

INTERAGENCY COUNCIL FOR APPLIED HOMELAND SECURITY TECHNOLOGY

# ICAHST

LONG-TERM RESEARCH NEEDS



SECOND EDITION



ICAHST — the Interagency Council for Applied Homeland Security Technology — is an ad hoc council of organizations involved in the information technology issues of homeland security, law enforcement and counterterrorism. Although it is not an official body, ICAHST provides a forum where organizations can meet and share research needs, results and lessons learned. The current members of ICAHST are:

#### U.S. Department of Defense

- Assistant Secretary of Defense for Networks and Information Integration\*
- Defense Advanced Research Projects Agency\*
- Combating Terrorism Technical Support Office
- Technical Support Working Group
- Joint Warfare Analysis Center

#### U.S. Army

- The National Ground Intelligence Center
- Space and Missile Defense Command

#### U.S. Navy

- Office of Naval Intelligence

#### U.S. Department of Energy

- Office of Intelligence and Counterintelligence
- Remote Sensing Laboratory
- Savannah River National Laboratory
- Lawrence Livermore National Laboratory

#### U.S. Department of Homeland Security

- Science and Technology Directorate\*
- Intelligence and Analysis Directorate
- Office for Bombing Prevention
- Federal Emergency Management Agency
- Customs and Border Protection
- Office of Operations Coordination

#### U.S. Department of Justice

- National Institute of Justice
- Federal Bureau of Investigation
- U.S. Marshals Service\*
- Bureau of Alcohol, Tobacco, Firearms and Explosives\*

#### U.S. Intelligence Community

- Office of the Director of National Intelligence
- Intelligence Advanced Research Projects Activity
- National Counterterrorism Center\*
- National Reconnaissance Office\*
- National Security Agency
- Central Intelligence Agency\*
- Defense Intelligence Agency\*
- National Geospatial-Intelligence Agency\*
- In-Q-Tel Program Office\*

#### U.S. Department of State

- Bureau of Intelligence and Analysis

#### U.S. Department of Commerce

- National Institute of Standards and Technology

#### U.S. Department of Treasury

- Office of Intelligence and Analysis

#### U.S. Department of Agriculture

- United States Forest Service/Law Enforcement Investigations

#### White House

- Office of Science and Technology Policy

#### State of Alabama

#### State of Nevada

#### Baltimore Police Department

#### Boston Police Department

#### District of Columbia Metropolitan Police Department

#### Miami-Dade Police Department

#### Las Vegas Police Department

#### Los Angeles County Sheriff's Department

#### Los Angeles Police Department

#### Mesa (AZ) Police Department

#### Richmond (VA) Police Department

#### Aurora (CO) Police Department

#### Prince George's County (MD) Police Department

#### Pacific Disaster Center

#### Maui High Performance Computing Center

#### INTERPOL Washington

\* ICAHST founding member



Homeland  
Security

Dear Colleagues,

The *Interagency Council for Applied Homeland Security Technology* (ICAHST) is an ad hoc council of federal, state, local and tribal organizations involved in the information technology issues of homeland security, law enforcement and counterterrorism. Although it is not an official body, ICAHST is a forum where government organizations and other entities dealing with these issues can meet and share research needs, results and lessons learned. This unique group — which was established in April 2004 — has participants from more than 50 organizations within the intelligence, law enforcement and homeland security communities.

The primary mission of ICAHST is to identify, investigate and assist in the implementation of new science and technology to improve the nation's counterterrorism and homeland security capabilities. In 2006, ICAHST published its first set of long-term research needs required to support these capabilities, and that document resulted in a number of studies, pilots and other technology evaluation efforts among ICAHST members. Now, under the guidance of its current chair, Dr. John S. Morgan, ICAHST is publishing the second edition of this important collaboration effort involving first responders, researchers, law enforcement personnel, intelligence analysts and associated management personnel.

I believe this document, which represents true cross-agency collaboration, can play an important role in accomplishing our shared mission of protecting America. I look forward to your feedback.

Sincerely,

A handwritten signature in black ink that reads "Randel L. Zeller".

Randel L. Zeller  
Director, Interagency and First Responder Programs  
Science and Technology Directorate  
U.S. Department of Homeland Security



## U.S. Department of Justice

### Office of Justice Programs

### *National Institute of Justice*

---

Washington, D.C. 20531

Dear Colleagues:

As the research, development and evaluation arm of the U.S. Department of Justice, the National Institute of Justice (NIJ) provides objective, independent, evidence-based knowledge and tools to meet the challenges of crime and justice in the United States.

Under The Homeland Security Act of 2002, NIJ is responsible for identifying law enforcement technology needs and developing solutions to meet those needs. NIJ's participation in the Interagency Council for Applied Homeland Security Technology (ICAHST) supports that mission.

NIJ is pleased to be a member of ICAHST, a forum through which we can share our information technology development efforts with other ICAHST members. This synergy gives all ICAHST members the opportunity to identify ways to leverage our respective technology investments.

I am proud to help publish *Long-Term Research Needs*, an important synthesis of the law enforcement, counterterrorism, homeland security, and intelligence research needs that will help keep our nation safe.

Sincerely,

A handwritten signature in black ink, appearing to read "Kristina Rose".

Kristina Rose  
Acting Director  
National Institute of Justice

# FOREWORD

In this publication — the second edition of *Long-Term Research Needs* — the Interagency Council for Applied Homeland Security Technology (ICAHST) describes 20 goals or “missions” that we believe should be supported through continuing innovation in science and technology. As a scientist, I know that innovation in technology depends on research.

We have synthesized the technology research needs of a number of ICAHST members, including the U.S. Department of Homeland Security; the National Institute of Justice; the National Counterterrorism Center and other elements of the Office of the Director of National Intelligence; the National Security Agency; the National Reconnaissance Office; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Technical Support Working Group and others.

We present these research needs — in no priority order — as components of the classic intelligence cycle: collection, processing, analysis and dissemination. In an effort to describe the “big picture” of long-term research needs, we have chosen not to cite specific programs, initiatives or agendas of ICAHST members; rather, our goal here is to offer a true synthesis of research areas that will meet the long-term needs of our nation’s diverse intelligence, law enforcement and homeland security communities.

It has been my honor to serve as the chair of this innovative group. In particular, I have been grateful for the opportunity to ensure that the needs of my agency’s key constituent — state and local law enforcement — are fully represented in our nation’s research agenda.

I hope that this publication raises awareness of ICAHST as a unique governmentwide collaboration dedicated to addressing homeland security issues. Participation in ICAHST allows members to share information and identify ways to leverage research opportunities through various collaborative efforts. Visit [www.ichst.org](http://www.ichst.org) for more information about symposia, workshops, conferences and pilot projects.

ICAHST members believe that meeting the security challenges of the future requires rapid prototyping, experimentation, and demonstration of new tools and technologies. I hope that everyone working on these important issues — at universities and laboratories, in private industry and public agencies — finds guidance in this publication regarding the research investments that will make our nation safer.

I believe this publication serves as an example of cooperation and collaboration across organizational boundaries in accomplishing our mission of protecting America. I welcome your comments and feedback.



John S. Morgan, Chair  
Interagency Council for Applied Homeland Security Technology



# CONTENTS

## COLLECTION OF INFORMATION

MISSION 1	Develop Methods and Technologies to Prepare Data .....	3
MISSION 2	Develop Methods and Technologies to Ensure Secure Data Storage .....	4
MISSION 3	Develop Information Retrieval Tools .....	5
MISSION 4	Develop Detection Technologies .....	6
MISSION 5	Develop Human Tracking and Locating Technologies .....	8
MISSION 6	Develop Tools and Technologies to Ensure Infrastructure Protection .....	9

## PROCESSING OF INFORMATION

MISSION 7	Develop Biometrics Technologies .....	13
MISSION 8	Develop Link Analysis Technologies .....	14
MISSION 9	Develop Language Translation Capabilities .....	14
MISSION 10	Develop Digital Forensics Tools and Technologies to Improve the Processing of Evidentiary Data and Information .....	15
MISSION 11	Develop Technologies to Assess and Evaluate Chemical and Biological Defense .....	16

## ANALYSIS OF INFORMATION

MISSION 12	Develop Information Analysis Technologies.....	19
MISSION 13	Develop Automated Organizational Structures Recognition Technologies.....	21
MISSION 14	Develop Geospatial Technologies.....	21
MISSION 15	Develop Predictive Analysis Technologies, Particularly Geared to Anomaly Detection.....	22

## DISSEMINATION OF INFORMATION

MISSION 16	Develop Technologies to Improve Access Control.....	27
MISSION 17	Develop Technologies to Improve the Access to and Integration of Information.....	27
MISSION 18	Develop Technologies to Disseminate and Share Information.....	28
MISSION 19	Develop Technologies to Disperse Information for Public Welfare.....	28
MISSION 20	Develop Technologies to Improve Cybersecurity.....	29



COLLECTION  
OF INFORMATION





## MISSION 1:

# Develop methods and technologies to prepare data

New tools and technologies are needed to prepare data. Data preparation includes data extraction, high-speed ingest and creation of data in electronic format.

### Extraction

Data must be rapidly extracted from external sources to maximize the utility of time-sensitive information. Without automated data extraction capability, analysts must manually identify and process data of interest for ingest into the information repository. Tools and technologies must be created that improve the acquisition of data by rapidly extracting relevant information and ingesting it into a targeted repository for analysis.

Data must be extracted from multimedia sources, such as text, audio, video and imagery. It also must be extracted from foreign language text, including native scripts, with a goal of achieving at least 95-percent accuracy for named entities, events, relationships, and temporal and spatial factors.

For example, technologies that support intelligence-led policing would use standards such as the Justice Reference Architecture (JRA) to collect and share criminal justice information; this also entails the creation of new specifications and technologies using criminal justice data with temporal and spatial attributes.

### Ingest

Timeliness and accuracy in preparing, tagging and transforming large data repositories for use in analytic applications are essential. Current high-speed data-ingest

tools were designed to get a stream of data into a database as quickly as possible without regard for the fidelity or completeness of the data source. Although these tools are useful for data transport, they do not appreciably increase operator productivity and efficiency.

Data repositories must be in a format that can be quickly exported to analytical tools and external queries. One significant challenge is the automation of metadata description, which, when generated manually, is labor-intensive and error-prone. Consolidating access to data and

metadata — which currently reside in thousands of disparate data systems — is essential to improving the productivity and efficiency of analytic tasks, such as predicting and determining terrorist relationships and activities.

Analyst productivity will also be improved by ensuring that high-speed data ingest technology:

- Focuses on integrated analysis of text, video, geospatial and speech inputs.
- Extracts, fuses and synthesizes situational information from multiple, disparate data sources.
- Batches load data stored in various geographic formats, including Vector Product Format (VPF) coverage, shapefile and geo-database formats.
- Ensures consistency between the source data and metadata and between metadata across the intelligence community, including backward compatibility in which emerging data marked to new metadata standards can be combined with data marked according to older, disparate standards.



- Has an automated learning functionality that rapidly adapts — without heavy human processing — to new sources.

## Electronic formatting

Data from many disparate sources and in many different forms — including structured and unstructured text, photographs and other images, audio and video files, tables, graphs, diagrams, maps, equations and chemical formulas — must be automatically put into electronic format.

Of paramount interest is technology that ensures the rapid processing of law enforcement field data — such as photos, manuals, written reports and evidence descriptions — into electronic format. Such technologies also must be able to capture “pocket litter,” such as notes and address books, and data from cell phone call logs, contact lists and storage devices. Creating a digital copy of such information is, however, only the first step; the greater challenge is digitizing the information in a meaningful, accessible way. For example, there are challenges when a single object contains links between multiple information objects, with the meaning of any object dependent on information contained within other objects.



Intelligence analysts and criminal justice professionals, including law enforcement using intelligence-led policing principles, must be able to construct a coherent, real-time picture from such scattered heterogeneous fragments of data. Tools must be developed that improve the entity resolution and correlation of persons, places and things and also must be able to:

- Understand and describe the nature of and relationships between objects.
- Process data that may have already been fused.
- Build upon geospatial data integration, correlation and analysis.
- Search, analyze and disseminate criminal justice information across jurisdictional boundaries.

A crucial component of intelligence-led policing is standards-based electronic information exchange.

Technologies that improve this process will allow experts from a variety of disciplines to understand the interconnectedness of data — for example, analysts who must consider the social, military, economic, political, governmental, multilingual, scientific and technical issues surrounding an event or location.



## MISSION 2: Develop methods and technologies to ensure secure data storage

New technologies and methods are needed to meet the growing volume of intelligence data. Such tools must expand current storage capacity to meet the increasing demands of data processing, including accessing, fusing and analyzing.

Advanced storage and processing technologies must filter information overload from petaflop processing and allow petabytes-capacity storage so that analysts can fully exploit data resources. Data storage also must ensure the protection of U.S. citizen personal data, including advanced data integrity technologies that automatically purge or anonymize personally identifiable information.

## MISSION 3:

# Develop information retrieval tools

Analysts must be able to perform sophisticated searches to retrieve data from many disparate local and remote sources. Currently, this is a time-consuming process because they potentially must use a different interface, format and configuration for each data source.

To ensure that distributed information retrieval technologies — including sophisticated, interoperable query and integration techniques — can access data across diverse networks, we should:

- Develop the capability to identify and link multiple, heterogeneous data sources with schemas, metadata and different physical locations.
- Reduce redundancy in data, databases, hardware and software.
- Establish shared-information strategies that collect information once at the source, where it is controlled by the owner, then allow it to be accessed — pursuant to enforced security policies — by others.

Secure mobile systems must be able to communicate anywhere, anytime, handling large amounts of data both on the move and by accessing remote locations using

physical computing and communications devices. Such devices include the next generation of interoperable communications tools and convergent broadband solutions.

Each technology — from radio and computer networks to wireless and untrusted systems, including laptops, wireless LANs, Internet, mobile ad hoc networks (MANETs) — comes with its own vulnerabilities. Therefore, information assurance tools must address unique confidentiality and

integrity issues, such as inherent denial-of-service vulnerabilities. This is of particular concern with wireless-based devices where jamming could be used. Assurance technologies must also address mitigation issues.

Technology development should ensure reliable communication where the end-points may be trustworthy but the networks are untrusted. This involves moving raw data from the field to analysts, then moving analyzed product from the analysts back to the field for action. In some instances, it may be possible to provide sufficient security at

lower protocol layers; therefore, research and development should consider the most scalable methods of achieving the goal, such as setting up virtual private networks (VPNs).



## MISSION 4:

# Develop detection technologies

Technologies are needed to detect, track and classify a wide range of threats from any point on earth and report back to authorities in real time. Whether the threat is borne by a person, vehicle, vessel or aircraft, tools must allow safe interdiction — including nonlethal compliance of people — by law enforcement. Such threats include:

- Contraband, including controlled substances such as narcotics.
- Firearms.
- Stowaways and other unauthorized persons.
- Explosives, including improvised explosive devices (IEDs).
- Weapons of mass destruction, including toxic industrial chemicals, biological materials (such as pathogens and toxins), and radiological and nuclear material.

New detection tools — including systems solutions — should work in indoor and outdoor environments, such as along terrestrial and maritime borders, tunnels, rugged terrain with concealing foliage and water obstacles, transportation hubs and critical infrastructure sites. Detection technologies are also needed to meet the challenges of novel biological threats to the agriculture and food industries, including the breakout of animal disease. Handheld detection tools must be able to rapidly distinguish threatening biological and chemical agents from nonthreatening agents without interfering with the stream of commerce.

Technologies should improve integrated chemical, biological, radiological, nuclear and explosive (CBRNE) sensor reporting. Future detection systems should be

built with standards that allow for the integration of new prediction, warning and reporting technologies.

With particular respect to IEDs, research is needed to:

- Improve the capability of detecting and defeating vehicle-borne improvised explosive devices (VBIEDs), particularly, nonexplosive and standoff-defeat technologies; this includes nonintrusive screening to interrogate a vehicle at a distant range through diagnostic and defeat procedures on explosives.

- Detect person-borne IEDs at standoff distances in high-throughput venues, including at vehicle and pedestrian ports-of-entry and border crossings.
- Tag explosives material.

Personnel-safe, handheld devices should facilitate the nonintrusive inspection of hidden or closed compartments. Technologies other than x-ray, gamma rays and neutrons are needed, including tools that detect contraband and human security threats through steel walls.



## Cargo and Containers

With more than 65,000 cargo containers crossing U.S. borders daily, maritime shipping is widely believed to be the most likely means for terrorism-related materials to enter the country. Currently, rule-based targeting techniques, combined with random inspections, are used to identify containers that then must be examined by an officer.

To ensure that predictive techniques are as effective as possible, the accuracy and completeness of cargo and

container data should be improved. Currently, for example, data that are critical to container security — whether the container has been breached after loading on a vessel or may contain an even relatively small amount of chemical, biological, radiological or nuclear material, for example — are not collected.

In addition to developing nonintrusive inspection tools and technologies for maritime cargo and containers, we should be able to screen 100 percent of air cargo for explosives and explosive devices, particularly bulk and break-bulk, palletized and containerized air cargo. Technologies are also needed to track domestic high-threat cargo, particularly cargo in domestic transit that has been designated Toxic Inhalation Hazardous (TIH).



Among the technologies that are needed to improve penetration, resolution, throughput, contrast sensitivity, reliability, mobility and interoperability — including integration with future Automated Target Recognition (ATR) capabilities — are:

- Seal security and detection intrusion devices, such as tamper sensors for mechanical and electromagnetic seals on all six sides of a container.
- Seismic sensors to detect an attempted breach.
- Single-use sensors to detect radiological, nuclear, chemical and biological and explosive material.
- Communications technologies for detecting and reporting anomalies.
- Networking technologies that allow a container to act as a communications relay point for another container; this, for example, could consist of an ad hoc system that allows the top container in a 10-container stack below the ship's deck to transmit data from the vessel to a space-borne communications system that would, in turn, relay data to a Continental U.S. (CONUS) operations center.

- Integrated GPS-related technologies that provide information on where a container is and has been.

With respect to fixed aviation and mass transit checkpoints, national-scale strategies and architectures are needed to increase detection rates in screening people for explosives and weapons while minimizing disruption to passenger flow. This includes improved screening and examination by nonintrusive inspection and automated systems solutions to detect conventional and novel (homemade) explosives, liquids and weapons in checked and carried bags.

Technological research and development, including systemwide solutions, should also increase the accuracy (and reduce the time and cost) of detecting insider threats and mitigating any harm caused by an unauthorized insider.

Technologies are needed to quickly identify the origin of gunfire and classify the type of a weapon fired. This technology would serve two purposes: to alert law enforcement personnel to incoming gunfire and to create forensic data.

Finally, continued information technology research and development are needed to improve the ability of intelligence analysts and other users to detect when new information is available. Currently, analysts are not automatically notified when data are updated or when a recently performed search would reveal additional results; therefore, analysts must repeatedly search the same sources to ensure that a product reflects the most current intelligence. Data change technologies — such as automated “push” technology — must be developed to notify users when new or modified nontrivial data are detected.

## Behavior detection

Technologies are needed to detect deception and hostile intent in real time, particularly the “human precursors” — behaviors, tactics, techniques and procedures (TTPs) —

that can help prevent IED attacks. Such technologies include noninvasive behavioral sensors and analytical methods that identify and model these TTPs. They should be based on a dynamic, computational framework that uses social and behavioral analytics to capture the adaptive TTPs of terrorists at the individual, group and network levels.

With specific respect to detecting potential attacks in the U.S., this framework should include a fundamental baseline description of our open, complex, multicultural environment. Models are needed to capture individual elements of radicalization — including detailed patterns of behavior — in every stage from group formation through dissolution.

New tools and technologies are needed to do the following in near real time:

- Recognize radicalization-related indications and warnings through social science-based pattern extraction, analysis and visualization.
- Predict culture- and adversary-based target and staging areas based upon CONUS and Outside the Continental U.S. (OCONUS) patterns of specific behaviors and TTPs.
- Prioritize intelligence, surveillance and reconnaissance (ISR) assets through formulating and testing customized hypotheses that use specific attack variables.

These behavior-detection capabilities should be flexible and scalable to ensure that they can be used by federal, state, local, tribal and territorial IED-threat responders.



## MISSION 5: Develop human tracking and locating technologies

The intelligence and law enforcement communities — including first responders — must be able to perform remote surveillance of people of interest in a lawful manner. Remote technologies should be able to monitor location and movement, determining, for example, when an individual on a watch list crosses a border, then pinpointing that individual's location to a specific address and allowing users to view that individual — and what he or she sees — in real time.



Such technologies should be nonproprietary, based on open standards and scalable to an enterprise data management system.

To improve situational awareness, remote surveillance capabilities include unmanned, self-operating, unsupervised monitoring technologies that provide high-resolution video and audio recording at locations where the frequency of incidents is generally too low to warrant permanent staffing. Such locations include schools, bridges, water supplies, prison perimeters, borders and critical infrastructures. “Intelligent” audio and video capabilities are needed to provide alerts of changes in normal patterns and events.

In the corrections environment, technologies are needed for staff and inmate identification and tracking. Remote

surveillance sensors should be able to monitor health and safety by providing duress alerts, identifying potential suicide risks and assisting officers with suicide watches. Research and development is also needed to improve devices that safely tether a noncooperative subject.

With respect to the physiological monitoring of first responders — particularly firefighters — new detection technologies would include integrated body-worn sensor suites that perform real-time health analysis and issue alarms to both wearer and command staff to reduce cardio-cerebral fatalities through early identification and mitigation.

Tactical command and control systems should be able to locate, identify and manage first responders and sensors in a single electronic map display with detailed “point and click” unit identification.

Nonterrestrial locator technologies — including airborne and satellite — are needed for mobile response, including

temporary deployments in tactical and emergency situations. Technologies should improve the tracking of subjects — including offenders when they are released to the community — who are beyond the “sight” of a satellite system. This includes when a subject is indoors, underground or outdoors when signals are blocked by structures or terrain. Currently, for example, real-time or near real-time notification of an offender’s whereabouts is limited by the availability of cellular communications. New technologies are needed to provide a two-way communications capability that can remind special-needs offenders of appointments, medication schedule or new requirements.

Tracking technologies are needed to determine the origin of explosives and bomb components in domestic IEDs. A variety of new tools are needed to improve forensic evidence investigations, such as biometrics, taggants and radio-frequency identification devices (RFIDs).



## MISSION 6:

# Develop tools and technologies to ensure infrastructure protection

A range of technologies are needed to protect the nation’s infrastructure from manmade and natural events. Highly transportable and affordable solutions are particularly needed with respect to utilities.

New tools and technologies should be able to rapidly assess damaged structures and quantify interdependencies and cascading consequences. Mitigation and recovery technologies are also needed.

Affordable blast-, fragment- and fire-resistant materials — along with low-cost strategies



—are needed to protect structures and occupants from vehicle-borne IEDs. Rapidly deployable blast-mitigation concepts for threat response and temporary protection (including decision-support systems) are needed to prevent or mitigate disruption.

Technologies are needed to reduce the damage from an IED attack — including catastrophic failure — in high-consequence infrastructures. Standards for models that predict blast effects should be able to consider the diversity and variability of construction in urban settings.





PROCESSING  
OF INFORMATION



## MISSION 7:

# Develop biometrics technologies

Biometrics technologies are needed to identify individuals — and detect false identity — in real time. Such technologies will improve the capability to verify the professional credentials of individuals in both preplanned and developing events.

Identity resolution of individuals and aliases should be noninvasive, highly reliable and allow unique characterizations to be stored in searchable, exchangeable records. Such biometric technologies include:

- Facial recognition (unique geometries of the facial structure).
- Hand printing (unique geometries of the hand skeleton).
- Fingerprinting, including electronic, contactless (without ink, paper or other hardcopy techniques) 10-print capture.
- Iris scanning (capturing and comparing unique aspects of the iris).
- Thermal scanning (imaging to determine unique thermal print).
- Physical attribute and suspicious behavior detection that is able to characterize physical attributes and detect changes, such as when an individual approaches an officer or inspection area.
- DNA, including rapid DNA testing to verify familial relationships.
- Voice stress and handwriting analysis.
- Conversation analytics.

New technologies are needed to improve capabilities in extreme conditions, including temperature. Mobile

biometrics screening devices — such as handheld, high-speed, high-fidelity 10-fingerprint capture — should be environmentally hardened, wireless and secure. Remote, standoff biometrics detection should also be able to uniquely identify individuals at a distance.



Identity resolution is critical to national security. Whether in a foreign theatre of operations, in a domestic law enforcement environment, in international waters, or at U.S. borders, the ability to positively determine the identity of a person — including passenger screening — is vital to achieving counterterrorism, law enforcement and force protection objectives. Biometrics technologies are also needed in other settings to:

- Prevent access by unauthorized people in schools, detect gang activities, identify people in secure or controlled areas, detect altered appearances, and identify and, if appropriate, authorize communications-system users.
- Process inmates in and identify visitors to corrections facilities.
- Perform employee background checks.
- Improve police officer safety and reduce costs in routine duties, such as traffic stops.
- Eliminate misidentification of innocent subjects and verify warrants.
- Track sex offenders.
- Help determine circumstances of death.

Improved capabilities are needed to confirm the identification of individuals with multiple, false and no documentation, and to increase the efficacy of queries within criminal justice databases.

## MISSION 8:

# Develop link analysis technologies

Link analysis technologies are needed to quickly resolve, in high fidelity, the relationships between people, places, things and events from large, disparate data sources, even when data or evidence is missing. Link analysis technology — sometimes called entity and relationship resolution — should be able to identify a single entity (a person, place, organization or location) from multiple, seemingly distinct entities. It should also be able to identify discrete relationships or events, such as “friend,” “attended,” “bought” or “gave to.”

Prior to resolution, data generally contain many-to-many mapping, in which multiple unique entities and relationships are identified in multiple nonunique ways. Link analysis technologies are needed to translate many-to-many mapping into one-to-many mapping, in which each instance of the same entity or relationship is associated with a unique identifier.



As theories of crime are operationalized into new link analysis tools, problems that are common to other systems — data-entry errors, people with similar or identical names, and other sources of benign errors — will have to be overcome. Such technologies are also needed to detect deceptive information and find anomalies that can complicate the resolution process.

Missing data is another challenge for link analysis tools. Because most current methods of analysis assume that networks are complete, they do not account for network evolution or identify missing evidence. New link analysis technologies — including social network analysis, such as Facebook and LinkedIn, which describe the relationships between individuals by synthesizing massive amounts of data — should consider missing nodes and edges and be able to adapt to the absence of temporal and spatial context.

## MISSION 9:

# Develop language translation capabilities

An analyst reviewing information in a foreign language should be able to isolate the most important data, ensuring that they do not get lost in information overload. This requires technologies that provide translation, transcription, speech recognition and automated filtering of written text and speech from audio and video sources.

The first step in translation is identification of the language, which can be complicated by various factors, including the type of data source (for example, electronic data stream, handwritten text, spoken language). Other factors can also complicate the translation process, such as

multiple speakers, background noise, misspellings, jargon, dialects, code words, abbreviations and poor handwriting.

Once the translation technology identifies the foreign language, it should allow the analyst make data queries in

English to extract key information, such as names, places, keywords and concepts.

Finally, foreign language translation technologies should be integrated with other tools that perform information extraction, fusion and summarization.



## MISSION 10:

# Develop digital forensics tools and technologies to improve the processing of evidentiary data and information

Digital forensics technologies are needed to process evidence from digital devices and to prevent, investigate and solve cybercrime. Currently, the acquisition of large digital evidence data sets is time-consuming, decreasing productivity and increasing case backlogs.

There are hundreds of mobile devices on the market, with more models introduced every month; there are also mobile devices that are no longer available commercially but are still in use. Currently, only a portion of these devices can be thoroughly examined for digital evidence.

Digital forensics investigative tools — including small-scale portable devices for first responders — encompass:

- Digital analytics.
- Forensic tools that identify and interpret all email formats (Outlook, LotusNotes, etc).
- Live analysis tools.
- Person to person (P2P) forensic tools that identify shared and transferred files or connections.

- Investigative tools for decentralized P2P file sharing.
- Imaging tools for networks and network-attached devices.



Technologies are needed to reverse-engineer and investigate criminal activities using The Onion Router (TOR), an Internet anonymity application that allows users to hide their identity and conduct untraceable financial transactions online.

More effective, less expensive tools are needed to recover data from damaged hard

drives. Generally, data on nonfunctioning hard drives or stored for a prolonged period of time are susceptible to mechanical failure. Currently available commercial data recovery options are expensive and can compromise the forensic integrity and chain of custody of digital evidence.

With increased availability (and lower cost) of storage space come more files that can be used legally and for nefarious purposes. More files require more investigative time. Faster tools with higher capacity storage are needed

to help investigators analyze digital evidence in forensic investigations.

Finally, tools and methods are needed to detect data-hiding and encryption, such as sector hashing and carving for partial multimedia files.

## MISSION 11:

# Develop technologies to assess and evaluate chemical and biological defense

Tools and technologies are needed to assess and evaluate the nation's defenses against chemical and biological attacks, including integrated CBRNE risk assessment. Technologies should be able to assess all the critical elements of chemical and biological defense strategies, including threat awareness, prevention and protection, surveillance and detection, and response and recovery.

With respect to biodefense, analytical tools are needed to improve biological surveillance by accessing and integrating diverse data from multiple domains.

New technologies should be able to assess, render safe and neutralize explosive threats, including those that protect against person- and vehicle-borne explosives.

New incident characterization technologies are needed to improve response and restoration, particularly fully integrated tools that support surveillance, detection, incident characterization and response systems. This also

encompasses a systems approach to characterizing the extent of contamination and the restoration (decontamination following the release of a chemical or biological agent) of a large urban center, including fixed (such as buildings) and moving (vehicles) infrastructure.

To help the first-responder community respond to public health issues, tools are needed to independently evaluate and validate commercially developed methodologies that address the full

spectrum of biological agents. Technologies also are needed to improve chemical and biological forensic analyses.





ANALYSIS  
OF INFORMATION



## MISSION 12:

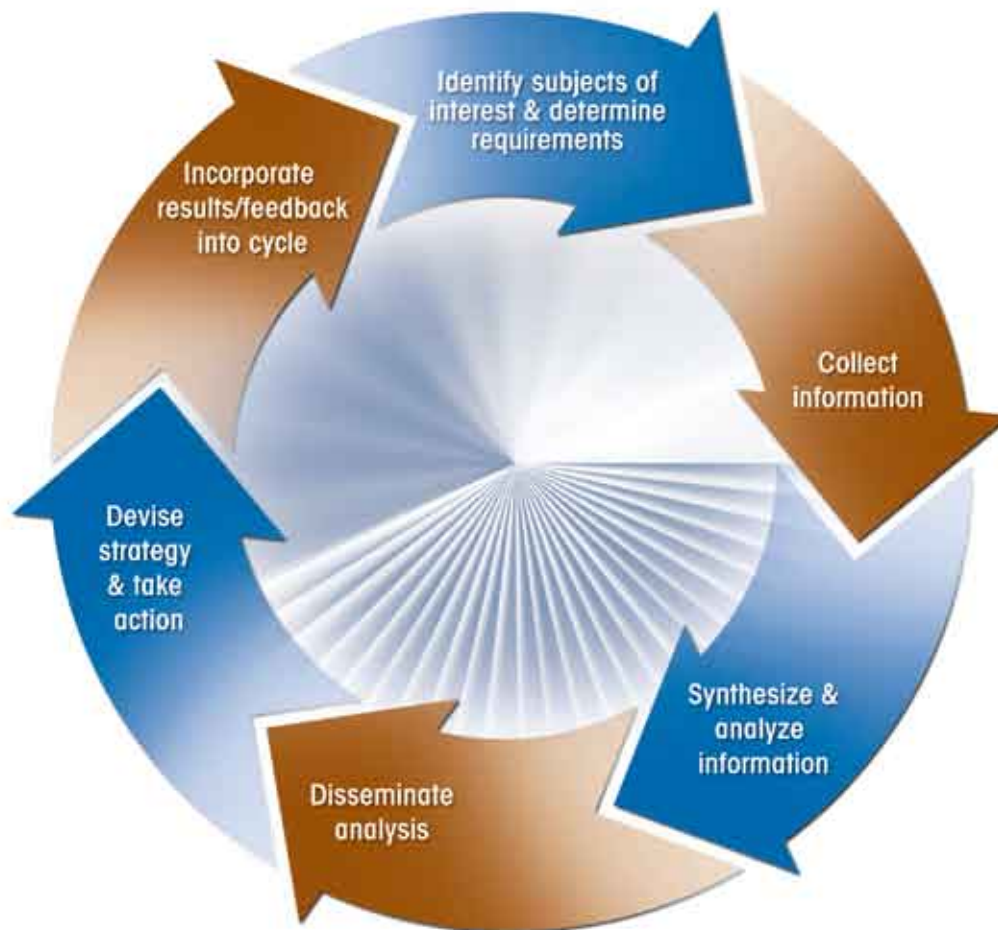
# Develop information analysis technologies

Information analysis technologies manage and integrate data from disparate sources to reveal fragmented, inconsistent or contradictory information. These technologies must be able to rapidly view entire scenes, then fuse, evaluate, compare and analyze information, thus allowing the analyst to focus on preparing products that follow the intelligence cycle (see figure).

Among such technologies are:

- Tools that automatically extract and resolve entities and relationships from a variety of multilingual text documents — manuals, textbooks, dictionaries, reports, Web pages and messages — into application-specific, problem-solving modules tailored to a particular strategy.

## The Intelligence Cycle



- Presentation tools that summarize information about emerging situations and offer initial response options and justifications.
- Automated metadata extraction and mapping that facilitate the addition of other data sources.
- Inference and reasoning procedures that use any (or all) of the data in a knowledge base to support or refute logical statements.
- Analysis and decision-making tools that assist in the development and implementation of border security initiatives.

Information analysis technologies allow agencies that are not co-located to share information in real time. Such technologies must support command center operations (such as fusion centers), allowing personnel to compare tasking and location of blue forces to new events and recommend courses of action. Information analysis technologies must be able to view entire scenes and provide alerts of anomalous and illegal activity.

Such technologies also must be able to visually display raw and derived data in multiple, dynamic and detailed ways. Because people process information and learn in different ways, visual displays of highly aggregated data should be able to offer an enhanced “big picture” of a developing situation. To improve assessment of a situation (including the identification of potential targets and even intentions), analysis charts should be able to display a situation pictorially.



Tools and technologies are needed to provide systematic collection and analysis of information in near real time, including:

- Intuitive and self-supporting walk-up interfaces.
- Geospatial representation and selective layering.
- Multiresolution displays.
- Cluster analysis.
- Timeline analysis.
- Link association analysis.
- Telephone/e-mail analysis.
- Attribute-specific highlighting.
- “What-if” analysis.
- 3-D visualization that geocodes and maps large buildings, including those with no electronic computer-aided design files.

Spatial data analysis visualization tools should be able to examine information in ways that have been hypothesized but not yet developed to better exploit databases containing crime data. Because analysts do not have the time to perform the ingest tasks often associated with advanced visualizations, new technologies are needed to quickly load data for viewing in a meaningful, dynamic way.

Visual displays also must support “drill-down,” in which a highly aggregated display provides the big picture, but allows the analyst to drill down to details. Tools are also needed to help analysts present simple, but robust, visual summaries to decision-makers.



## MISSION 13:

# Develop automated organizational structures recognition technologies

Organizational structures recognition describes entities — people, places, things, times — and the relationships between them, such as “met,” “married,” “occupied,” “after.” Automated organizational structures recognition technologies are needed to search massive amounts of data to identify and analyze the membership and structure of highly structured organizations as they transform into small, isolated groups that may be indirectly influenced by the larger organization.



New organizational structures recognition technologies would also include social network analysis, which looks

at the relationships — including geographic location — between people, groups and organizations.

Such tools and technologies will allow analysts to recognize and understand groups (including their extensions and divisions) that are completely disconnected from previously known groups. These new technologies will characterize the internal structure of an organization — its leaders and core and peripheral members — and liaisons between organizations,

including any overlap of membership, geospatial relationships and changes in these features over time.



## MISSION 14:

# Develop geospatial technologies

Geospatial technologies are needed to improve situational awareness. Such technologies — including the automated mapping of threats to critical infrastructure vulnerabilities — should:

- Be based on assessments of threat-stream information, including the possible means, mode, geographical location and timing of a potential attack.
- Identify infrastructure elements that are vulnerable to identified threats.
- Be capable of retrieving information about particular infrastructure elements.

Specific threat-stream data should be identified, consolidated and mapped onto known vulnerabilities that could become terrorist targets. Although such threat maps currently exist, they depend on the manual input of data — therefore, new technologies are needed to link threat-stream and vulnerability data onto geospatial mapping.

Many of these technologies are of critical importance to first responders, including impact analysis and 3-D locator tools that provide “x/y/z” accuracy of better than one meter in a multilevel building to allow incident commanders to rapidly track and deploy or redeploy personnel. These types of analyses can present challenges

— for example, a private sector entity’s concerns regarding the proprietary nature of specific infrastructure data — that automated collection mechanisms could help mitigate.

Tools are also needed to analyze GPS monitoring data for criminal offenders. This includes technologies that identify patterns and anomalies in an individual offender’s behavior and that can also correlate these data to groups of offenders.

Finally, new technologies are needed to ensure integrated modeling, mapping and simulation capabilities. This includes a real-time, stimulation-based training tool that



analyzes disaster response and recovery operations, tactics, techniques, plans and procedures.

Modeling and simulation tools are needed to respond to “what if” scenarios, focusing on immersive visualization in a decision-making environment. The goal of such technologies is to balance the complexity of real-world phenomena, including multiple scenarios, with clear, transparent modeling. Visual software applications should offer a display of conclusions

and potential policy implications and could include system dynamics, geographic information systems, data mining, statistical analysis and 3-D modeling applications.



## MISSION 15:

# Develop predictive analysis technologies, particularly geared to anomaly detection

Predictive analysis technologies are needed to detect anomalies in the pattern of a “transaction.” A transaction is an activity — related, for example, to communications, finances, or the movement of goods and people — that may be of interest to the intelligence, law enforcement and homeland security communities. Currently, analysts use a variety of risk-management principles and rules-based algorithms to determine when further inspection of a transaction is warranted.

The underlying principles of predictive analytics — which includes the statistical and structural analysis of historical data — have been used by the private sector for decades; credit card companies, for example, use predictive analytics to identify retail transactions that are unusual for

a customer. In law enforcement, this type of analytics is sometimes called “predictive policing.”

With respect to protecting cargo shipments and U.S. borders, automatic target recognition technologies should be nondestructive, using imagery detection, for example, to inspect hidden or closed compartments for contraband, stowaways and security threats.

Predictive analysis technologies are needed to look for anomalies in patterns of shipping and data handling. Particular factors or “attributes” that should be analyzed in a cargo transaction, for example, would include the type of commodity, manufacturer, country of origin, country of export, shipper, exporter, importer, broker, port of export, port of import, dates and transit points. With

respect to passenger transactions, attributes would include name, citizenship, place of birth, passport number, port of departure, port of arrival, airline and flight number.

## Deception detection

Predictive analysis technologies also would include the detection of deception. “Deception” encompasses many behaviors that are used in a variety of enterprises, including terrorist, criminal, and terrorist and criminal.

New deception technologies should be able to recognize and predict:

- Purposeful withholding of truthful information (concealment).
- Substitution of false or truthful information (falsification) regarding past behavior or future behavior (intent).
- Patterns of deceptive actions that may suggest terrorist activity.
- Single instances of deceptive behavior.

These technologies should be capable of operating in a multilevel security- and service-oriented network.



They also should be able to detect both retrospective and real-time deception. This includes analyzing data from governmental and commercial transaction-processing systems and could extend to noninvasive collection and analysis of physiological data obtained during real-time detection of deception.

Finally, deception detection technologies should be able to discern when information is incorrect due to inadvertent errors in data entry, data transmission, or operator, entity or relationship resolution.

## Incident management

First responders need predictive analysis tools and technologies to predict criminal and terrorist activities. This includes management enterprise systems that enhance situational awareness in critical incidents by providing timely information — regarding available and anticipated human and material resources, including transportation — in rapidly changing situations with shifting priorities.

Incident management technologies include the use of geospatial data to create a seamless system between federal, state and local first responders with the goal of establishing virtual continuity-of-operations capabilities when key infrastructures and facilities are unavailable.





DISSEMINATION  
OF INFORMATION

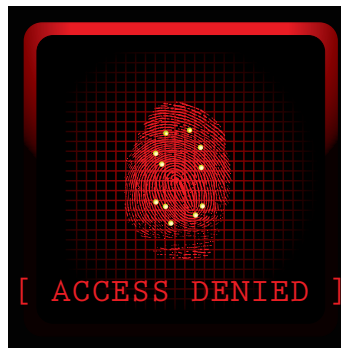


## MISSION 16:

# Develop technologies to improve access control

Technologies are needed to manage identities, rights and authorities across networks, according to each source's policies regarding user identification, privacy, roles, U.S. Persons law, security classification and access privileges. Such tools and technologies also require standards that enable external identity adjudication.

Currently, analysts must log on to each data source separately, which is an inefficient process. Although much has



been done in the past — through integration of networks and personnel among agencies — new tools are needed to allow global, secure access to multiple data sources with a single sign-on.

Such tools and technologies also should be able to perform audits, determining, for example, which resources and records have been accessed by which users (user ID) and the frequency of access, including date and time stamp.

## MISSION 17:

# Develop technologies to improve the access to and integration of information

Analysts have access to numerous sources of counter-terrorism data, such as law enforcement and intelligence community networks that operate at various security levels. Currently, each source must be accessed separately to make queries, and the search results must be manually integrated into yet another production environment.

New tools and technologies are therefore needed to accesses disparate data from many repositories, applications and networks, and then rapidly and seamlessly integrate the

data into a coherent analysis or visualization of emerging threats.

The challenge is not only to make information accessible, but to present it in a simplified, easy-to-navigate format that is acceptable to the security policy boards of each contributing network. Development of a single host network environment is needed to authenticate the user, transfer data across networks and security levels, and create a single product for analysis.

## MISSION 18:

# Develop technologies to disseminate and share information

Technologies are needed to automatically distribute a wide variety of structured, unstructured and streaming data, such as product information, actionable intelligence, law enforcement bulletins and unclassified intelligence. New dissemination tools and technologies are needed to improve disaster preparedness and situational awareness and support decision-making, both horizontally across federal law enforcement and intelligence agencies and vertically through federal, state, local and tribal partners.

Automated, dynamic, real-time data processing and visualization capabilities are needed to improve situational awareness. This would include the development of information-sharing protocols between jurisdictions regarding suspicious activities and persons.

New technologies should support a common collaborative environment (CCE) for the intelligence community



and its partners when they are using diverse networks with various security levels. A CCE is a force multiplier, enabling users to locate, share and analyze information within a single, secure, multilevel virtual environment. CCE technologies should:

- Enable users to make a “call for assistance” that prompts the rapid formation of communities of interest (COIs), bringing experts, analytical tools and data into a single virtual environment to address an issue.
- Tailor presentation methods to individual users while safeguarding the system and ensuring user and COI privileges and authorizations regarding sensitive data.
- Allow the addition or removal of analysts, analysis tools and data sets throughout a COI lifecycle.

## MISSION 19:

# Develop technologies to disperse information for public welfare

New technologies are needed to improve situational awareness — including the management of critical resources — at all levels of government. Such tools and technologies should increase the ability of local officials to

communicate clear, credible information — for example, warnings and instructions regarding an IED — to the public. They must provide emergency managers with seamless data, voice and video information.

To achieve these goals, new tools and technologies are needed to:

- Standardize, pilot and evaluate wireless broadband data technologies and applications.
- Develop message interface standards for emergency information sharing and data exchange, particularly regarding eXtensible Markup Language (XML) for communications devices and software systems.
- Develop testing and evaluation procedures for multiband radios for civilian use in emergency communications and day-to-day operations.
- Provide seamless access — through a unified communications device — to voice and data networks and identify and refine potential platforms, interfaces and applications.
- Perform interoperability compliance testing on emergency response communications devices and systems, including the development and implementation of an interoperability compliance assessment program.

Tools and technologies also are needed to create ad hoc and mesh networks that link local, state and federal personnel in emergency situations.



## MISSION 20: Develop technologies to improve cybersecurity

Technologies are needed to improve protection of the nation's cyber infrastructure. Such technologies would address usability and security issues, including the development of:

- Internet protocols, including standard security methods.
- Models that understand Internet topography and can measure the effects of cyberattacks, particularly security and risk in IT infrastructure components.
- Comprehensive next-generation network models, particularly those that apply to the design, construction and evaluation of IT systems.



- Analytical techniques for security across the IT system-engineering lifecycle, particularly those that detect, visualize and measure system security.

- Process control systems security, including improving the assessment of wireless communications and system vulnerability.

Insider-threat detection models and mitigation technologies are also needed to increase the ability and reduce the cost of detecting unauthorized insiders.

Finally, new tools and technologies are needed to perform software testing and vulnerability analysis, particularly building, testing and analyzing source and binary forms of software in realistic operational environments.







[WWW.ICAHST.ORG](http://WWW.ICAHST.ORG)

