

ICAHST Long-Term Technology Needs

Collection of Information

MISSION 1: Develop methods and technologies to prepare data.

New tools and technologies must be developed 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% accuracy for named entities, events, relationships, and temporal and spatial factors.

For example, technologies that support information-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 is 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 descript, 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 information-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 information-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, multi-lingual, scientific and technical issues surrounding an event or location.

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

New technologies and methods must be developed 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. To ensure the protection of U.S. citizen Data storage also must ensure the protection of U.S. citizen personal data and provide 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 must:

- 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 therefore 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 must 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 must be developed that 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 non-lethal 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
- 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 — must 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 non-threatening agents without interfering with the stream of commerce.

Technologies must 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 improvised explosive devices (IEDs), research is needed to:

- improve the capability of detecting and defeating vehicle-borne improvised explosive devices (VBIED), particularly, non-explosive and standoff-defeat technologies; this includes non-intrusive screening to interrogate a vehicle at 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
- mark explosives material

Personnel-safe, handheld devices — containing, when required, both sensor and active source — must allow the non-intrusive 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 must be improved. Currently, for example, data that is 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 — is not collected.

In addition to developing non-intrusive inspection tools and technologies for maritime cargo and containers, we must 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 must be developed to improve penetration, resolution, throughput, contrast sensitivity, reliability, mobility and interoperability — including integration with future Automated Target Recognition 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 explosives 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 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 must be developed to increase detection rates in screening people for explosives and weapons, while minimizing disruption to passenger flow. This includes improved screening and examination by non-intrusive 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 system-wide solutions, must also increase the accuracy (and reduce the time and cost) of detecting insider threats and mitigating any harm caused by an unauthorized insider.

Technologies must be developed that quickly identify the origin of gunfire, but also classify the type of a weapon fired.

Finally, continued information technology research and development is 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 is 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 non-trivial data is detected.

Behavior Detection

Technologies — in particular, non-invasive behavioral sensors — are needed to detect deception or hostile intent in real-time. This requires non-invasive sensors and analytical methods that identify and model the human precursors of IED threats and terrorist activities within CONUS using unstructured data and novel computational models.

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. Remote technologies must monitor location and movement, determining, for example, when an individual on a watch list crosses a border, then pinpoints their location to a specific address and allows users to view them — and what they see — in real time.

Such technologies should be non-proprietary, 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 must 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 must 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 non-cooperative 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 must be able to locate, identify and manage first responders and sensors in a single electronic map display with detailed “point and click” unit identification.

Non-terrestrial locator technologies — including airborne and satellite — are needed for mobile response, including temporary deployments in tactical and emergency situations. Technologies must 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 must also provide a two-way communications capability that can remind special-needs offenders of appointments, medication schedule or new requirements.

Tracking technologies must be able to determine the origin of explosives and bomb components in domestic improvised explosive devices. 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 man-made and natural events. Highly transportable and affordable solutions are particularly needed with respect to utilities.

New tools and technologies must 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 — must be developed to protect structures and occupants from vehicle-borne improvised explosive devices (IED). Rapidly deployable blast-mitigation concepts for threat response and temporary protection must be developed, including decision-support systems that prevent or mitigate disruption.

Technologies are needed to reduce the damage from an IED attack — including catastrophic failure — in high-consequence infrastructures. Techniques and tools must stabilize damaged structures and prevent their collapse. Standards for models that predict blast effects should consider the diversity and variability of construction in urban settings.

Processing of Information

MISSION 7: Develop biometrics technologies.

Biometrics technologies must be able to identify individuals — and detect false identity — in real time. Such technologies must also improve the capability to verify the professional credentials of individuals in both pre-planned and developing events.

Identity resolution of individuals and aliases must be non-invasive, 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)
- fingerprint, 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 attributes and suspicious behavior detection; characterizing physical attributes and detecting changes, such as when an individual approaches an officer or inspection area, and to more intensively train security officials in protocols and procedures that will allow them to better identify people who merit additional intensive screening
- DNA, including rapid DNA testing to verify familial relationships
- voice and handwriting stress analysis
- conversation analytics

Although versions of these technologies currently exist, they must be improved to respond to extreme working conditions, including temperature. Mobile biometrics screening devices — such as handheld, high-speed, high-fidelity 10-fingerprint-capture — must be environmentally hardened, wireless and secure. Remote, standoff biometrics detection must also be able to uniquely identify individuals at a distance.

Identity resolution is critical to national security. Whether in a foreign theatre of operations, domestic law enforcement, international waters, or at U.S. borders — including passenger screening — the ability to positively determine the identity of a person is vital to achieving counter-terrorism, law enforcement and force protection objectives. Biometrics technologies must also be capable of being used in other settings, such as:

- preventing access by unauthorized people in schools, detecting gang activities, identifying people in secure or controlled areas, detecting altered appearances, and identifying and, if appropriate, authorizing communications-system users
- processing inmates in and identifying visitors to corrections facilities
- performing employee background checks

- improving police officer safety and reducing costs in routine duties, such as traffic stops, eliminating misidentification of innocent subjects, verifying warrants, and sex offender tracking
- making identifications in determining 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 Information System (CJIS) databases.

MISSION 8: Develop link analysis technologies.

Link analysis technology — sometimes called entity and relationship resolution — must quickly, and in high-fidelity, resolve the relationships between people, places, things and events from large, disparate data sources, even when data or evidence is missing. Entity-resolution technology must be able to identify a single entity — person, place, organization or location — from multiple, seemingly distinct entities. Relationship-resolution tools must 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 non-unique ways. Link analysis technologies 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 — must be overcome. Such technologies must also detect deceptive information and find anomalies that can complicate the resolution process.

Missing data is another challenge for link analysis tools and technologies. Because most current methods of analysis assume that networks are complete, they do not account for network evolution or missing evidence. New link analysis technologies — including social network analysis such as Facebook and LinkedIn, which describe the relationships between individuals by synthesizing relationships from massive amounts of data — must 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 must be able to isolate the most important data, ensuring that it does 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 a number of 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 must allow the analyst to query the data using English to extract key information, such as names, places, keywords and concepts.

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

MISSION 10: Develop digital forensics tools and technologies that improve the processing of evidentiary data and information.

Digital forensics technologies must be developed to process evidence from digital devices and to prevent, investigate and solve cyber-crime. Currently, the acquisition of large digital evidence data sets is time-consuming, which reduces productivity and increases case backlogs.

There are nearly 500 models 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 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
- P2P forensic tools that identify shared or 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 while online.

More effective, less expensive tools are needed to recover data from damaged hard drives. Generally, data on a non-functioning hard drives or those stored for a prolonged period of time are susceptible to mechanical failure. Currently, commercial data recovery options available today are expensive and may compromise the forensic integrity and chain of custody of digital evidence.

With the increased availability and lower cost of massive storage space brings the onset of an increased number of files, for both every day legal use as well as nefarious purposes.

The increased number of files means additional time required to conduct an investigation. Faster tools with higher capacity storage are required by investigators to effectively and efficiently conduct their forensic investigation on a suspect's computer.

Finally, tools and methods also must be developed that allow for the discovery of 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 CBRN Risk Assessment. Technologies must 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. Such technologies must be used proactively to assess the potential consequences of attacks on the nation's population, agriculture and chemical facilities and other critical infrastructure.

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

New technologies sought to assess, render safe, and neutralize explosive threats, particularly tools 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 need also encompasses a systems approach to characterizing the extent of contamination and the restoration (decontamination) of a large urban center, including fixed (such as buildings) and moving (vehicles) infrastructure, following the release of a chemical or biological agent.

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, or assays. Technologies also must be developed that 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 intelligence products. <<INSERT INTELLIGENCE CYCLE GRAPHIC WITHIN THIS TECHNOLOGY NEED>>

Among such technologies are:

- tools that automatically extract and resolve entities and relationships from a variety of multi-lingual text documents — manuals, textbooks, dictionaries, reports, web pages, messages and other informal documentation — into application-specific problem-solving modules tailored to a particular strategy
- presentation tools that summarize information about emerging situations and uncertainties and offer initial response options, along with justifications
- automated meta-data extraction and mapping that facilitates the addition of supplementary data sources
- inference and reasoning procedures that are capable of using any or all of the data in a knowledge base to support or refute logical statements
- analysis and decision-making tools that ensure 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. They must be capable of viewing entire scenes and providing alerts about anomalous and illegal activity.

In addition, such technologies must be able to visually display raw and derived data in multiple, dynamic and detailed ways. Because people process information and learn in various ways, visual displays of highly aggregated data offer an enhanced “big picture” of a developing situation. Analysis charts display a situation pictorially to better assess a situation and potentially determine future targets—or even intentions. Additional technologies and tools are needed in this area.

These tools must provide systematic collection and analysis of information in near-real-time. Such technologies include:

- intuitive and self-supporting walk-through interfaces
- geospatial representation and selective layering
- multi-resolution displays
- cluster analysis
- timeline analysis
- link association analysis
- telephone/email analysis
- attribute-specific highlighting
- ‘what-if’ analysis

- 3-D visualization tools and technologies that geo-code and map large buildings, including those with no electronic CAD files

Spatial data analysis visualization tools must examine information in ways that have been hypothesized but not yet developed and that 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 must 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 uses data that describes entities — people, places, things, times — and the relationships between them, such as “met,” “married,” “occupied,” “after.” These technologies 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 are indirectly influenced by the larger organization.

New organizational structures recognition tools and technologies will allow analysts to recognize and understand groups, such as 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, geo-spatial relationships and the changes in these features over time.

MISSION 14: Develop geospatial technologies.

Geospatial technologies must be developed 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 the identified threats
- provide capability to retrieve information about particular infrastructure elements

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

Such technologies are of critical importance to first responders. They include impact analysis and 3-D locator tools that provide “x/y/z” accuracy of better than 1 meter in a multilevel

building to allow incident commanders to rapidly track and deploy or redeploy first responders.

These types of analysis 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.

Social network analysis technologies are needed that analyze the relationships — including geographic location — between people, groups and organizations.

Tools are also desired to analyze GPS-monitoring data from criminal offenders. This includes technologies that identify patterns and anomalies in an individual offender's behavior and that can also correlate this data to groups of offenders.

Finally, new technologies must 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, which respond to "what if" scenarios, should focus on immersive visualization in a decision-making environment. The goal of such technologies is to balance the complexity of real-world phenomenon including multiple scenarios with clear, transparent modeling. Visual software applications include system-dynamics, geographic information systems, data mining, statistical analysis and 3-D modeling applications, resulting in a visual display of conclusions and potential policy implications.

MISSION 15: Develop predictive analysis technologies, particularly geared to anomaly detection.

Predictive analysis technologies that detect an anomaly in the pattern of a "transaction" must be developed. A transaction is an activity — related 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 for decades in the private sector; credit card companies, for example, use these principles to identify retail transactions that are unusual for a customer. In law enforcement, this type of analytics is often called "predictive policing."

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

Predictive analysis technologies also look for anomalies in patterns of shipping and data-handling. Particular factors or "attributes" to be analyzed in a cargo transaction include the 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 include name, citizenship, place of birth, passport number, port of departure, port of arrival, airline and flight number.

Deception Detection

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

Deception technologies must 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 be elements of terrorist activity
- single instances of deceptive behavior

These technologies — which must be capable of operating in a multi-level, security- and service-oriented network — must detect both retrospective and real-time deception. This includes analyzing data from governmental and commercial transaction-processing systems and could extend to non-invasive collection and analysis of physiological data obtained during real-time detection of deception and malicious intent.

Finally, deception detection technologies must be able to distinguish the accidental supplying of incorrect information through data entry, data transmission, operator, entity and relationship resolution, and system errors.

Incident Management

First responders need these 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.

Such incident management tools 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 that improve incident management 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 must be developed that allow global, secure access to multiple data sources with a single sign-on.

Such tools and technologies must also 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, particularly law enforcement and intelligence community networks that operate at various security levels. However, each source must be accessed separately to make queries and the search results must be manually integrated into yet another production environment.

Technology must be developed that accesses disparate data from many repositories, applications and networks, and then rapidly and seamlessly integrates it into a coherent analysis or visualization of emerging threats.

The challenge is to not only 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. The solution is the development of a single host network environment that is capable of authenticating the user, transferring data across networks and security levels, and creating a single product for analysis.

MISSION 18: Develop technologies to disseminate and share information.

Technologies must automatically distribute a wide variety of structured, unstructured and streaming data, such as product information, actionable intelligence, law enforcement bulletins and unclassified intelligence. Dissemination tools 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 also needed to improve situational awareness. This would include the development of information-sharing protocols between jurisdictions regarding suspicious activities and persons.

New technologies must 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, multi-level virtual environment. Such CCE technologies must:

- enable users to make a “call for assistance” that prompts the rapid formation of communities of interest (COI), bringing experts, analytical tools and data into a single virtual environment to address an issue
- tailor presentation methods to individual users, while also 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 that disperse information for public welfare.

New technologies must improve situational awareness — including the management of critical resources — at all levels of government. Such tools and technologies must enhance the ability of local officials to communicate clear, credible information — such as warnings and instructions regarding an improvised explosive device — to the public. They must provide emergency managers with seamless data, voice and video information.

To achieve these goals, we must:

- standardize, pilot and evaluate wireless broadband data technologies and applications
- develop message interface standards for emergency-information sharing and data exchange, particularly eXtensible Markup Language (XML) standards for communications devices and software systems
- develop test procedures, including the testing and evaluation of multi-band 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

Such technologies also include the development of ad-hoc and mesh networks to link local, state and federal personnel in emergency situations.

MISSION 20: Develop technologies to improve cyber security.

Technologies are needed to improve the 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 cyber attacks, 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 (PCS) 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.