Homeland Security

Privacy Office, Mail Stop 0550

November 23, 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009

Re: **DHS/OS/PRIV 07-197/Hofmann request**

Dear Ms. Hofmann:

This is the first partial response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated November 20, 2006, seeking records from January 1, 2004 to the present, concerning the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) program, to include the following:

1. E-mails, letters, reports, memoranda, or other records discussing the use of ADVISE by DHS to mine data or otherwise analyze information about U.S. citizens for permanent residents;

2. All records, including Privacy Act or system of records notices, that discuss or describe DHS' collection, maintenance, or use of personally identifiable information; and

3. Any Privacy Act Impact Assessments (PIAs) performed for the ADVISE program.

Our April 9, 2007 letter to you advised you that our office would coordinate among several DHS components and issue a consolidated response to your request, rather than having each component respond independently. We also notified you that the following DHS components were queried for responsive records: the Office of Intelligence and Analysis (OI&A), the Science and Technology Directorate (S&T), Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE).

Our search of CBP did not product any records responsive to your request.

Our search within ICE produced one record, which is publicly available on the DHS website. You will find a copy of the 2007 Data Mining Report, DHS Privacy Office Response to House Report 109-699, July 6, 2007 at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2007.pdf. Pursuant to 5 U.S.C. §§552(a)(1) and (a)(2), DHS need not make available under the FOIA records that are published elsewhere.

As it relates to our searches within OI&A, S&T and the Privacy Office, due to the volume of records located, our office will provide records to you on a rolling basis, as their review is complete. This response pertains to 115 pages of documents, which were located as a result of our searches of OI&A and S&T. Of those pages, I have determined that 111 pages of the records are releasable in their entirety, 2 pages are partially releasable, and 2 pages are withheld in their entirety pursuant to Title 5 U.S.C. § 552 (b)(2)(low), (b)(2)(high) and (b)(5), FOIA Exemptions 2(low), 2(high) and 5.

Enclosed are 113 pages with certain information withheld, as described below.

FOIA Exemption 2(low) protects information applicable to internal administrative personnel matters to the extent that the information is of a relatively trivial nature and there is no public interest in the document.

FOIA Exemption 2(high) protects information applicable to internal administrative and personnel matters, such as operating rules, guidelines, and manual of procedures of examiners or adjudicators, to the extent that disclosure would risk circumvention of an agency regulation or statute, impede the effectiveness of an agency's activities, or reveal sensitive information that may put the security and safety of an agency activity or employee at risk. Whether there is any public interest in disclosure is legally irrelevant. Rather, the concern under high 2 is that a FOIA disclosure should not benefit those attempting to violate the law and avoid detection.
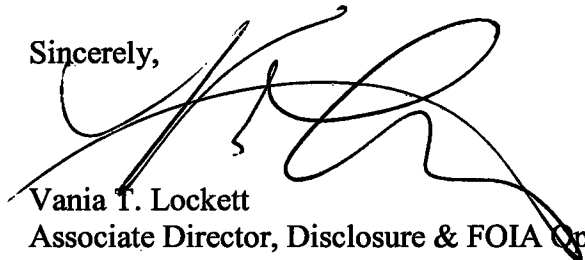
FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. After carefully reviewing the responsive documents, I determined that portions of the responsive documents qualify for protection under the deliberative process privilege. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.

You have a right to appeal the above withholding determination as well as our determination that no records exist within CBP that are responsive to your request. However, we ask that you hold any appeals in abeyance as we continue to process your request. Your agreement to hold any appeals in abeyance pending the issuance of our final response will not preclude your right to appeal. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of our final response, to: Associate General Counsel (General Law), U.S. Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at www.dhs.gov/foia.

Our office continues to process your request. We appreciate your patience as we continue with processing of the remaining documents.

Please note that our mailing address has changed; therefore, you should direct all further written inquiries to: U.S. Department of Homeland Security, Privacy Office, Mail Stop 0550, 245 Murray Lane, S.W., Washington, D.C. 20528-0550. You may also reach us via telephone at 866-431-0486 or 703-235-0778.

Sincerely,

Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: Statement for the Record, Dr. Charles E. McQueary, February 16, 2005
ORD Threat and Vulnerability Testing and Assessment Program Overview
DHS S&T: Actionable Information to Support Intelligence Threat Analysis

ORD Threat and Vulnerability Testing and Assessment (TVTA) Program Overview

Science and Technology Directorate

Office of Research and Development

Sandy Landsberg
TVTA Program Manager

Homeland Security

ORD TVTA Team

- Sandy Landsberg
  - [b2]
  - [b2]
- Dave Shepherd
  - [b2]
  - [b2]
- Karen Walker
  - [b2]
  - [b2]
- Ted Plasse
  - [b2]
  - [b2]

Homeland Security

TVTA Portfolio

Mission Statement

Develop, test, and deliver – in collaboration with intelligence, law enforcement, and homeland security community agencies – tools and methodologies for assessing terrorist threats and understanding terrorism.

Strategic Objectives

- Develop computationally based tools and methodologies for assessing information about and creating, applying, and disseminating knowledge on terrorist threats and activities

- Determine the motives and intents of and identify terrorists by understanding the socio-political, cultural, economic, and behavioral aspects of terrorism and developing reliable biometric indicators

- Assess terrorist capabilities for developing and deploying threat agents

Homeland
Security

TVTA – Developing tools for assessing threats

Portfolio Application
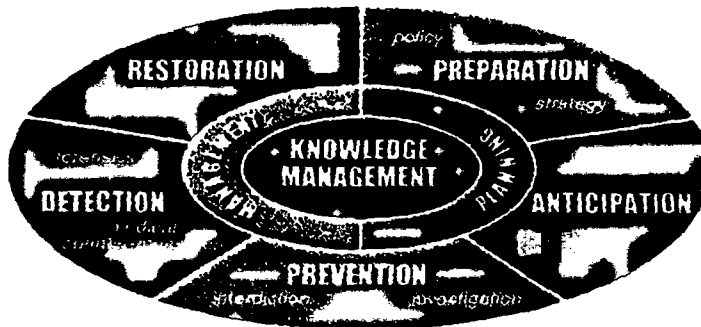
Portfolio Customer Base

- **DHS analysts and operational personnel (IAIP, BTS, EP&R)** – Providing technologies and techniques for threat assessment
- **S&T technical staff** – Informing decisions on science and technology development
- **Intelligence and Law Enforcement Community technical and analytical staff** – Collaborating on tool development and evaluation
- **Government, academic, and commercial research community** – Leading research in specialized areas

Portfolio Span of Interest

Premises:

risk = f (threat, vulnerability, consequence)

threat = f (capability, motive & intent)

Programs Areas:

Knowledge Management Technologies

Capability and Threat Assessment

Motivation and Intent Analysis

Homeland Security

Portfolio Programs

Knowledge Management Technologies
Data Sciences and Data Representation
Visualization and Analytics
Modeling & Simulation and Discrete Sciences
Interagency Test and Evaluation
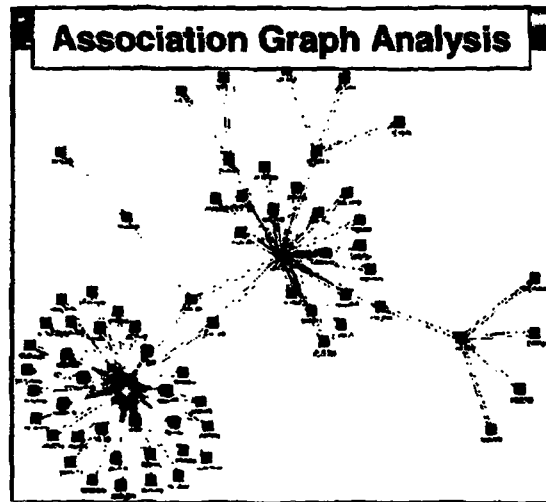**Threat Assessment**
All-WMD Capability Assessment
Nuclear Assessment Program
**Motivation and Intent Analyses**
Socio-political, Cultural, and Behavioral Factors
Biometrics including Deception Detection

ORD TVTA Program Thrust Areas

Association Graph Analysis

- **Knowledge Discovery and Dissemination**

- **Visualization Analytics Centers**

- **Modeling & Simulation and Decision Support**

- **Threat Awareness and Characterization**

- **Motivation and Intent (new start)**
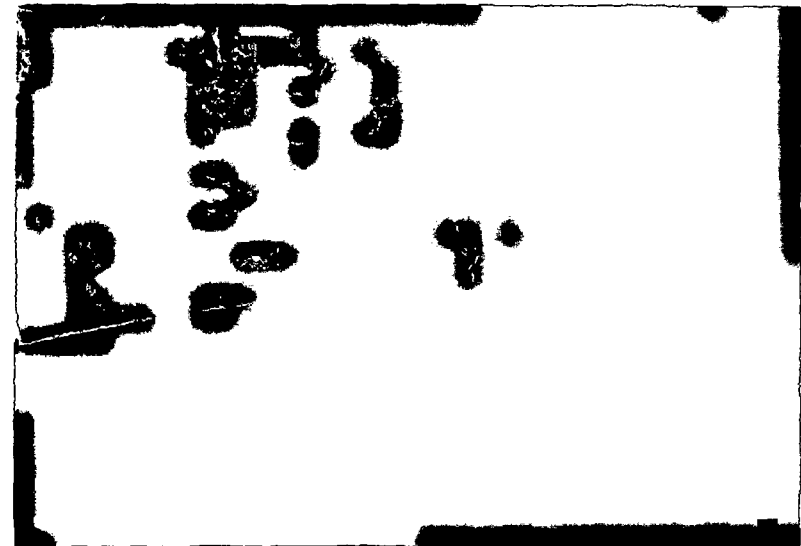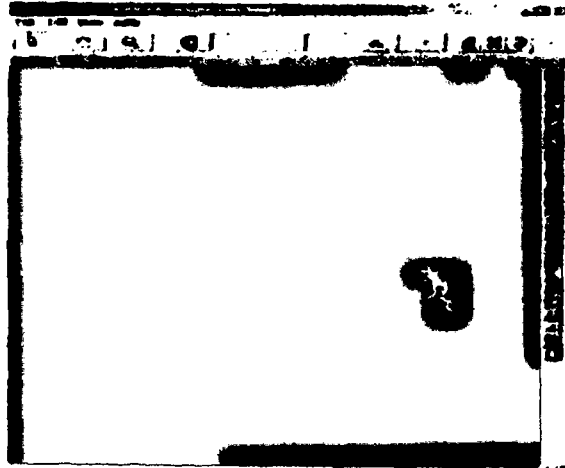
Homeland
Security

Knowledge Discovery and Dissemination

Knowledge Discovery and Dissemination –

Data intensive techniques for rapid knowledge ingest, fusion, and query

KDD Challenges

Volume of data – Scalability of systems

Complexity of data – high dimensionality; incomplete/fuzzy; constantly changing; stemming from multiple ontologies, languages, cultures, etc.

Multiple media types – text, imagery, video, voice, web, sensor data, etc.

TVTA Solutions

Data aggregation, information extraction and integration, knowledge fusion

Use relationships among data, based on concepts rather than facts (for better interoperation)

Link discovery and pattern analysis

Algorithms for high performance query

Homeland
Security

Info Extraction Level	Data relations	Enabled analyses
Shallow	Syntactical, attributes	Time/location entity; actions
Medium	Simple semantic relations	Simple co-references
Deep	Complex semantic relations	All ties and co-references; entities plus roles

Knowledge Discovery and Dissemination

Thrust Area: Knowledge Discovery and Dissemination
Thrust Area Leader & Organization: Bob Burleson, LLNL

Technical Objective: Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) architecture (LLNL, LANL, ORNL, PNNL)

- Knowledge Extraction: populate knowledge management systems from structured/unstructured texts and media

- Visualization: view relations determined in knowledge bases

- Analysis: connect ad hoc analysis groups via integration of data and information

- Knowledge Management: scalable architectures for data integration; watch and warning systems; data pedigrees

Technical Objective: ADVISE Deployments (LLNL, LANL, ORNL, PNNL)

- TVIS: Operational system for IAIP

- All WMD Deployment: TVIS deployment for WMD analysts

Homeland
Security

Visualization Analytics Centers

Visualization Analytics – reasoning using visual representations *and* interaction techniques

Data representation and transformation useful for "broadest bandwidth into the brain"

Viz Challenges

Overwhelming amount of data, changing information sets, temporally-challenged analysts

How best to interact with science-based and info-based data and to easily construct and visualize hypotheses/scenarios ?

TVTA Solutions

Creating tractable knowledge signatures and datasets, linking to source docs

Mapping signatures to visual metaphors for perception, discovery, navigation

Merge interaction and discourse into visualization to support foraging, structuring, ... other analyst activities?
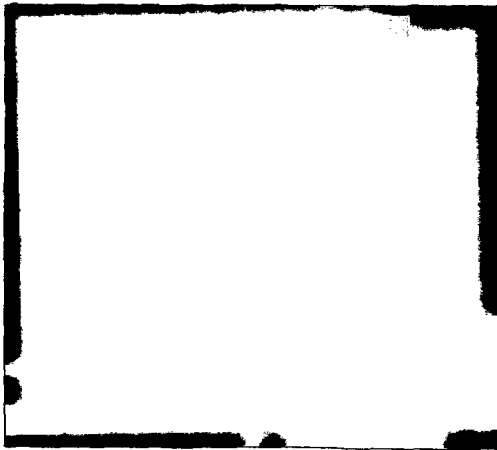
Document-centric Information display

Homeland Security

Castro's speeches pre-Bay of Pigs (temporal/content display)

Visualization Analytics Centers

Thrust Area: Visualization and Analytics Centers

Thrust Area Leader & Organization: Jim Thomas, PNNL

Technical Objective: Visualization Analytics Leadership (PNNL)

- Attain and hold national leadership in Vizualization Analytics. Tactical program planning, educational outreach, coordination with University Programs, and liaison with government stakeholders.

Technical Objective: Research and Development (PNNL)

- R&D Portfolio: large-scale graph perception, analytic discourse, calibration and verification

Technical Objective: Partnerships (PNNL)

- Create and expand partnerships on regional levels (RVACs, IVAC, GVACs, DOE labs). IVAC intended to bridge to industrial partners, seed commercial R&D projects, evaluate industrial software relevant to IC. GVAC intended to serve government agencies outside of DHS.

Homeland
Security

Knowledge Discovery and Dissemination

KDD/Viz tools delivered to IA:

- **ADVISE (TVIS) knowledge management system tools**
  - **Nebraska:** fuses individual facts and relationships among the facts in a large semantic graph (LLNL)
- **IN-SIGHT document clustering**
  - document-centric
  - collection-centric
  - temporal slicer
- **Starlight: visualization**
  - Integrates multiple information types and displays relationships

Homeland Security
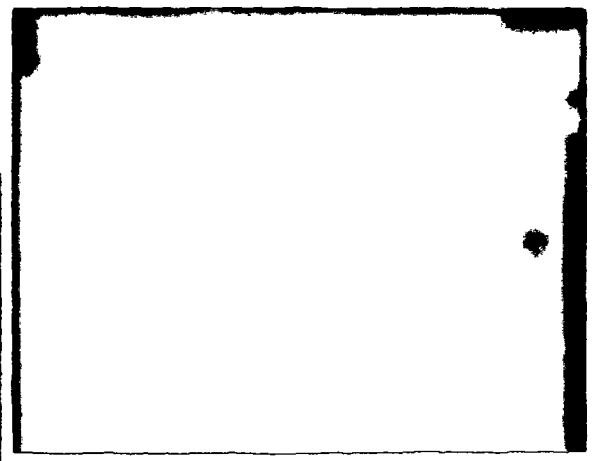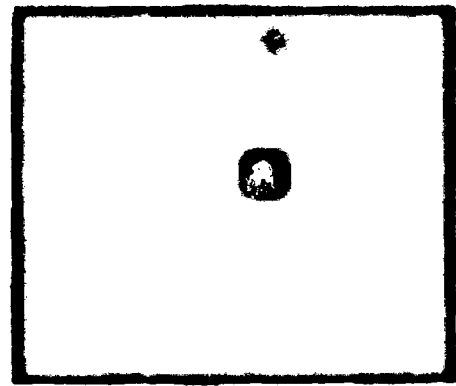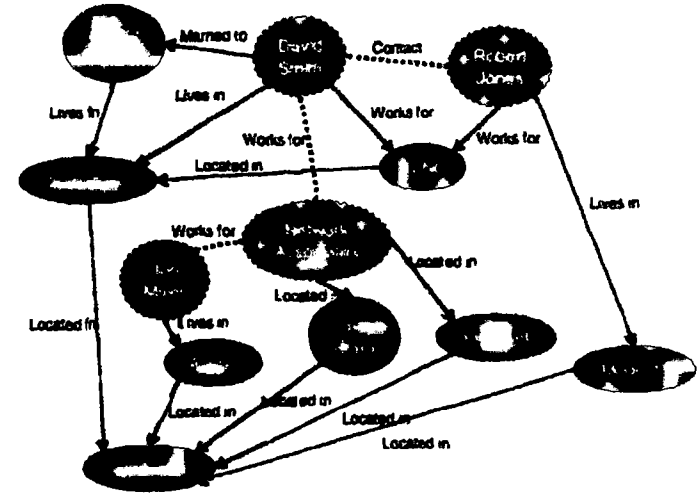
Modeling & Simulation and Decision Support

Advanced computing algorithms and hardware architectures for modeling, simulating, and managing threat data in real time and with high resolution

Thrust Area: Modeling & Simulation and Decision Sciences
Thrust Area Leader & Organization: Steve Ashby, LLNL

Technical Objective: Data Sciences (LLNL, ORNL, SNL)

• Large-Scale Data Integration and Querying: integrate dynamic, multi-modal, distributed information sources
• Scalable Information Analysis and Knowledge Discovery algorithms

Technical Objective: Simulation Technologies (LLNL, ORNL, SNL, LANL)

• Discrete Simulation Technologies: scalable software framework for multi simulation analyses. Agent-based modeling of FMD spread and terrorists' impact on economy.
• WMD Counter-Measures Modeling: model airborne toxins in outdoor and large-scale indoor environments

 Homeland
Security

Modeling & Simulation and Decision Support

DOE Advanced Scientific Computing (ASC) program supports MSDS thrust area. Recent accomplishments:

- Established *Institute for Discrete Sciences* to investigate and develop the specialized computing algorithms and hardware architectures to analyze massive amounts of diverse data from multiple, disparate, distributed data sources. National center with university, industry and government participation.

- Delivered parallel 2D-hypergraph partitioning algorithms which reduced communication by 10-100X for semantic graph querying and analysis in support of threat characterization. (Supports IA)

- Delivered 10X speedup in DNA signature algorithm and development of first draft-sequence alignment algorithm for improved pathogen detection. (Supports BKC)

- Reduced grid generation time 5000X via a novel and automated adaptive cut-cell approach that provides IMAAC with essential new capabilities for urban dispersion modeling. (Supports EP&R)

Homeland
Security

ASC develops new data science capabilities for DHS operational assets

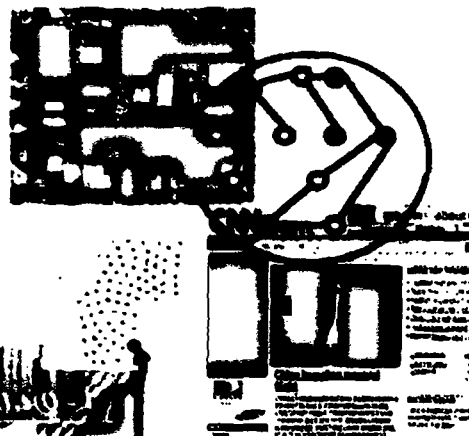*ASC supports DHS customers indirectly by delivering new capabilities to operational assets*

BKC

ADVISE provides IA and IC analysts with actionable information

These capabilities are integrated into ADVISE

ASC researchers develop new knowledge discovery capabilities

ASC "next generation" capabilities for faster, more accurate analyses

ADVANCED
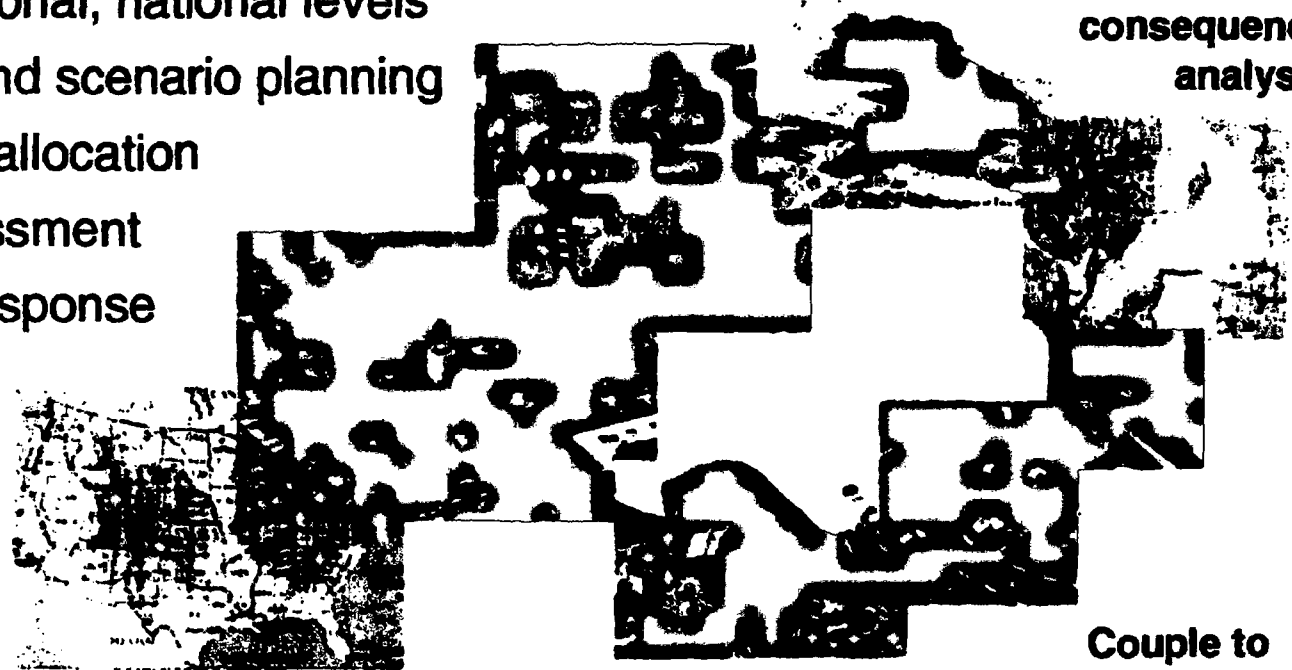**S**CIENTIFIC
COMPUTING
P R O G R A M

Homeland
Security

ASC's vision: Integrate capabilities into decision support tools

Teaming with others to define a National Incident Management decision support framework

Couple with dispersion modeling for consequence analysis

- Local, regional, national levels
- Training and scenario planning
- Resource allocation
- Risk assessment
- Incident response

Couple to transportation modeling for emergency response

Homeland Security

Threat Awareness and Characterization

All-WMD Capability Assessment and Nuclear Assessment Program

Assess capabilities of foreign and domestic terrorist groups to develop and deploy WMD threat agents and determining the credibility of communicated threats

Threat Awareness and Characterization Deliverables:

- Produce all-CBRNE capability assessments – analyze an additional 20 foreign terrorist groups' capabilities and intentions using information from intelligence community

- Create an encyclopedia of all-WMD threat data and incorporate into the ADVISE system

- Integrate all-WMD capability assessments with NAP credibility analyses

Homeland
Security

Threat Awareness and Characterization

Thrust Area: Threat Analysis and Characterization
Thrust Area Leader & Organization: Mary Beth Ward, LLNL

Technical Objective: All-WMD Assessments (LANL, LLNL, ORNL, PNNL, SNL)
• WMD Threat Capability Assessments: all source analysis of terrorist efforts, interests, and motives
• Target Assessments: written reports on terrorist development of CBRNCE weapons
• CATPAW Knowledge-Info Tool: integrated analyses and reports displayed as user-friendly tool
• Support to other TVTA tool development (ADVISE, M&I)
• Technical Reachback: on-request technical assessments of WMD threats
• Special Assessments: written, classified assessments of special topics

Technical Objective: Nuclear Assessment Program (LLNL, Yarrow)
• Intel and field assessments of nuclear threats, samples, black market activities

Technical Objective: Secondary Reachback Program (LLNL, LANL, SNL, RSL)
Assess detector and instrumented alarms from remote locations

Homeland
Security

Nuclear Assessment Program

A unique national capability to assist in the fight against nuclear crime and terrorism
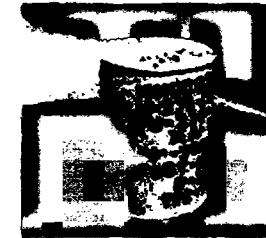
Assess nuclear threats

Identify credible threats
Provide rationale
Support federal
    decision makers

Behavioral
Resolve

Technical
Feasibility

Operational Practicality

Analyze illicit trafficking

Sales assessments
Illicit trafficking databases
Nuclear terrorism indicators
Special reports

Resources

Skilled assessors
Advanced analysis techniques
Coordinating center
Databases
Emergency communications
Deployable assets

Provide technical support

Special events preparedness
On-scene technical support
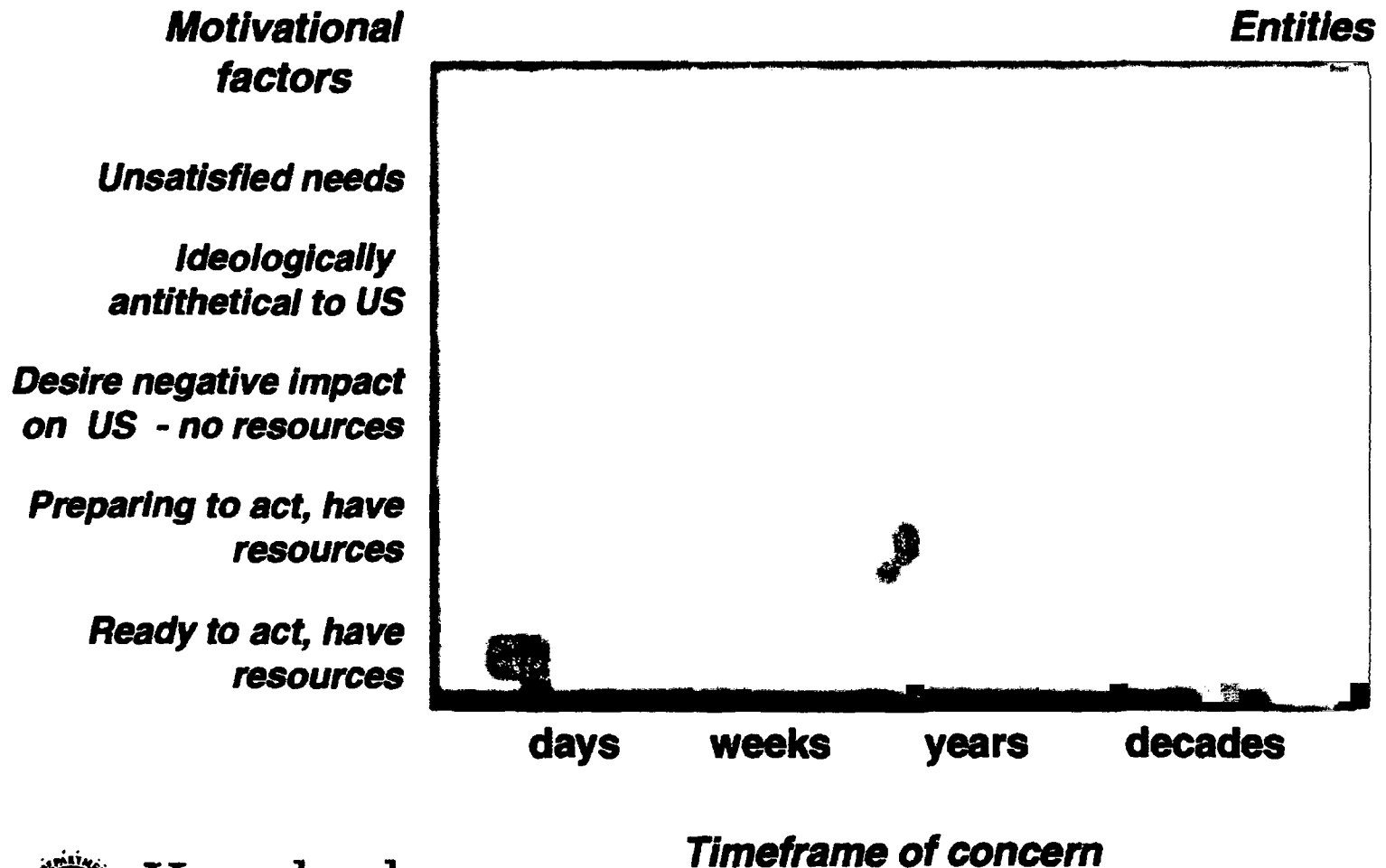National and international training

Homeland
Security

Motivation and Intent (New Start in FY05)

- **The Motivation and Intent (M&I) thrust area will** review, evaluate, develop, and deliver <u>behavioral methods</u> that can be integrated into an overarching and dynamic terrorism risk assessment process, leading to an enduring capability to understand and exploit terrorist intent, motives and behaviors.

- **M&I responds to user requirements to:**

  - Find and characterize M&I

  - Augment assessment capabilities

  - Perform comparative analysis to vet assessments (including confidence levels, probabilities and identification of intel gaps)

- *FY 05 Focus Problem: How does the information analyst infer M&I from a network of terrorist actors?*

Homeland
Security

Bounding the Threat Space

Motivational factors

Entities

Unsatisfied needs

Ideologically antithetical to US

Desire negative impact on US - no resources

Preparing to act, have resources

Ready to act, have resources

days   weeks   years   decades

Timeframe of concern

Homeland Security

Process Flow for M&I

Rely on and inform
Knowledge
Discovery Tools and
Techniques

To deploy countermeasures

Homeland
Security

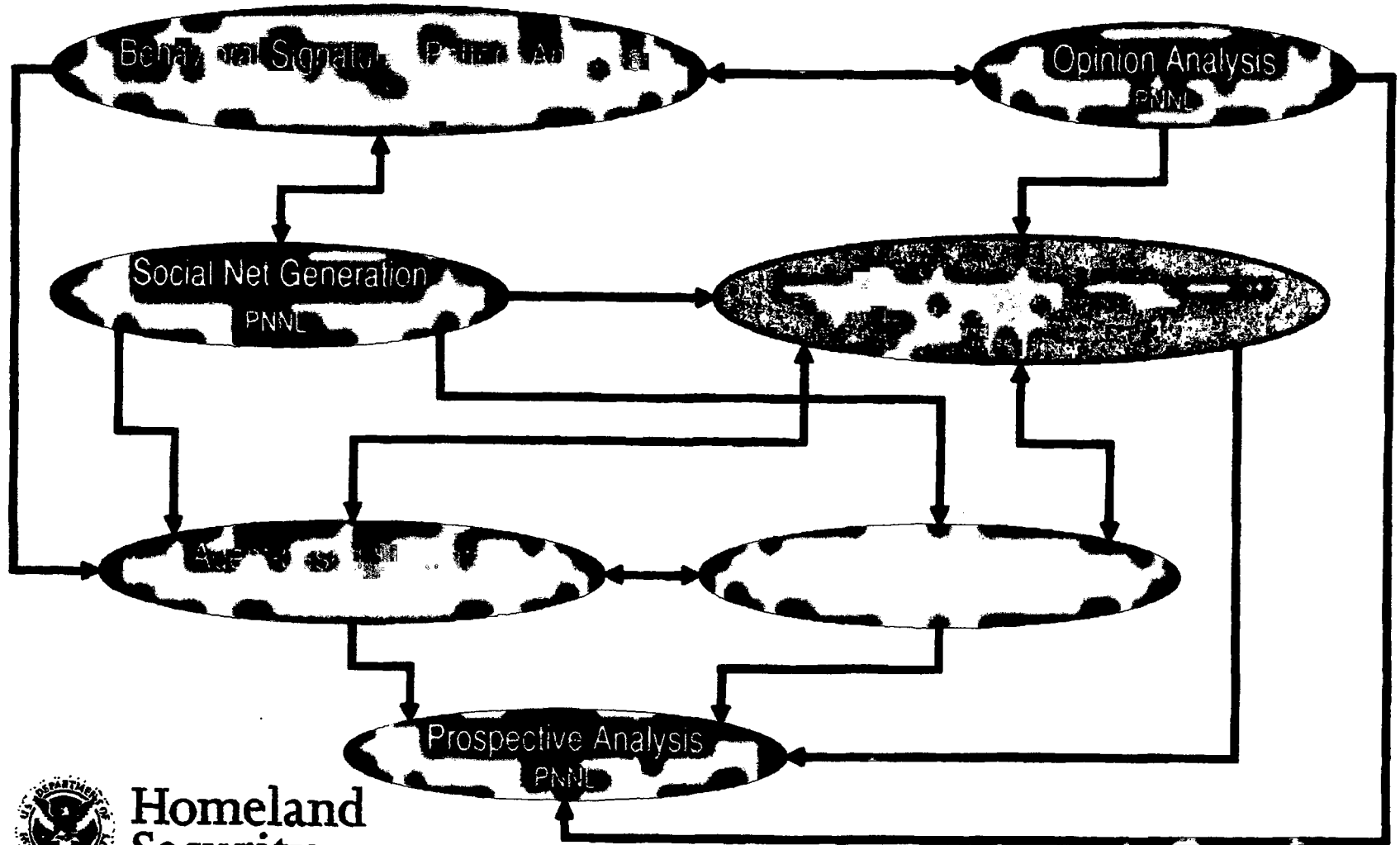As input to dynamic risk and threat assessment models
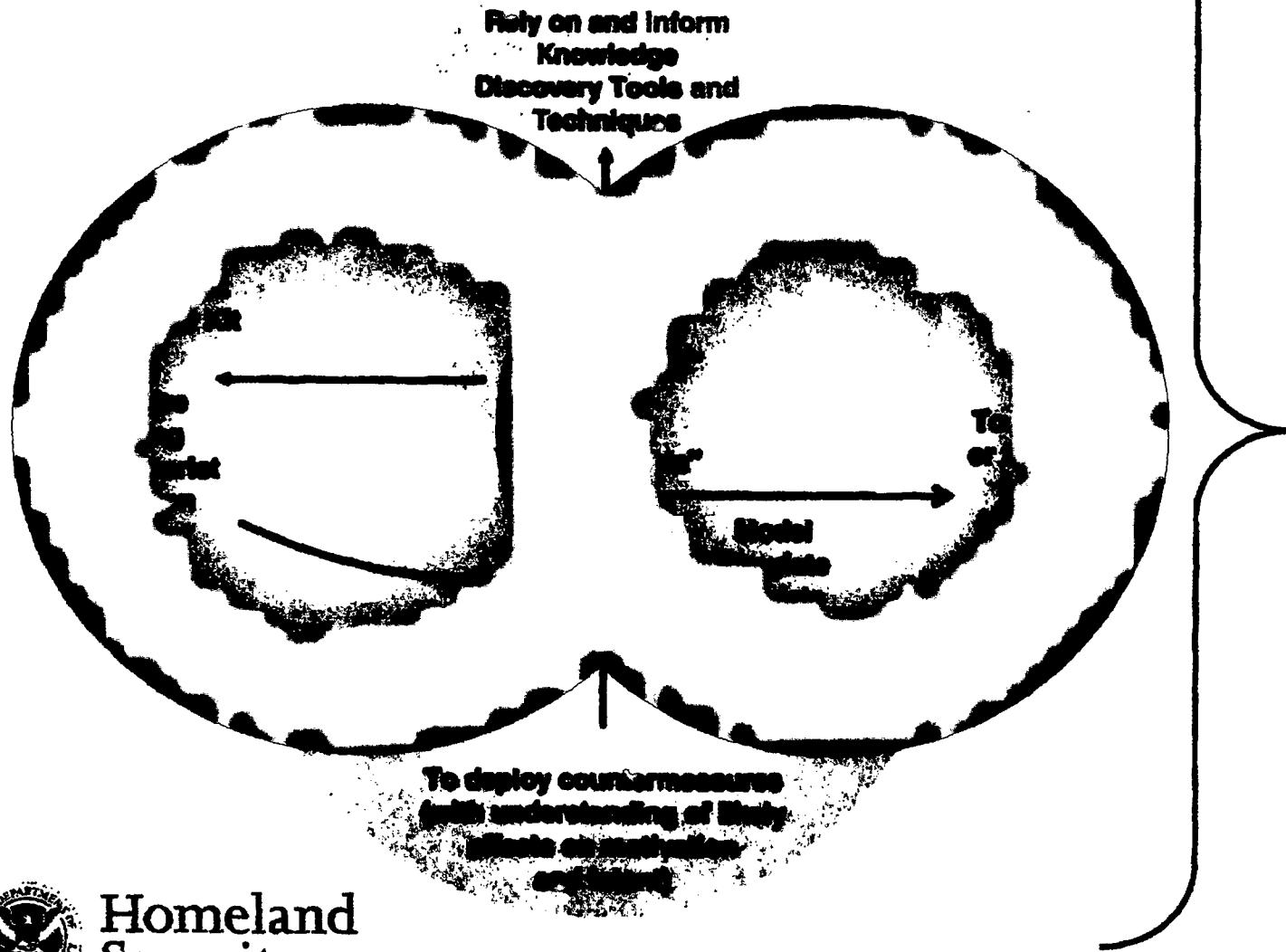
M&I Objectives and Deliverables

- **User Requirements**
  - Document use cases
  - SME collaborations

- **M&I Capability Development**
  - Develop and evaluate prototype capabilities against user-defined focus problem and data sets

- **M&I Operational Capability Integration**
  - Capture domain knowledge
  - Thrust area integration (joint development of ontologies)
  - Reach-back capability to SMEs in social-behavioral sciences
  - Deliver operational M&I capability (06 and onward)

- **Technical Review and Spiral Development**
  - Technology Roadmap (capabilities, integration and deployment)

Homeland
Security

Capabilities to be Developed for M&I

Behavioral Signature Pattern Analysis

Opinion Analysis
PNNL

Social Net Generation
PNNL

Prospective Analysis
PNNL

Homeland
Security

Threat Awareness

- TVTA Portfolio
  - Knowledge Discovery and Dissemination
  - Visualization Analytics Centers
  - Modeling, Simulation, Decision Support
  - Threat Awareness and Characterization
  - Motivation and Intent (new start)

- **Biodefense Knowledge Center (BKC)**

- **Emerging Threats**

- **Enhanced International Travel Security (EITS)**

Homeland
Security

Biodefense Knowledge Center (BKC)

Thrust Area: Biodefense Knowledge Center
Thrust Area Leader & Organization: Bill Colston, LLNL

Technical Objective: Exploit existing scientific knowledge base to anticipate/respond to bio attack (LLNL, ORNL)
- ***Established 24/7 S&T reachback support (includes SCI-level support)***
- Expand and integrate BKC analyst environment

Technical Objective: Accelerate understanding of Classical, Engineered, and Emerging Threats (LLNL, ORNL, PNNL, SNL)
- Expanded set of tailored knowledge products
- Material Threat Assessments for BioShield

Technical Objective: Knowledge Management Technologies/BKC Infrastructure (LLNL, ORNL, PNNL)
- Architecture integration with ADVISE KDD thrust
- Classified (SCI-level) knowledge management capability
- Analytical capabilities to view relationships across different information domains
- Knowledge acquisition

Homeland
Security

Biodefense Knowledge Center (BKC)

- **Rapid (<1 hour)**
  - Minimum research required--chiefly based on analyst experience or info available in knowledge base from previous inquiry

- **Near-term (1hr – 24hrs)**
  - Research required, but minimal information synthesis

- **Mid-term (days)**
  - Thoroughly researched assessments with a format that follows a research journal, including figures and tables

- **Long-term (wks - months)**
  - Multidisciplinary studies, such as the BioShield material threat assessments

TACTICAL

STRATEGIC
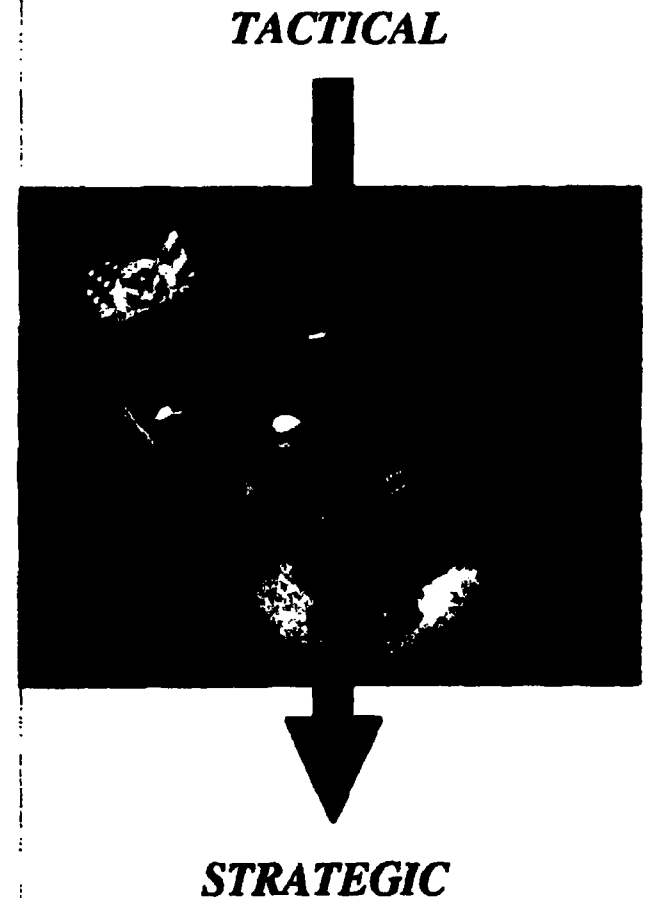
Homeland Security

Emerging Threats

Thrust Area: Emerging Threats

Thrust Area Leader & Organization: Mary Beth Ward, LLNL

Technical Objective: Emerging Threats & Technologies
(LLNL, LANL, SNL)

- Emerging Threats Workshops and Summary
- Emerging Threats Perspective Applied to WMD Analyses: threat reports specific to WMD
- Expand Compounded Infrastructure Threat (CIT) analysis (use of infrastructure as a Weapon of Mass Effect)
- Accelerate situational awareness following detection of a foot-and-mouth disease (FMD) outbreak
- Tech Trending: analyze emerging WMD threats
- Unexpected Threats and Innovative Solutions

Homeland
Security

Enhanced International Travel Security (EITS)

Thrust Area: Enhanced International Travel Security

Thrust Area Leader & Organization: Jeff Martin, SNL

Technical Objective: Create an international system of systems to share passport data and photographs of travelers in advance of their arrival at destination countries

- Proof of Concept scheduled for late 2005
- International in scope: UK, Australia, USA
- Secure, rapid transmission of data between governments
- Governance structure
    - Working Groups established on business/policy, governance, privacy/legal, and technical
- Awaiting HSC approval

Homeland Security

Our question to you:

How can we improve TVTA technology
and technology transition to IAIP?

Other questions?

Homeland
Security

Homeland
Security

Homeland
Security

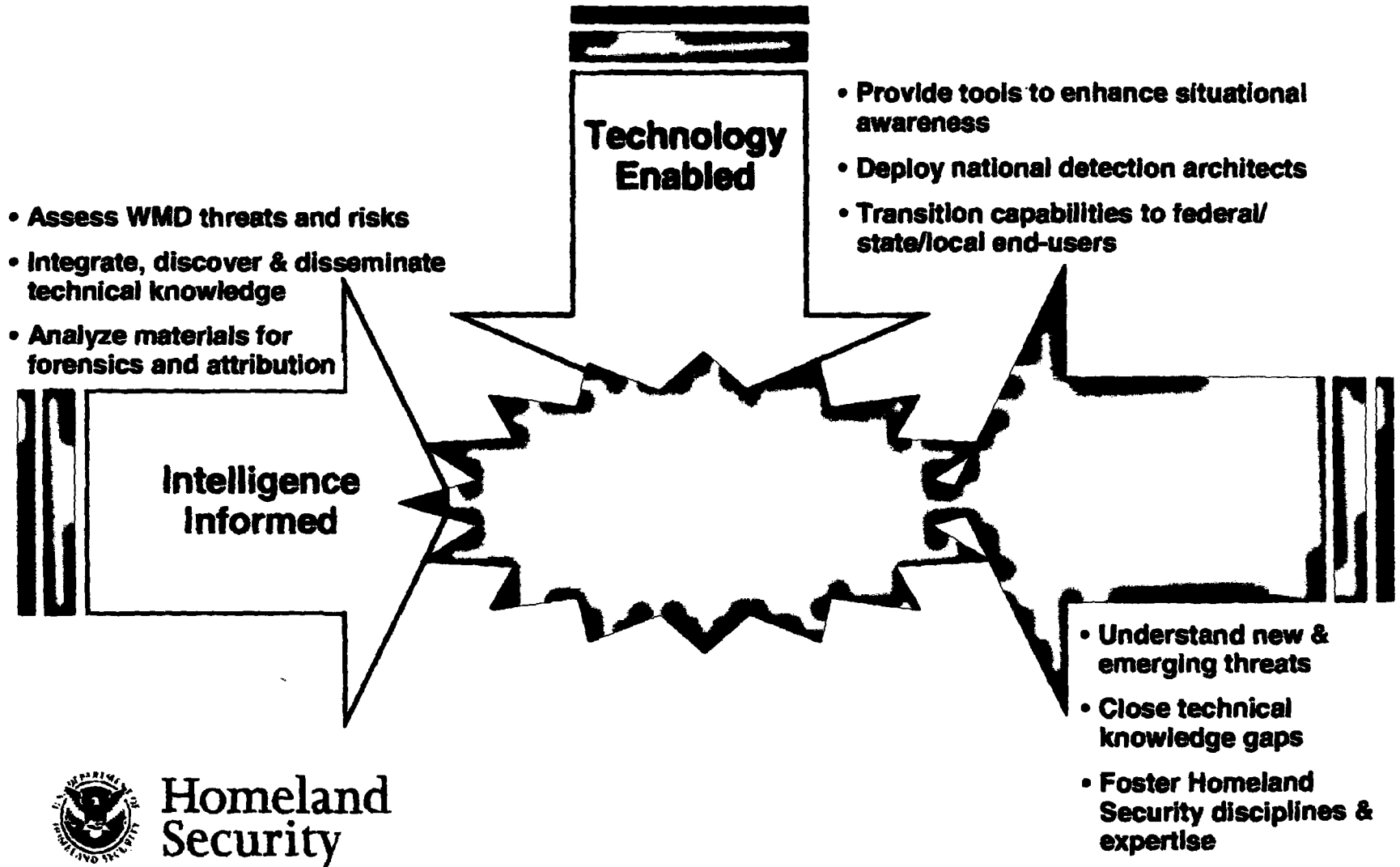# DHS S&T: Actionable Information to Support Intelligence Threat Analysis

Dr. Maureen McCarthy, Director
S&T Transition
Science and Technology Directorate
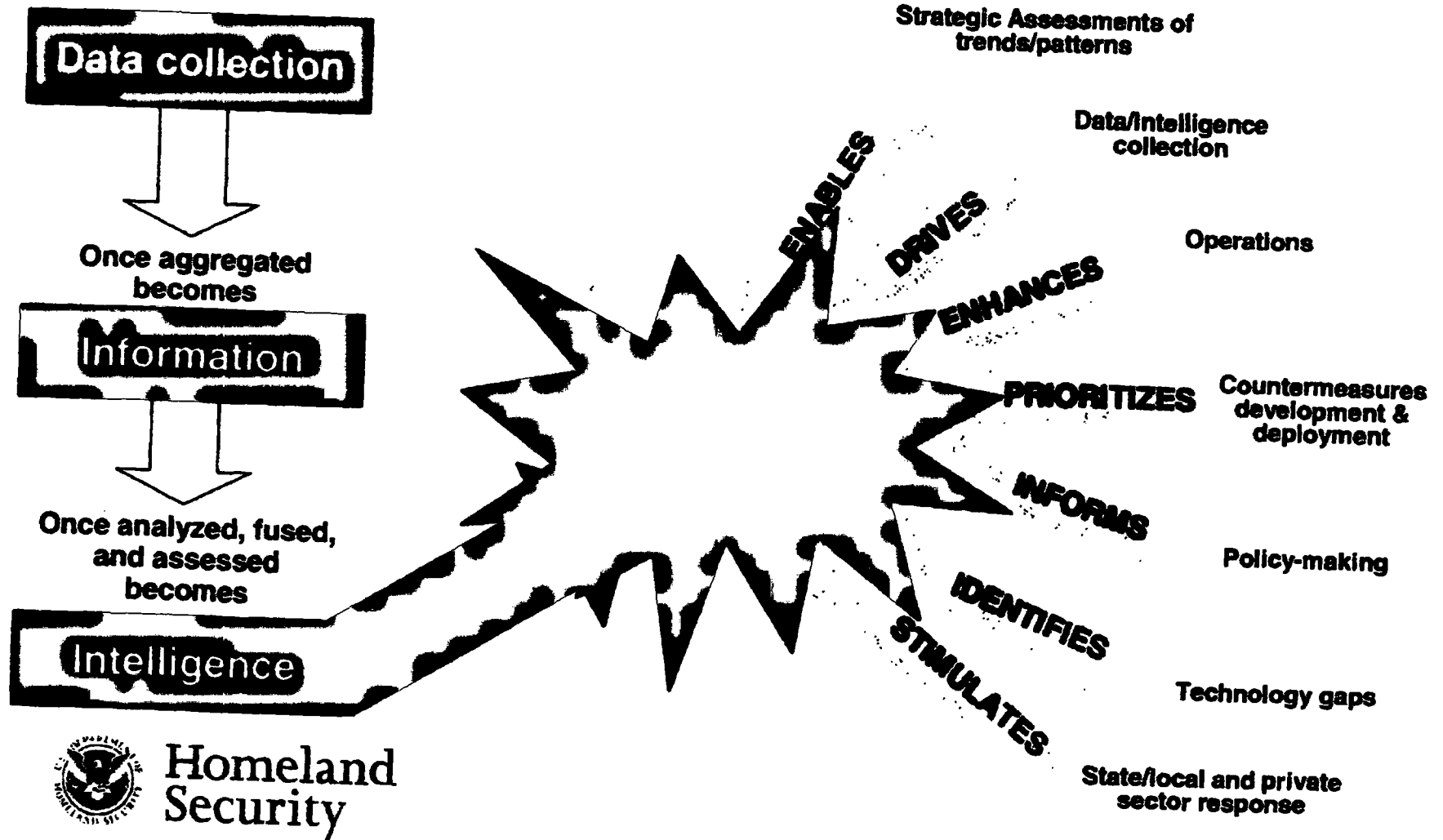Department of Homeland Security

Homeland
Security

S&T is the **Force Multiplier**
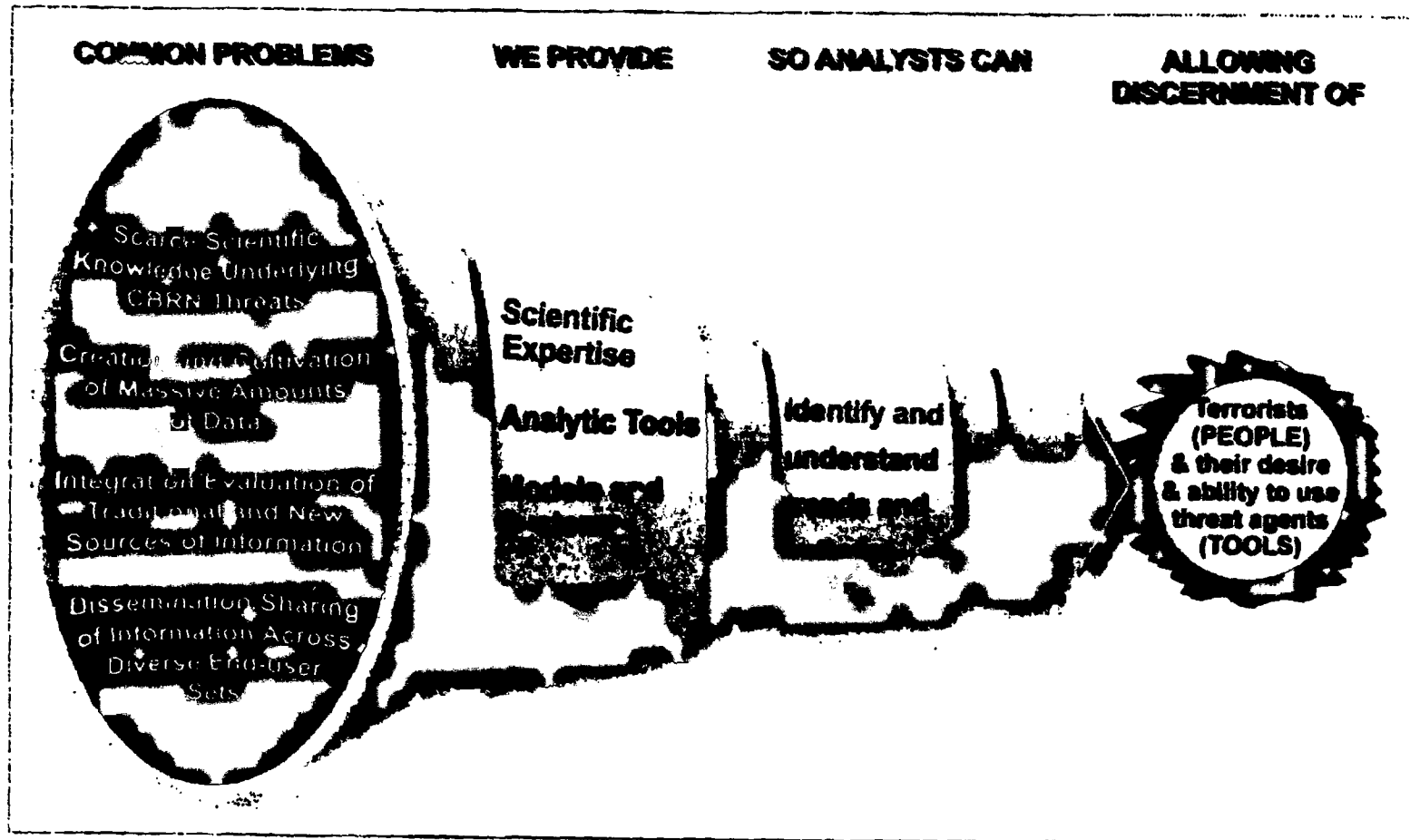# Our job is to make DHS Operations:

Technology Enabled

- Provide tools to enhance situational awareness
- Deploy national detection architects
- Transition capabilities to federal/ state/local end-users

- Assess WMD threats and risks
- Integrate, discover & disseminate technical knowledge
- Analyze materials for forensics and attribution

Intelligence Informed

- Understand new & emerging threats
- Close technical knowledge gaps
- Foster Homeland Security disciplines & expertise

Homeland Security

From Data Collection to Actionable Intelligence

S&T: Challenges and Strategies in Threat Awareness

COMMON PROBLEMS

- Scarce Scientific Knowledge Underlying CBRN Threats
- Creation and Cultivation of Massive Amounts of Data
- Integration Evaluation of Traditional and New Sources of Information
- Dissemination Sharing of Information Across Diverse End-user Sets

WE PROVIDE

- Scientific Expertise
- Analytic Tools
- Models and

SO ANALYSTS CAN

- Identify and understand needs and

ALLOWING DISCERNMENT OF

- Terrorists (PEOPLE) & their desire & ability to use threat agents (TOOLS)

Homeland
Security

Building an Enduring Capability to Enhance DHS Operations

Objective

CUTTING-EDGE SCIENTIFIC and TECHNICAL SUPPORT for IDENTIFICATION, INTERDICTION and MITIGATION of TERRORIST THREATS

Programs

Supporting Centers

Underlying Infrastructure

Technical insight and
Modeling and simulation
Exploration of motivation
Science based CBRN analysis

link analysis
Integration of massive data sets
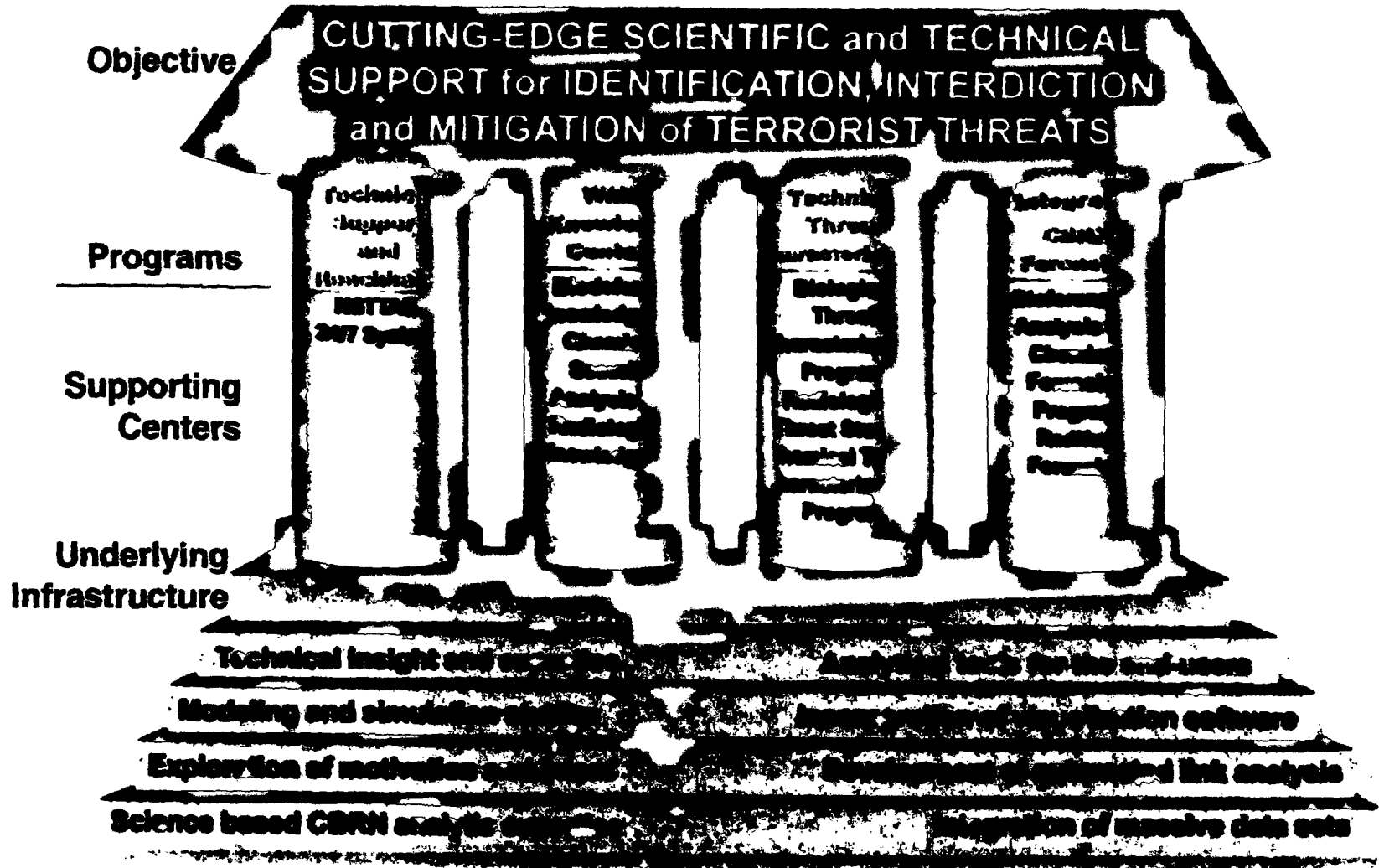
S&T Programs Supporting OI&A Threat Analysis

- **Threat Awareness Portfolio**
  - Knowledge Discovery Tools
  - Threat Awareness and Characterization

- **National S&T Threat Assessment and Reachback (NSTTAR)**
  - 24 hours a day / 7 days a week technical reachback service

- **Biological Countermeasures Portfolio**
  - National Biodefense Analysis and Countermeasures Center (NBACC)

- **Chemical Countermeasures Portfolio**
  - Chemical Security Analysis Center (CSAC)

- **Emerging Threats Portfolio**
  - Emerging Threats

Homeland Security

Threat Awareness Programs (TAP): Support DHS Missions

- Awareness
  - Identify and understand threats, determine potential impacts, and disseminate timely information
  - Fuse intelligence/information data; analyze and coordinate access to information
  - Provide timely, actionable, and valuable threat information
  - Ensure quick and accurate dissemination of intelligence

- Prevention
  - Detect, deter, and mitigate threats
  - Provide operational end-users with technology and capabilities to detect and prevent terrorist attacks means of terrorism, and other illegal activities

Homeland
Security

Knowledge Discovery Tools

ADVISE, designed for use by DHS analysts and operators, is a knowledge management architecture for collecting, analyzing, and synthesizing massive amounts of threat information from multiple, distributed, and disparate data sources.

Semantic Graph Technology:
- Fuses individual facts and relationships
- Analyze scenarios
- Test hypotheses
- Provide decision support
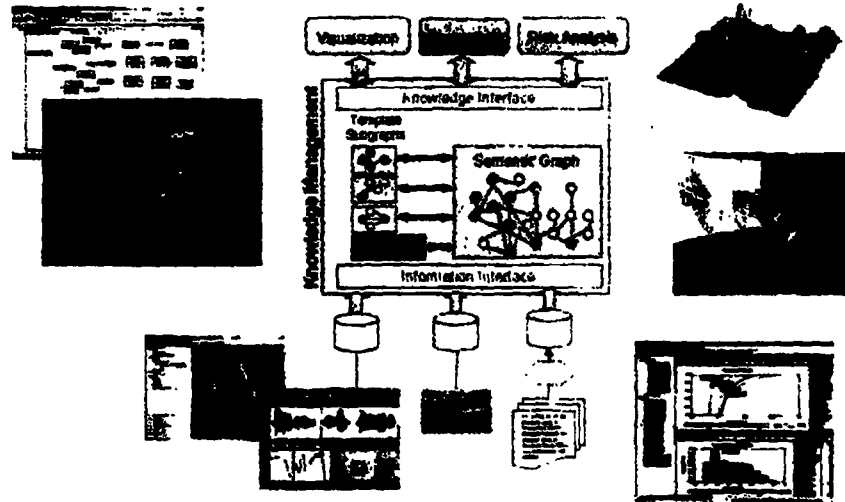
Visualization:
Cluster documents and analyze unstructured text to:
- Understand the relationships among documents
- Discover unexpected associations
- Rapidly identify most frequently used terms in the documents
- Collect documents into meaningful groups for comparison
- Query documents with word search or by thematic content

Homeland
Security

ADVISE Deployment at I&A: Threat-Vulnerability Integration System

- Status:
  - Loading data, demonstrations to analysts
  - Working with 3 groups:
    - Border Protection & Terrorist Travel (BP&TT): loading data, developing advanced queries
    - Terrorist Plans, Organizations & Networks (TPON): loading data, demonstrating capabilities with I&A data
    - Advanced Terrorist Weapons & Techniques (ATWT): loading data, demonstrating capabilities with I&A data
  - Direct support by National Laboratory analysts during initial rollout

- Relevance to customer:
  - Capturing high value documents not in any other retrieval environment
  - Capturing knowledge of analysts before they leave organization
  - Fusing with data entered from other parts of the organization
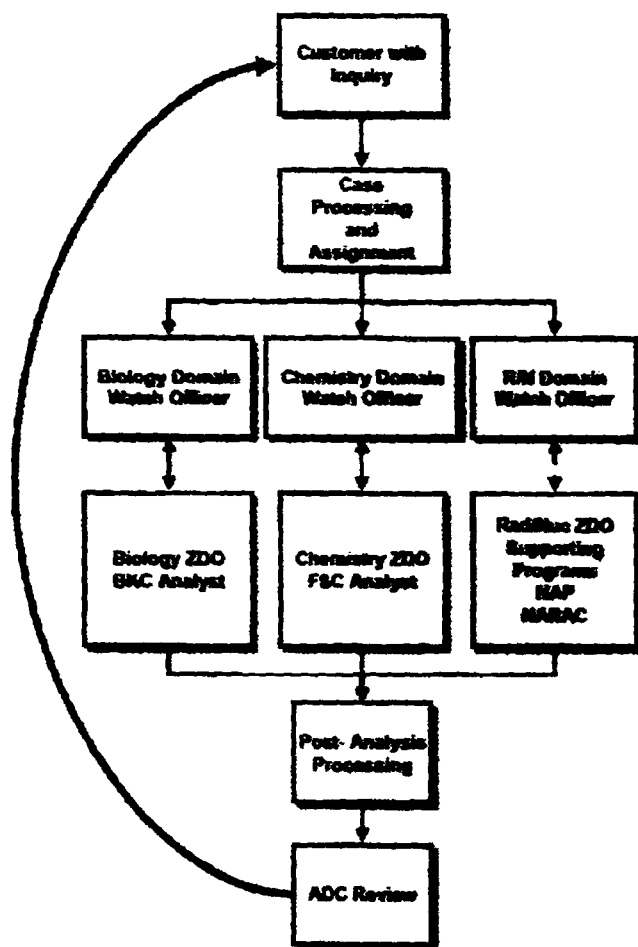
Homeland
Security

(b) (2)(high)

(b) (5)

# National S&T Threat Awareness and Reachback (NSTTAR) Service

- • *Provides 24 hours/day, 7 day/ week technical reachback for HSOC, DHS/I&A, DHS/S&T, ...*

- ▪ Focused on short-term, time critical tactical requests.

- ▪ Knowledge Center Domains are engaged in reachback activities as required by nature of request.

- ▪ Shapes analysis into appropriate reporting format and assures quality.

- ▪ Engages domain appropriate Authorized Derivative Classifier to ensure report conforms to regulatory standards

Homeland Security

NBACC: Secure Characterization and Evaluation of Biologicals
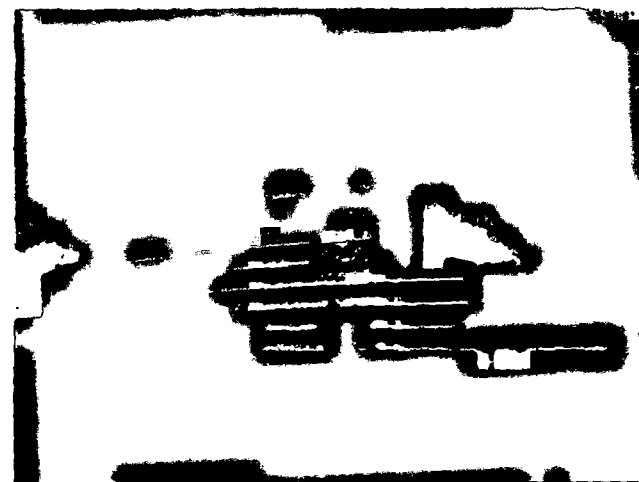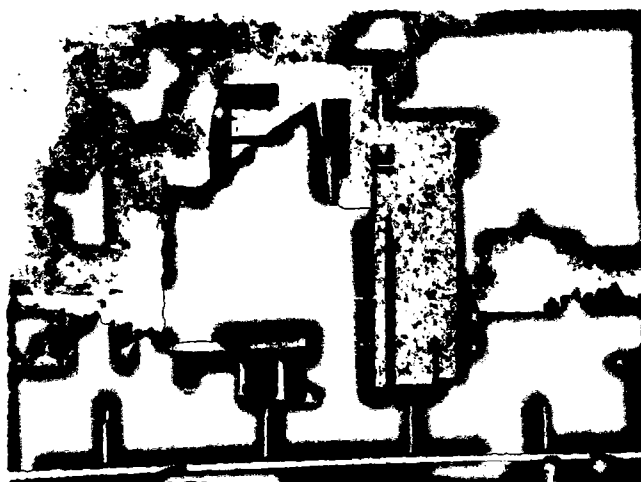
- The National Biodefense Analysis and Countermeasures Center (NBACC) facility (2008) will be the world's first fully-SCIFed high containment research facility:

  - **Bioforensics Analysis Center (BFAC)** is the lead federal facility for coordinating, directing, and executing forensic analysis to support casework and attribution of biologicals

  - **Biological Threat Characterization Center (BTCC)** characterizes current and emerging biological threats through literature and laboratory studies

  - **Biodefense Knowledge Center (BKC)** evaluates and integrates biological threat agent data to enable expert analysis and reachback support for targeted end user communities
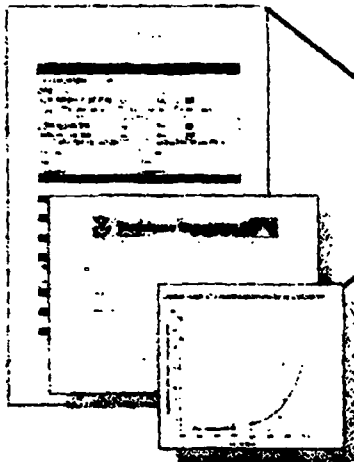
Homeland Security

$$(h)\left(2\int ds\,h\right)$$

S&T Activities Supporting DHS OIA

S&T IPAs provide IA augmentation of on-site technical expertise and

S&T knowledge centers provide IA analysts 24/7 reachback support and tailored WMD assessments to address technical requirements

S&T and IA collaborate on technical threat assessments that identify key intelligence gaps and requirements
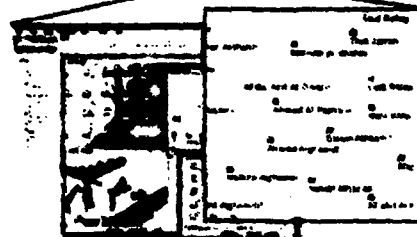
Homeland Security

S&T developed and deployed ADVISE analytic toolset based upon requirements and feedback from IA leadership
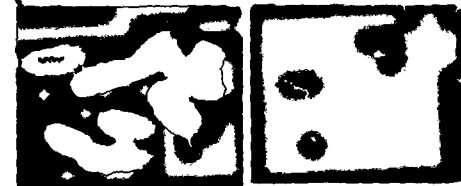
S&T laboratories obtain and evaluate CBRN samples to provide insights that inform IA WMD threat assessments

Outstanding Challenges for S&T

- Identifying and communicating intelligence requirements that target collection needed to close key CBRN technical gaps.

- Fostering and leveraging national technical expertise to better understand motivation and intent of hostile actors.

- Ensuring sufficient communication between performers and end users for timely identification and rapid satisfaction of S&T technical infrastructure requirements.

- Anticipating evolution of needs to target S&T investments and develop core competencies in appropriate disciplines.

Homeland
Security

Homeland
Security

Homeland
Security