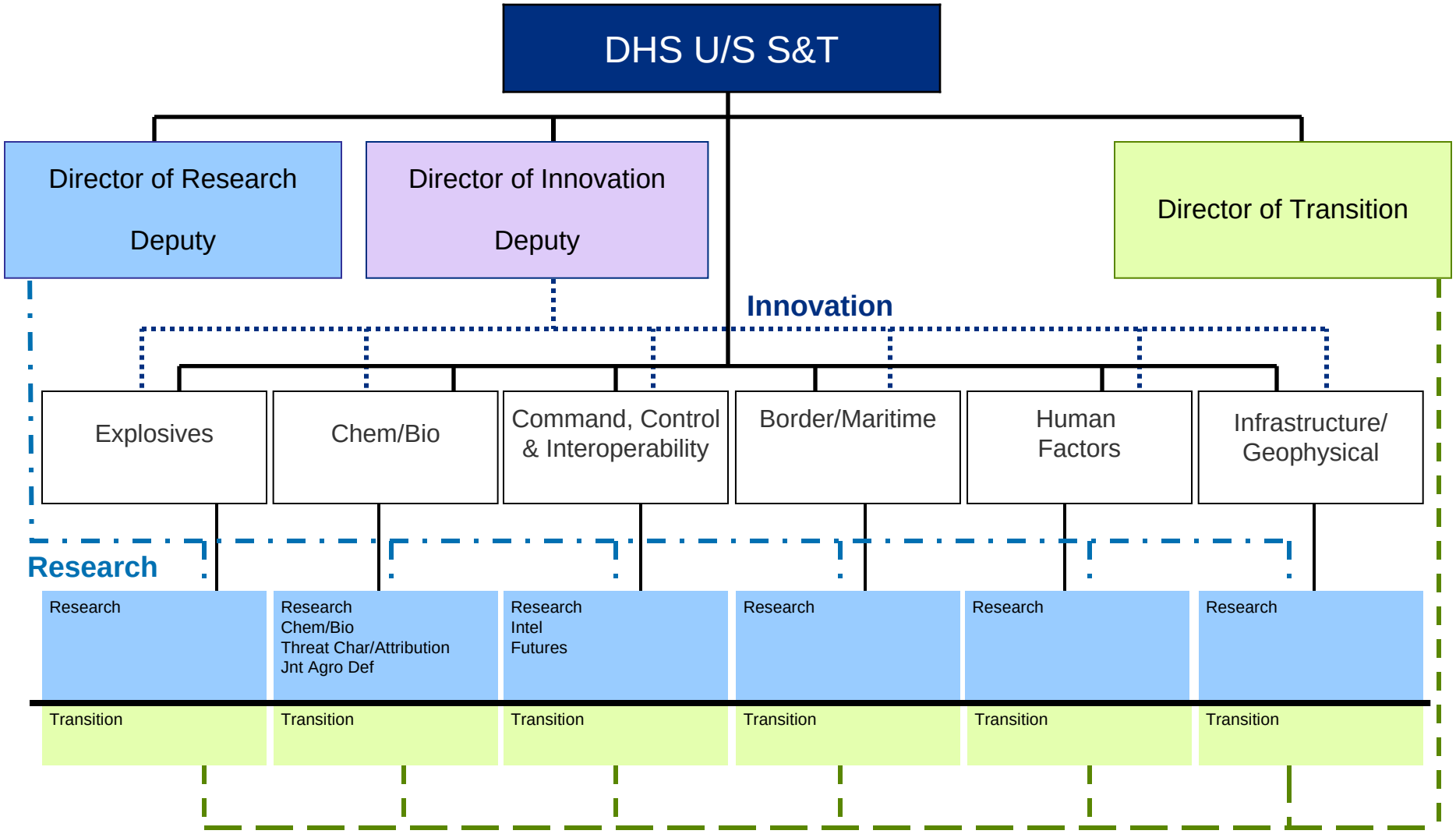
The common, accepted definition of technology usually embraces only equipment and infrastructure.

Homeland Security

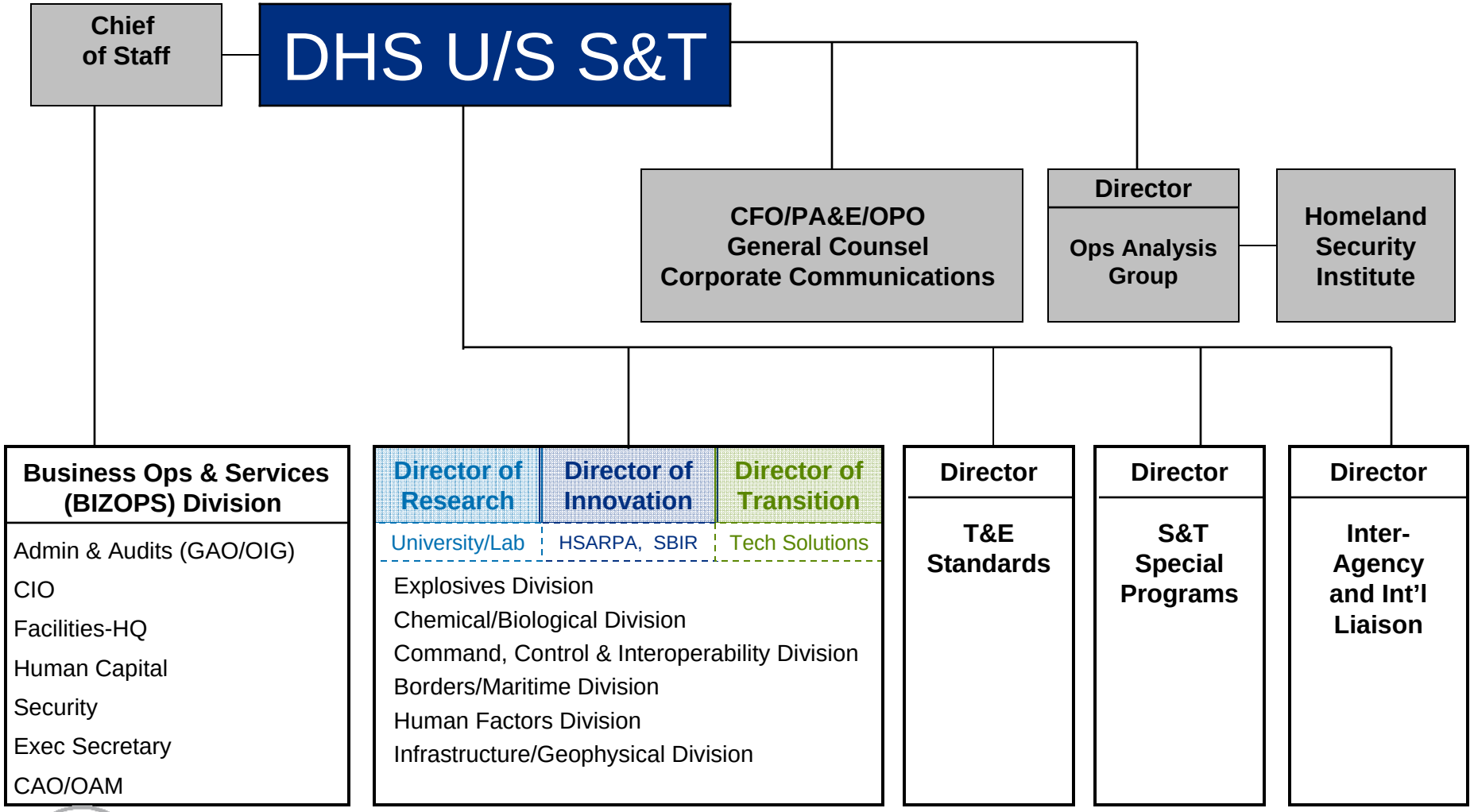
U.S. DEPARTMENT OF HOMELAND SECURITY



S&T Organization



DHS S&T Directorate



Homeland Security

DHS S&T Directorate:
S&T Mission and Objectives

Mission: To Protect the homeland by providing Federal and local officials with state-of-the-art technology and other resources

The directorate fulfills its mission through strategic objectives to:

- Develop and deploy state-of-the-art, high-performance, low-operating-cost systems to prevent, detect, and mitigate the consequences of chemical, biological, radiological, nuclear, and explosive attacks
- Develop equipment, protocols, and training procedures for response to and recovery from chemical, biological, radiological, nuclear, and explosive attacks;
- Enhance technical capabilities of the Department's operational elements and other Federal, State, local, and tribal agencies to fulfill their homeland security related missions
- Develop methods and capabilities to test and assess threats and vulnerabilities, and prevent technology surprise and anticipate emerging threats
- Develop technical standards and establish certified laboratories to evaluate homeland security and emerging responder technologies, and evaluate technologies for SAFETY Act certification
- Support U.S. leadership in science and technology

Homeland Security

Special Programs Division (SPD)

Special Programs Division Overview

Mission:

- To provide components of Department of Homeland Security, the Intelligence Community and other government agencies programmatic and technical expertise in Emerging Threats, Risk Sciences, Intelligence Surveillance, and Reconnaissance, and other areas applicable to Homeland Security that may be especially sensitive, classified, or deserving of extraordinary security protection.

Key Deliverables:

- Integrated S&T risk assessments
- Technological support to the ISR program
- Continue developing countermeasures identified as capability gaps
- Integrated Emerging Threat/Technologies/Tactic assessments
- Collaboration with the Intelligence Community

Homeland Security

Special Programs Division

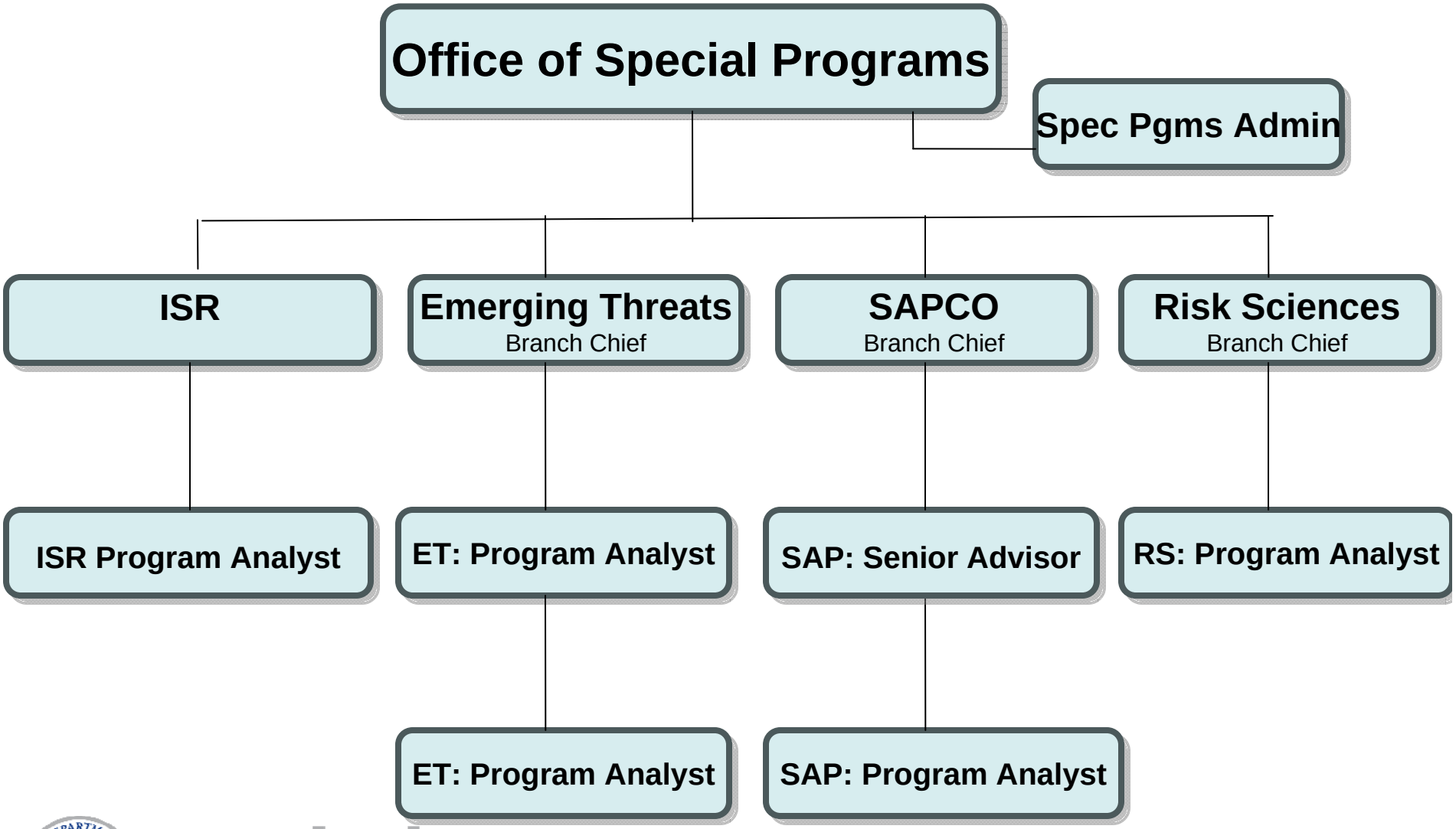
SPD is comprised of four branches that have unique objectives in fulfilling the overall mission of the division.

The four branches are:

- Intelligence, Surveillance, and Reconnaissance
- Emerging Threats
- Risk Sciences
- Special Access Programs

Homeland Security

S&T Office of Special Programs



Homeland Security

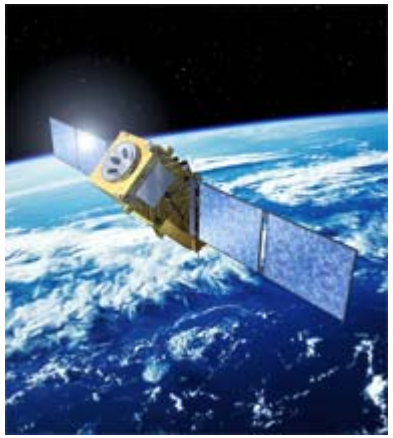
Special Programs Division

Requirements:

The Office of Special Programs (SPD) receive their requirements through three different methods:

- Via IPT sessions
- During the normal budget cycle, use current trends and previous assessments to plan for current and near-term fiscal projects
- A customer with intelligence that indicates that there is an emerging threat that was not planned for during the normal budgetary cycle

Homeland Security



Intelligence, Surveillance, and Reconnaissance

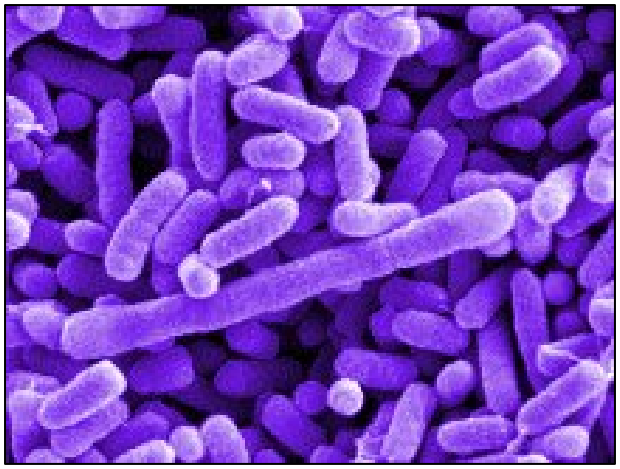
Homeland Security

Intelligence, Surveillance, and Reconnaissance

Objective:

The objective of the Intelligence Surveillance and Reconnaissance Branch is to support basic research activities to improve the collection and dissemination of intelligence information through the use of satellites, radars, sensors, and unmanned platforms in support of DHS components and other relevant federal and DoD agencies.

The Intelligence Surveillance and Reconnaissance Branch will establish an open working relationship with the Office of Intelligence and Analysis, ISR Branch. This relationship will develop and recommend implementation of technology solutions toward an integrated DHS ISR Enterprise. It will assess ISR integration efforts being discussed within the other DHS components, levy the S&T ISR projects from other intelligence agencies to fulfill the technological gaps identified within the OI&A ISR Branch, and will provide S&T support to the National Applications Office in addressing identified technological capability gaps with respect to “disadvantaged” customers.



???

Emerging Threats

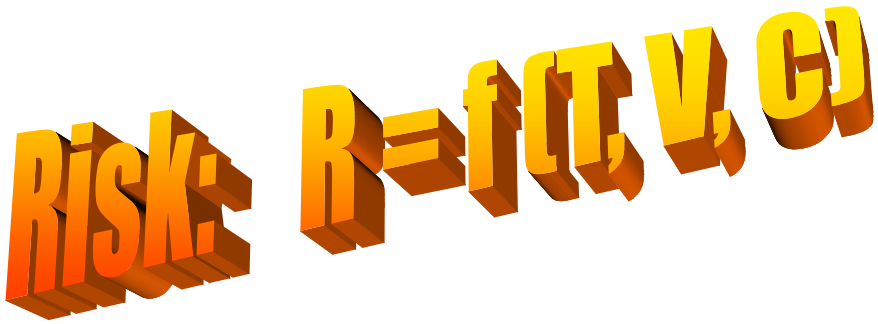
Homeland Security

Emerging Threats

Objective:

The objective of the Emerging Threats (ET) Branch is to address emerging technologies that will present a homeland security threat in the 5 to 20 year timeframe. The ET Branch use studies on emerging technologies to identify possible threats or concerns. The ET Branch also funds development of countermeasure technologies to mitigate emerging threats to the homeland.

The Emerging Threats Branch is also responsible in fostering a cooperative atmosphere between DHS S&T and the S&T Intelligence Community (IC) and identifying collaborative efforts between the S&T IC and DHS S&T.



Risk Sciences

- Risk: R = *f* (P, C)
- Probability: P = *f* (T, V)
- Threat: T – a function of ***other*** ***(****terrorism****)***
  - Intent
  - Capability
    - Nature of Attack
- Vulnerability: V – a function of ***self***
  - Factors such as
    - Target Hardness
      - Nature of Attack
    - Single Point Failures
    - Redundancy and Reconstitution Capability
- Consequence: C = *f* (T, V, other factors)

Homeland Security

Risk Sciences

Objective:

The objective of the Risk Sciences Branch is to foster more systematic, transparent, and goal-focused application of risk concepts and tools to provide better support to strategic, operational and tactical decision-makers across the national homeland security enterprise.

In addition to its efforts related to "Risk" in a more narrow sense, the Risk Sciences Branch will continue to use the Comparative Studies program model which was already in progress when the Risk Sciences Branch was created. The Comparative Studies model examines the competition between terrorists and security forces as an ongoing competition between intelligent, strategically-driven and adaptive adversaries in which each move by one side is met with counter-moves by the other. This longer range strategic view focuses on "next threat" and "threat after next" – i.e., "over the horizon" or "future risk" – as well as potential threats that might arise in the Department's peripheral blind spots. This also entails directing a "future think" effort on behalf of the Policy Directorate/Office of Strategic Planning to improve DHS's capabilities in innovative and longer-range strategic thinking.

Special Access Program Control Office (SAPCO)

Homeland Security

SAPCO

Objective:

The Special Access Program Branch is matrixed from the DHS Headquarters Office of Security (DHS/OS) to ensure appropriate execution of all security program requirements for S&T Special Access Program (SAP) initiatives. The objective of the SAP Branch is to provide direction, management and security administration of the Special Access Program Control Office (SAPCO) for the S&T organization. The SAPCO, under DHS/OS authority, provides security policy, guidance, and oversight for those Special Access Programs under the cognizance of the Under Secretary for Science and Technology. This office is the single point of contact for SAP requirements and the conduit for coordination between S&T and other Executive Branch Departments/Agencies requesting S&T support or participation in Special Access Programs.

Thrust Area Descriptions

Identification and Assessment:

This program area focuses on anticipating and defining potential threats arising from new scientific and technological advances, and evaluating terrorist use of existing capabilities in new or unexpected manners.

Countermeasure Development:

This program area focuses on developing capabilities to counter emergent threats for which countermeasures capabilities do not yet exist. It addresses mission support technology development, mitigation of vulnerabilities, and defense against new and emergent threats.

Future Capabilities Research and Development:

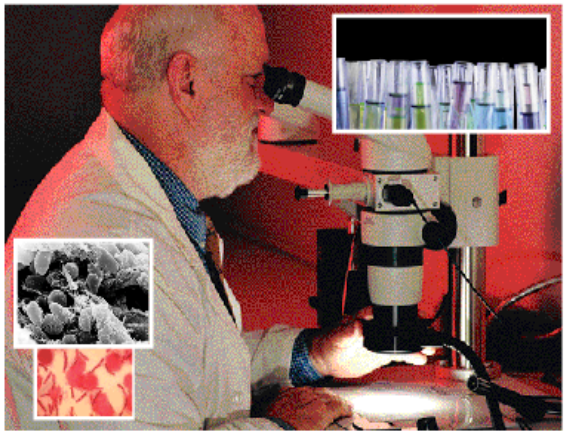
This program area focuses on conducting high-risk, high-payoff basic technology research in areas relevant to emerging threats in homeland security. Activities include research collaboration with external agencies and international partners on emerging threats.

Homeland Security

FROM SCIENCE...SECURITY

Explosives

Chemical/Biological

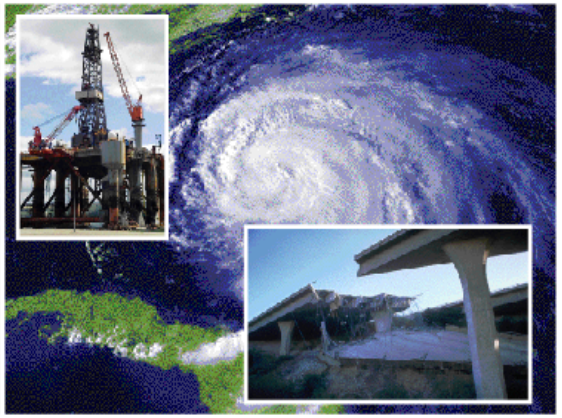


Command, Control and Interoperability

Borders/Maritime

Human Factors

Infrastructure/Geophysical



FROM TECHNOLOGY...TRUST

Contact Information

Kevin “Spanky” Kirsch
202.254.6425 (Office)
202.254.6402 (Fax)
UNCLAS- Spanky.Kirsch@dhs.gov

Homeland Security