

Overview of the Human Factors Division in DHS S&T

Sharla Rausch, Ph.D., Division Head
Department of Homeland Security (DHS)
Science and Technology (S&T) Directorate
Human Factors Division
March 1, 2007



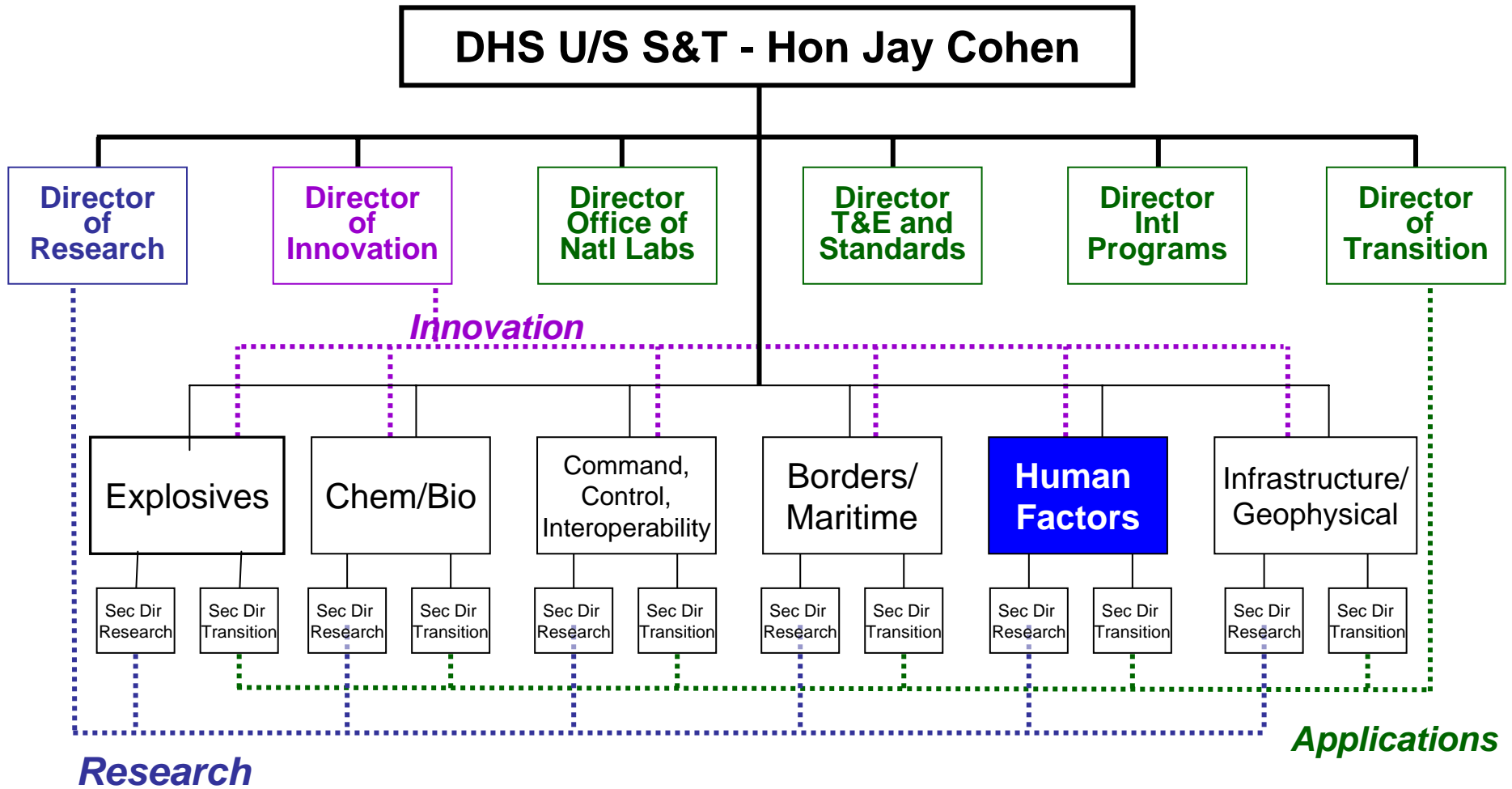
**Homeland
Security**

Human Factors Division (HFD) Mission Statement

To apply the social and behavioral sciences to improve detection, analysis, and understanding of the threats posed by individuals, groups, and radical movements; to support the preparedness, response, and recovery of communities impacted by catastrophic events; and to advance national security by integrating human factors into homeland security technologies.

Know our enemies, understand ourselves; put the human in the equation.

Science and Technology

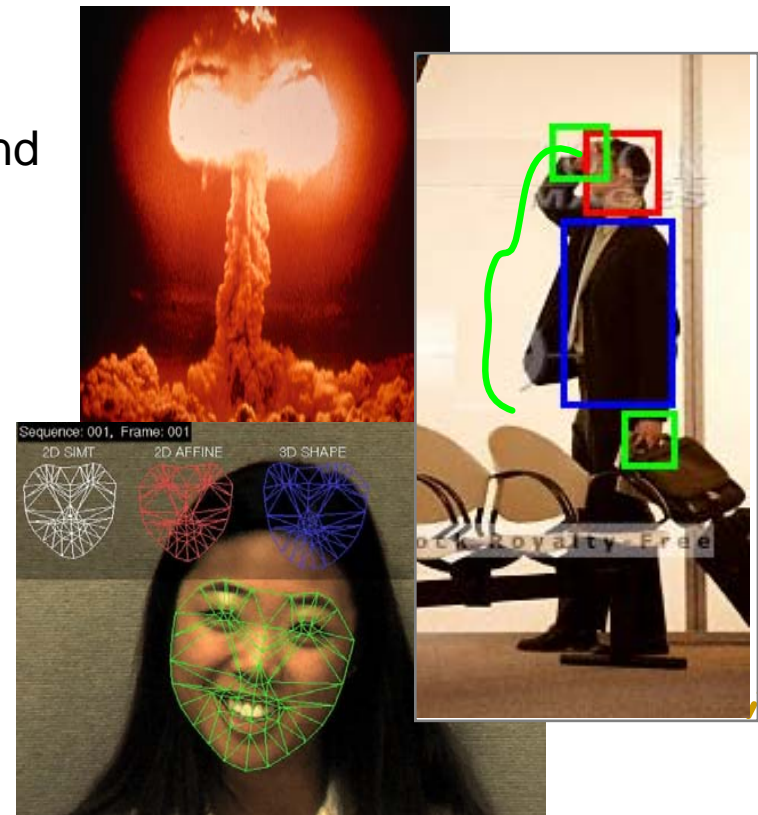


Homeland Security

HFD Thrust Areas

The DHS S&T Human Factors Division is comprised of two primary thrust areas, with programs under each:

- Social-Behavioral Threat Analysis
 - Motivation and Intent
 - Suspicious Behavior Detection
 - Community Preparedness, Response, and Recovery
- Human Systems Integration
 - Personal Identification Systems
 - Technology Acceptance and Integration
 - Technology-Human Integration



HFD Goals

1. Enhance the capability to control movement of individuals into and out of the United States and its critical assets through accurate, timely, and easy-to-use biometric identification and credentialing validation tools.
2. Enhance safety, effectiveness, and usability of technology by systematically incorporating user and public input.
3. Enhance the analytical capability of the Department to understand terrorist motivation, intent and behavior.
4. Improve screening by providing a science-based capability to identify deceptive and suspicious behavior.
5. Mitigate impacts of catastrophic events by delivering capabilities that incorporate social, psychological and economic aspects of community preparedness, response and recovery.

Social-Behavioral Threat Analysis

- Enhance our awareness of threats across multiple layers of analysis
 - At the individual level – detect and model the behavioral, linguistic, and physiological cues of deception and/or hostile intent exhibited by individuals
 - At the group (and movement) level – based on social and behavioral science data and theories, model indicators of group (and movement) intent to engage in violence

Mission directed behavioral science adds value to national security.



**Homeland
Security**

Social-Behavioral Threat Analysis (cont.)

- Understand and deter radicalization
 - Study radicalization through varying lenses
 - DHS S&T is an active participant in an internal DHS Radicalization Working Group
 - Share up-to-date science on radicalization
 - DHS S&T brings together top researchers to share science with United States government policy, operations, and science communities



Social-Behavioral Threat Analysis (cont.)

- Support preparedness, response, and recovery of communities
 - Evaluate and improve risk communication messaging during emergencies
 - Assess and quantify the psychological, social, and indirect economic impacts of extreme events to inform risk analysis, preparedness, response, and recovery
 - Examine gaps in responding to the public during and after catastrophic events



Partnerships with Social, Behavioral, and Human Factors Scientists and Others – Outreach Activities

- United States government
- International partners
- Academia and the private sector

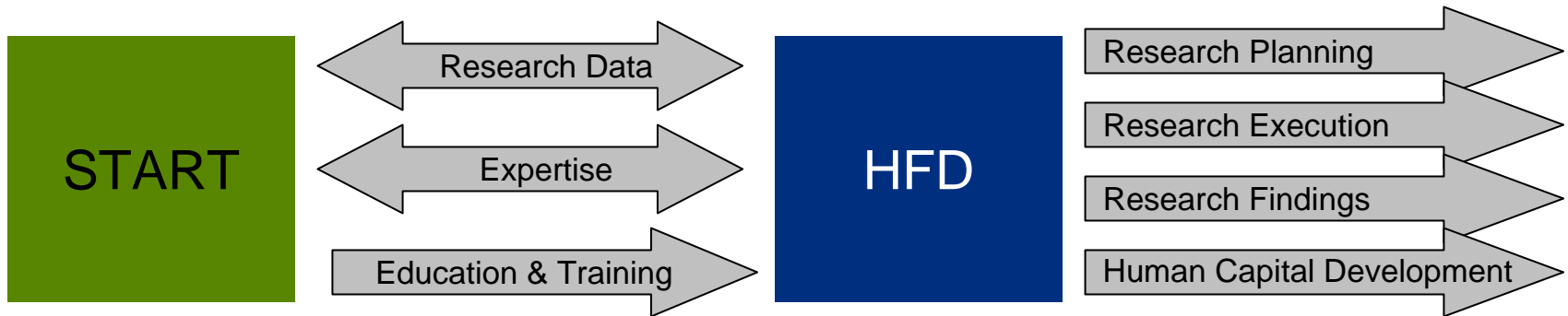


We're always looking for new colleagues and new partners.



Homeland
Security

HFD and START



Maximizing outputs by leveraging the strengths and resources of partners.



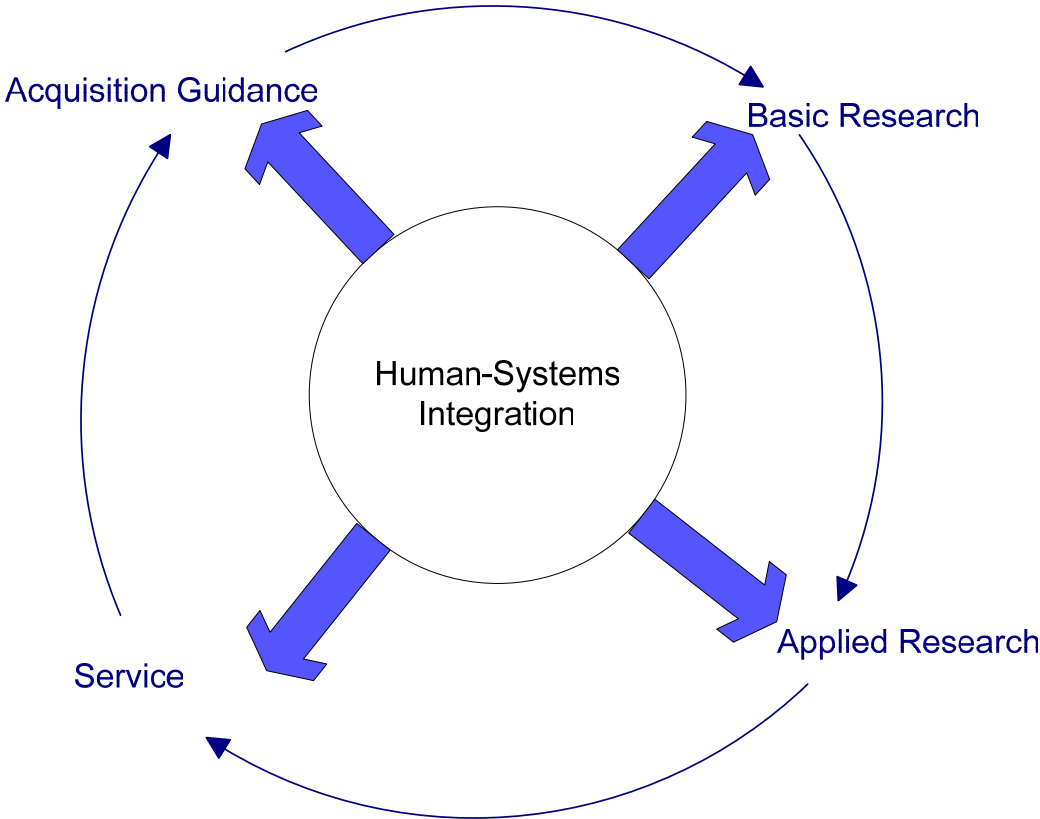
Human Systems Integration (HSI)

- Design for *usability* – incorporate human factors research into technology development across science and technology divisions
- Design for public acceptance (e.g., Community Acceptance of Technology Panel)
- Maximize human factors expertise and resources through partnerships (e.g., Transportation Security Lab, NASA)
- Current program example
 - Developing a simple and effective multi-biometrics capability for diverse identification scenarios, such as border crossings, ports of entry, and visa application sites

Human factors research results in better system effectiveness and safety.



HSI Program Elements



We Are Always Looking for Good People...

1. Motivation & Intent Program Manager
2. Human Systems Integration Program Managers
3. Biometrics Program Manager
4. Tech Acceptance & Integration Program Manager
5. Social, Behavioral, and Economics Program Manager
6. Community Preparedness and Response Program Manager
7. Group Violent Intent and Radicalization Program Manager
8. Suspicious Behavior Detection Program Manager
9. Human Systems Integration Engineer



**Homeland
Security**

None of the related problems [of terrorism] can be solved by technology alone; every solution is subject to the reality of being implemented and operated by humans. These are system issues, where individual, social, and organizational behaviors are part of the system and, therefore, must be part of the research and design.

Making the Nation Safer, page147



**Homeland
Security**



Homeland
Security

Biometrics

Product Description

- Multi-modal biometric tools (finger, face and iris) to identify known terrorists --- Accurate, real-time, & contactless
- A multi-modal biometric framework that can be implemented across DHS operational mission space

Program Elements and Performers

- Multimodal biometrics test and evaluation framework; reference multimodal data set; prototype system
- CITeR (Center for Identification Technology Research), NIST, Kentucky CIP Laboratory, University of Notre Dame
- Planned Demos/Deliverables/Transitions
- System Design – FY07
- Multi-modal Biometrics T&E Framework – FY08
- Contactless Multi-modal Biometrics ID Prototype – FY08
- Multi-modal Reference Dataset – FY08
- Demonstration and Test – FY09



Payoff

- Accurate biometrics-based identification of known terrorists prior to their entering U.S.
- Increased throughput of travelers across the U.S. border



Other Agency/Consortium Projects

NIJ

- Fast Capture Fingerprint Palm Print
- 3D Facial Images from Surveillance Video
 - Multimodal Fusion with Quality Metrics
- Dimensionality Increasing Facial ID
- Biometrics Standards Tools Development
- Biometrics Catalog Support

NIST

- Image Quality Standards for Fingerprint and Face Images
- Evaluation Standards for Latent Fingerprint Matches
- Standard for Human Computer Interface and Usability of Biometric Systems
- Multimodal Biometric Accuracy Research Kiosk (MBARK)
- Rapid Eval



1401 Tech Transfer

- Automated Biometric Identification System (ABIS)
- Common Access Card (CAC)
- The Advanced Vehicle/Driver Identification System (AVIDS)
- Biometric Identification System for Access (BISA)
- Defense Biometric Identification System
- Portable Forensic Laboratory
- NDRC/Detainee Reporting System
- Navy Maritime Interception Operations (MIO)
- Portable Biometric System (PBS)
- Hand-Held Interagency Identity Detection Equipment (HIDE)
- Biometrics Automated Tool Set (BAT)
- Biometric Access Management System (BAMS)



- Quality Based Restitution of Iris Features in High Zoom Images for Less Constrained Iris Recognition Systems
- Recovering the Frontal Facial Image from Surveillance Video
- A Dynamic Hierarchical Fusion Architecture for Biometric Systems
- Encryption of Biometric Templates using Biometrics as the Key
- Adaptive Biometric Authentication
- Fingerprint Matching Using Level 3 Features
- Multispectral & Multiframe Iris Analysis
- Video-Based Metrology for Automated Human Identity Profiling



Homeland
Security

Credentialing

Product Description

- Develop and test an accurate, real-time, contactless, biometrics-based card-and-reader system
- R&D work supporting SCO for its LA/Long Beach TWIC (Transportation Worker Identity Credential) demonstration
- Design, development, and demonstration of secure, standoff interrogation capability

Planned Demos/Deliverables/Transitions

- Demonstration Design – FY07
- LA/LB Port Demonstration – FY07
- Contactless System Requirements & Design – FY08
- Contactless Prototype– FY09
- Contactless Demonstration & Test – FY09
- Remote Interrogation System Design – FY10
- Remote Interrogation System Prototype – FY10



Payoff

- Ensures security of U.S. ports and other facilities
 - Provides a tamper-proof, electronic, biometrics/biographical credential to identify 850,000 port and transportation workers
- Provides technical foundation for credentialing systems applicable throughout U.S.



Homeland
Security

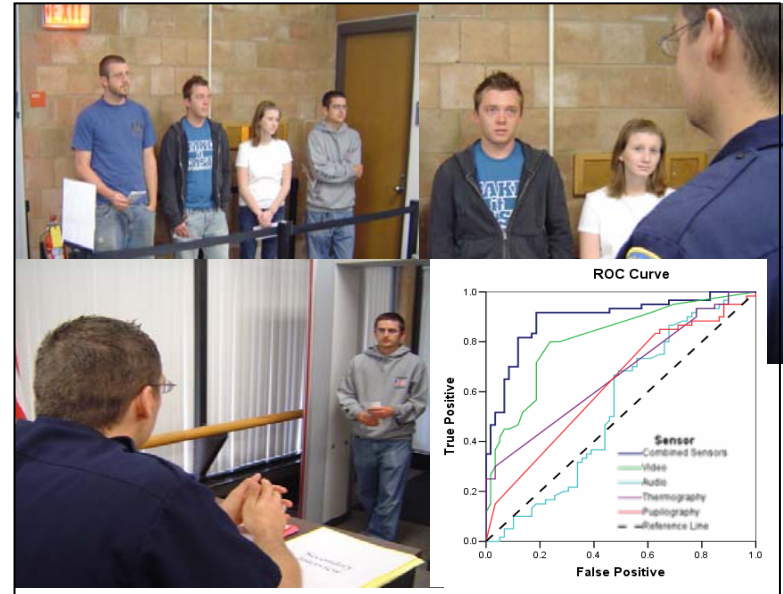
Hostile Intent

Product Description

- Real-time, multi-modal, culturally independent hostile intent detection prototype (Behavioral, physiological, auditory) to identify unknown or potential threats terrorists --- Accurate, real-time, & non-invasive
- A multi-modal intent detection framework that can be implemented across DHS operational mission space

Planned Demos/Deliverables/Transitions

- Transition Baseline Behavior-Based Indicators
- Demo Near Real-Time Intent Detection – FY 08
- Demo Integrated Biometric/Intent Framework– FY09
- Demo Real-Time Auto Intent Detection – FY09
- Transition Computer-Base Intent Training – FY010
- Transition Multi-Modal Auto Intent Detection – FY10
- Transition Cross-Culturally Validated, Reconfigurable Auto Intent Detection – FY12



Payoff

- Provides multiple layers of accurate non-invasive screening of unknown threats prior to their entering U.S.
- Increased security and throughput of travelers across the U.S. border through reduced false alarms.

Group Violent Intent Modeling (GVIM)

Product Description

- Intelligence analysis framework that includes information extraction of signatures of terrorist intentions, systematic estimation of future terrorist behavior based on social and behavioral sciences, and modeling and simulations of influences on future terrorist behavior

Program Elements and Performers

- Information extraction and content analysis; ontology; modeling and simulation capabilities; system integration
- LANL, LLNL, ORNL, PNNL, SNL

Planned Demos/Deliverables/Transitions

- Integrated system, version 1 – FY07
- Integrated system, version 2; first implementation at user site – FY08
- Final system delivery – FY09



Payoff

- Increase confidence in estimates of a group's intention to engage in violence
- Increase ability to rapidly assemble and test competing scenarios



Community Acceptance of Technology Panel

Product Description

- Develop and successfully adopt application-specific and user/public friendly technologies and processes.
- Increase the effectiveness of technology development, testing and deployment.
- Improve the understanding of user/public sensitivities toward a technology before it is deployed.
- Increase the public trust in those technologies being deployed by the Department.



Program Elements and Performers

- Panel of scientific, industry, public interest, and community-oriented organizations to meet 3 to 5 times each year.
- Issue and recommendation papers.

Planned Demos/Deliverables/Transitions

- Deploy at least 2-3 vetted technologies in FY07.

Payoff

- Outcomes will guide development and implementation of S&T-led technology and process improvements.
- Public acceptance and support enables cost-effective designs and deployments of technologies.

