



Photo courtesy of the Department for Homeland Security.

Protecting our Nations

In September 2001, the world changed forever when the World Trade Centre was destroyed when two planes, flown by terrorists, brought each tower down. The event killed nearly three thousand people. The reaction was to dramatically increase Homeland Security against this new and terrifying enemy. Helen Jameson looks at the role that technology plays in this vital network of protection.

A new and deadly enemy was revealed to the world in the aftermath of the 9/11 terrorist attacks – Al Qaeda. There have always been terrorist attacks going way back into history, but this was a new, sinister and unpredictable network - difficult to track, to locate and to defeat. We now find ourselves being told that this group may be at its strongest since the devastation of 9/11. We have all witnessed the aftermath of bombings in London, in Bali, the Yemen, Madrid, Istanbul and, as a result of the group's activities, we have all been much more vigilant than before.

Now imagine a government's role in keeping their country safe from harm and what that entails with the plethora of agencies under their umbrella. It's an incredible task. When we think of homeland security, terrorism is the principal threat that comes to mind but it also embraces a series of aspects including:

- Emergency preparedness;
- Domestic intelligence;
- Protection of critical infrastructure;
- Border security;
- Transportation security;
- Biodefence;
- Detection of radioactive materials; and
- Next generation security technological research.

Homeland security is a national effort by all levels of a government to counter threats that could potentially cause harm to the country whether they are inflicted by man or nature or even an external force. Information Communications Technology (ICT) is playing an enormous and hugely significant role in the battle to keep our seas,



ports, airports, hospitals, communities, transportation - and everything else - safe. Communications play probably the most important role within the mandate put down by Homeland Security and the interoperability of communications systems and equipment used by each department involved is essential. They must be able to communicate with each other both internally and externally with access to information as and when it is required at a moment's notice. Correct decisions must be made quickly and they must be informed. Here again, communications are of great importance.

TETRA – public security or threat to public health?

TETRA or Terrestrial Trunked Radio is a digital trunked mobile radio standard developed by the European Telecommunications Standards Institute (ETSI) to meet the specific needs of professional mobile radio users such as those in the domain of public safety (police, fire departments), transportation, utilities, government agencies, military, commercial and industrial and oil and gas, for example. Mobile networks are of paramount importance to these types of users but, at the same time, they cannot provide the increased promise of security that is required by such users who often disseminate sensitive information, and the analogue networks cannot provide the added functionality that is so often required in this day and age. Enter TETRA. TETRA allows users to communicate outside of these public mobile-radio networks.

Interoperable

TETRA technology has been developed to be fully interoperable so that the network may be used in conjunction with different radio terminals built by different manufacturers, therefore promoting open standards (TETRA is supported by many manufacturers) and giving the user a wider choice of terminal. The TETRA Memorandum of Understanding (MoU) Association developed their Interoperability Certification Process to enable a truly open multi-vendor market for TETRA equipment and systems thus enabling fast development of new product models and, in turn, greater competition. It also opens up a wider, accessible market with faster take-up and potential for investment.

What are the benefits of using TETRA?

The core technologies used within TETRA are digital, trunking and Time Division Multiple Access (TDMA). Let's look at what each technology offers:

- **Digital** – In the 21st Century, everything is going digital. The migration from analogue to digital is already occurring everywhere we look. Digital can provide advantages over analogue in terms of voice quality, Radio Frequency (RF) coverage, it can offer non-voice services and also offers enhanced security and lower cost.
- **Trunking** – Trunking provides spectrum efficiency due to its automatic and dynamic assignment of a small number of communications channels over a large number of users. The trunking system will also support more radio users than a conventional system thus reducing pressure on Private Mobile Radio (PMR) spectrum demands. The principal feature that users of the new system wish to retain is the 'all informed net' operation with push to talk capability. Trunking utilises a control channel that handles all call requests. Its automatic call handover system takes away the need for manual channel selection. In addition, the automatic and dynamic assignment of a small number of channels among a large number of users means that an equal quality of service is available to all users on the system. From a security point of view, the dynamic and random allocation of channels makes it much more difficult for eavesdroppers to monitor conversations and any cases of abuse may be kept to a minimum as the identity of all users and the time and duration of calls is known and can be traced back to the origin.
- **TDMA** – Four time slot TDMA was adopted by TETRA as it offered the best solution to balance the cost of equipment with that of supporting the services and facilities required by its user organisations for a medium to high capacity network, providing single site local RF coverage and /or multiple site wide area coverage. TDMA provides four independent communications channels in a 25 kHz bandwidth channel making it twice as

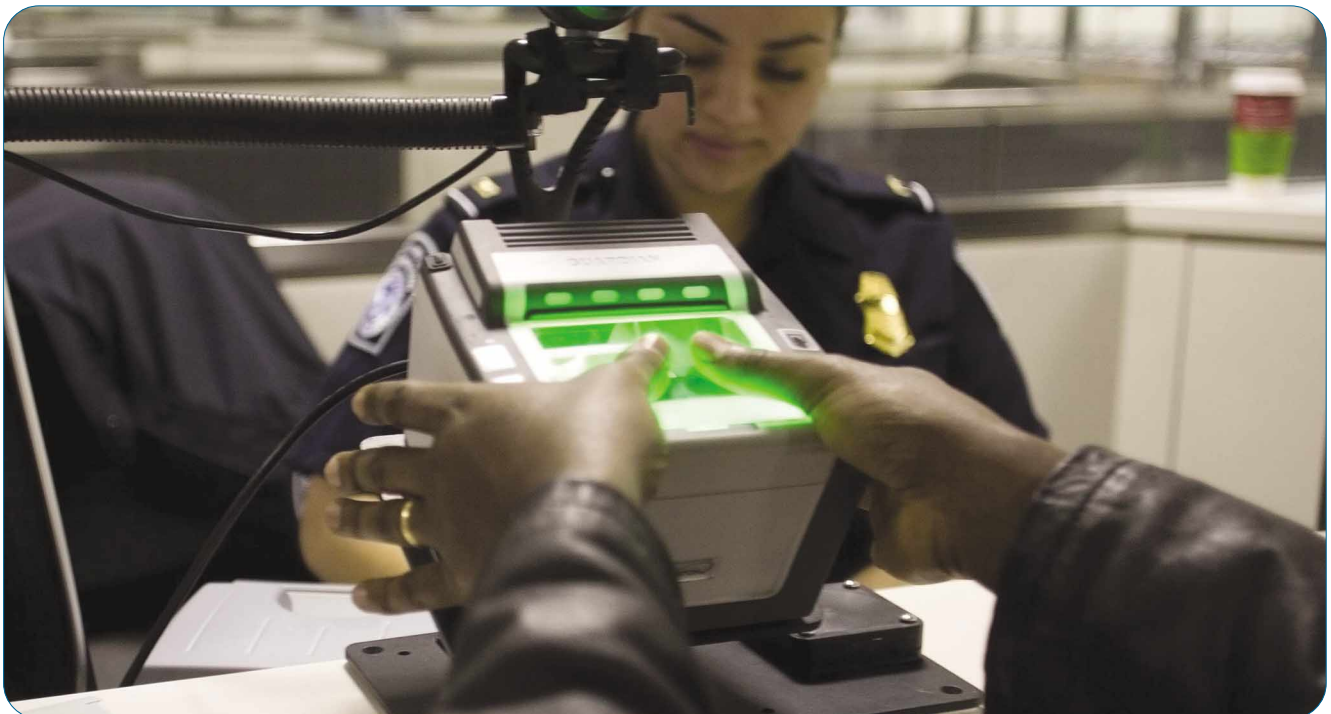


Photo courtesy of the Department for Homeland Security.



FBI awards Lockheed Martin next generation identification program

The Federal Bureau of Investigation (FBI) awarded Lockheed Martin a ten-year, \$1 billion contract to develop and maintain the Bureau's Next Generation Identification (NGI) system, a multi-modal, state-of-the-art biometrics system for use by state, local and federal authorities.

"We were proud to collaborate with the FBI on the Integrated Automated Fingerprint Identification System, the largest system in the world of its type," said Judy Marks, President, Lockheed Martin Transportation and Security Solutions. "We're tremendously pleased to partner with the agency once again to deliver the next quantum leap in capability."

The NGI system will expand fingerprint capacity, doubling the size of the current database, and will now also include palm prints, iris and facial recognition capabilities. Additionally, the system requires a significant degree of technical flexibility in order to accommodate other biometric modalities that may mature and become important to law enforcement efforts in the future.

"Together, our team brought to bear all the elements the FBI required," said Carlaine Blizzard, Vice President of Secure Enterprise Solutions, Lockheed Martin Transportation and Security Solutions. "We offered the Bureau vitally important flexibility – particularly as the agency's mission has expanded beyond traditional law enforcement to include counter-terrorism efforts."

The Lockheed Martin-led team includes Accenture, BAE Systems Information Technology Inc., Global Science & Technology (GST), Innovative Management & Technology Services (IMTS), Platinum Solutions and the National Center for State Courts (NCSC).

Lockheed Martin will provide program management and oversight as well as biometric and large systems development and integration expertise. Accenture's responsibilities will include interoperability and change management; BAE Systems Information Technology will work on external interface requirements engineering, as well as security design.

GST and IMTS, both West Virginia small businesses with a long history of working with Lockheed Martin on the IAFIS program, will provide important program continuity in addition to systems engineering. Platinum Solutions and the NCSC each offer the team key niche capabilities. Platinum Solutions is currently working with the FBI Laboratory on related technologies. NCSC will help shape and oversee the privacy considerations for the program; it will also provide guidance on interfacing with state court systems.

In May of last year, Lockheed Martin opened the Biometric Experimentation and Advanced Concepts (BEACON™) center in White Hall, WV, to serve as a collaborative center in the development of integrated biometrics solutions for both current and future initiatives. In addition to other programs, the center will support the FBI and the NGI program.

Lockheed Martin has significant experience in the development of biometric technology for use in pioneering programs. In addition to designing, developing, deploying and maintaining IAFIS, the company is the lead systems integrator for the Registered Traveller program led by Verified Identity Pass, Inc. The company is also the lead contractor for the Transportation Worker Identification Credential (TWIC) program, a Transportation Security Administration initiative to protect ports by issuing a biometrically-based credential to vetted port workers requiring unescorted access to the ports.

efficient as a conventional 12.5 kHz bandwidth Frequency Division Multiple Access (FDMA) channel. Using TDMA, the cost and equipment space at the base station can be significantly reduced as compared with FDMA. TDMA can also accommodate additional and important services required in today's fast-moving, information-dependent world such as higher data rates, improved throughput in poor RF signal conditions, bandwidth on demand, concurrent voice and data and full duplex voice communications.

On paper, TETRA sounds like a very versatile, reliable and secure system for use in the context of homeland security. The system has been widely deployed across Europe. For networking the vast array of government agencies with their varying needs, it seems to be a perfect solution. For example, T-Systems successfully developed a TETRA-based system for Hamburg's police and fire departments during the 2006 FIFA World Cup due to its stable communications, clear voice and excellent capability in large-scale deployment scenarios. TETRA can also be deployed at short notice in the event of a disaster that will inevitably bring together a large amount of personnel from various different agencies such as NGOs, police, fire and military. In the event of a catastrophe, there is unlikely to be adequate mobile connectivity and if it does exist, the capacity to accommodate such a large team of people will be inadequate. A digital exchange for the TETRA system, a TETRA base station, dispatching equipment and a TETRA connectivity server, standby terminals, a mobile power supply and a mast plus TETRA antenna would be required in such an instance. Obviously, coverage would be dependent on the terrain and height of the mast. Minimal training would also be required for those using the terminals as they are very simple to operate meaning they are available for search and rescue tasks quickly.

However, there is a lot of discussion about the safety of TETRA. This revolves around the frequency that the system works on – 17.5 Hz. Concerns have already been raised about the radiation in the 16Hz region – a frequency the brain is highly sensitive to – what does this mean for TETRA? There is also great debate over the effect of the frequency that devices work on in hospitals and ambulances by health workers, by petrol station workers, the fire service, in airports etc.

Border protection

Last year, the Boeing Company was awarded a US\$64 million task order to design, develop and test an upgraded Common Operating Picture software system to provide the department with enhanced capability in its effort to secure the border. It is called SBInet.

A critical component of the SBI strategy is SBInet, a comprehensive program to transform border control technology and infrastructure. The goal of this program is to field the most effective proven technology, infrastructure, staffing, and response platforms, and integrate them into a single comprehensive border security suite for the department. US Customs and Border Protection will serve as executive agent for the department's SBInet program — leading, managing, and working with an industry integrator to implement this aggressive new Department of Homeland Security program.

The US Customs and Border Protection SBInet Program Management Office (PMO) supports the mission of the Department of Homeland Security (DHS) by providing the resources and capabilities necessary to bring effective control to the Nation's borders both at and between the Ports of Entry (POEs).

SBInet's strategic goals are to:

- Ensure border security by providing resources and capabilities



to gain and maintain control of the nation's borders at and between the POEs;

- Lead the development and deployment of a Common Operating Picture (COP); and
- Provide responsible acquisition management.

By accomplishing these strategic goals, the SBInet program will ensure successful implementation of the Secure Border Initiative (SBI) within CBP.

The "National Plan to Achieve Maritime Domain Awareness" outlines an essential task list that includes:

- Persistently monitoring (in the global maritime domain) vessels and craft, cargo, vessel crews and passengers, and all identified areas of interest; and
- Collecting, fusing, analysing, and disseminating information to decision makers to facilitate effective understanding of the maritime domain.

Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States. However, this does not mean that knowing everything everywhere in the maritime domain is a requirement to achieving MDA. Conceptually, MDA is the integration of Global Maritime Intelligence and Global Maritime Situational Awareness. Global Maritime Intelligence is the product of legacy, as well as changing intelligence capabilities, policies and operational relationships used to integrate all available data, information, and intelligence in order to identify, locate, and track potential maritime threats. Global Maritime Situational Awareness results from the persistent monitoring of maritime activities in such a way that trends and anomalies can be identified.

Enterprise Hubs are being developed from within existing organizations with capabilities that already make substantial contributions to MDA in one or more of the following subject areas:

- vessels;
- cargo;
- people;
- infrastructure; and
- architecture management.

CBP has been designated to lead the Cargo and People hubs. Designation as an Enterprise Hub confers two primary responsibilities; overall coordination of information flow for the respective subject area both domestically and internationally, and facilitating the sharing of related intelligence, information, and data. Enterprise Hubs are intended to leverage their experience and expertise to provide leadership for the community in a particular area, not to be the exclusive federal provider of information and products for that subject area.

Boeing has received full acceptance of the Secure Border Initiative Project 28 border security prototype from US Customs and Border Protection (CBP). A demonstration of the SBInet security solution, P28 networks cameras, radars, sensors and communications along 28 miles of the US -Mexico border near Arizona was developed as a proof-of-concept of Boeing's overall SBInet technology solution. P28 serves as a test and evaluation system in an operational environment.

Using P28 technology, US Border Patrol agents apprehended more than 2,000 illegal immigrants during initial operations testing between September 2007 and February 2008. In the coming months, CBP will conduct operational and technical tests of P28. "We're very happy the customer has accepted P28," said Jack Chenevey, Boeing SBInet Program Manager. "While we've learned a lot from the integration work we've completed, the information we'll capture from actual frontline field use of the system is invaluable to our systems

engineering and design efforts for future SBInet technology deployments."

By the end of the year, Boeing will replace P28 mobile surveillance towers as part of the larger Tucson Sector deployment with permanent towers equipped with camera, radar and communications technology that incorporate feedback from operational tests.

Eyes in the sky

Satellites play a crucial role in homeland security due to their ability to see what we can't see. Earth observation and spy satellites provide incredibly detailed information and can act as an early warning system in times of conflict. Lockheed Martin have developed the first Space-Based Infrared System (or SBIRS) geosynchronous orbit named GEO-1. The spacecraft is currently being put through tests before it embarks on its environmental test phase. These tests, entitled the Baseline Integrated System Test, will help the manufacturer to see how the GEO-1 will perform and will establish a baseline before environmental testing. The first phase of BIST has already been completed and, after assembling the spacecraft into flight configuration, a test of the integrated satellite has begun. The BIST is expected to reach completion in May, after which the satellite's solar arrays will be integrated along with the deployable light shade, thermal blankets and will then go into tests for acoustic and pyroshock. This will ensure that the satellite can withstand the forces inflicted upon it during launch.

On top of the satellite tests, the ground segment and satellite must also be tested and validated to ensure that they can effectively work together during launch and operation in orbit.

"Our steady progress in this critical integrated satellite test phase reflects the entire team's hard work and dedication to operational excellence on this vital national security program," said Jeff Smith, Lockheed Martin's SBIRS Vice President and GEO-1 Program Manager. "This first-of-its-kind satellite will provide unprecedented new capabilities for our warfighters and we look forward to achieving mission success for our customer."

The satellite will be launched late in 2009.

Protecting our assets – critical infrastructure

Critical infrastructure can easily be destroyed or damaged by various events such as terrorist attacks, natural disasters, computer hacking, criminal activity and malicious behaviour. The critical infrastructure that is intrinsic to the way we live and work today must be protected. The loss of any part of a nation's critical infrastructure can have a domino effect upon other parts of the infrastructure. The reliance on the Internet and ICT-related networks and also the energy supplies such as gas and electricity are prime examples – if these are brought down, the consequences could be devastating. Examples of critical infrastructure include:

- Energy installations and networks;
- Communications and information technology;
- Finance;
- Health;
- Food;
- Water;
- Transport;
- Production; and
- Government.

Encouraging preparedness

Businesses and governments across the world are realising the importance of having a plan 'B'. If the worst was to happen, there must be a system in place to assure that vital communications and critical infrastructure are not affected. When terrestrial infrastructure is knocked out the back up technology that immediately comes to mind is satellite. Independent of any terrestrial infrastructure, satellite can be deployed as a failover system in case of disruption. In today's



world, outages cannot be tolerated and governments, hospitals, police departments for example, must be able to switch systems instantly when outages occur.

Loral Skynet offers a suite of satellite-based contingency services designed to help businesses and government organisations minimise IP data network outages caused by large-scale natural disasters as well as everyday outages. The suite comprises the following:

- **SkyReachSM Ensure** – A business continuity solution designed to provide pre-planned continuous network connectivity for all vital business and government functions; and
- **SkyReach SAVER** – An emergency restoration network solution designed as a disaster recovery option where a rapid response mechanism is built into a network to minimise downtime and loss of production.

If a business or government has invested in a satellite-based solution they can be assured of continuous connectivity and communications no matter what happens. In a world where there is no room for failure and constant connectivity is of the utmost importance, this is something that must be considered. As the saying goes – ‘fail to prepare and prepare to fail’.

UAVs for homeland security

NASA and the Ames Research Centre are collaborating on a homeland security project using unmanned aerial vehicles. The project is based around the simulation of a terrorist attack. A device was detonated at a collapsed structure site. This detonation released a plume into the sky that simulated a chemical weapon attack. A UAV equipped with imaging sensors and a chemical detector was deployed and within minutes was 800 feet above the target area taking samples and feeding the information back, illustrating just one of the uses of UAVs for homeland security. UAVs have proved themselves to be

suitable for a wide range of applications. Not only do they not put lives at risk, but they are cost-effective. They can facilitate real-time data and imagery and may be used for urban emergencies, disaster assessment and search and rescue.

They may also be used for the tracking of terrorists, for example. Once all the information gathered by the UAV has been relayed to the incident centre, the responders can build up a detailed picture of the incident and can therefore make accurate and swift decisions – vital in an emergency situation.

Civilian applications for UAVs are evolving all the time and more and more investment is being poured into the technology. The most prevalent application for UAVs in the context of homeland security is for local monitoring and surveillance. UAVs are also being trialed for the monitoring of illegal entrants into countries and for the protection of government buildings and other facilities.

They are becoming simpler and less expensive to maintain and will therefore be much more widely used. The role of UAVs in law enforcement has huge potential. For example, the US Transportation Department is looking at security functions for UAVs. The variety of UAVs is broad and the development of the technology continues to evolve. The global appetite for UAVs is destined to grow and grow.

Technology's leading role

Here we have explored just some of the ways in which technology and communications are helping to protect our assets and our lives. Public safety interoperability is going to continue to be a very important theme. Developments in voice and data communications along with IP technology mean that keeping in touch and keeping watch over our seas, our borders and protecting our interests is becoming easier. The threats that exist today have changed and the technology that we use has had to change with these threats. It has never been so important to be aware and to use the fantastic array of communications available to us. ●

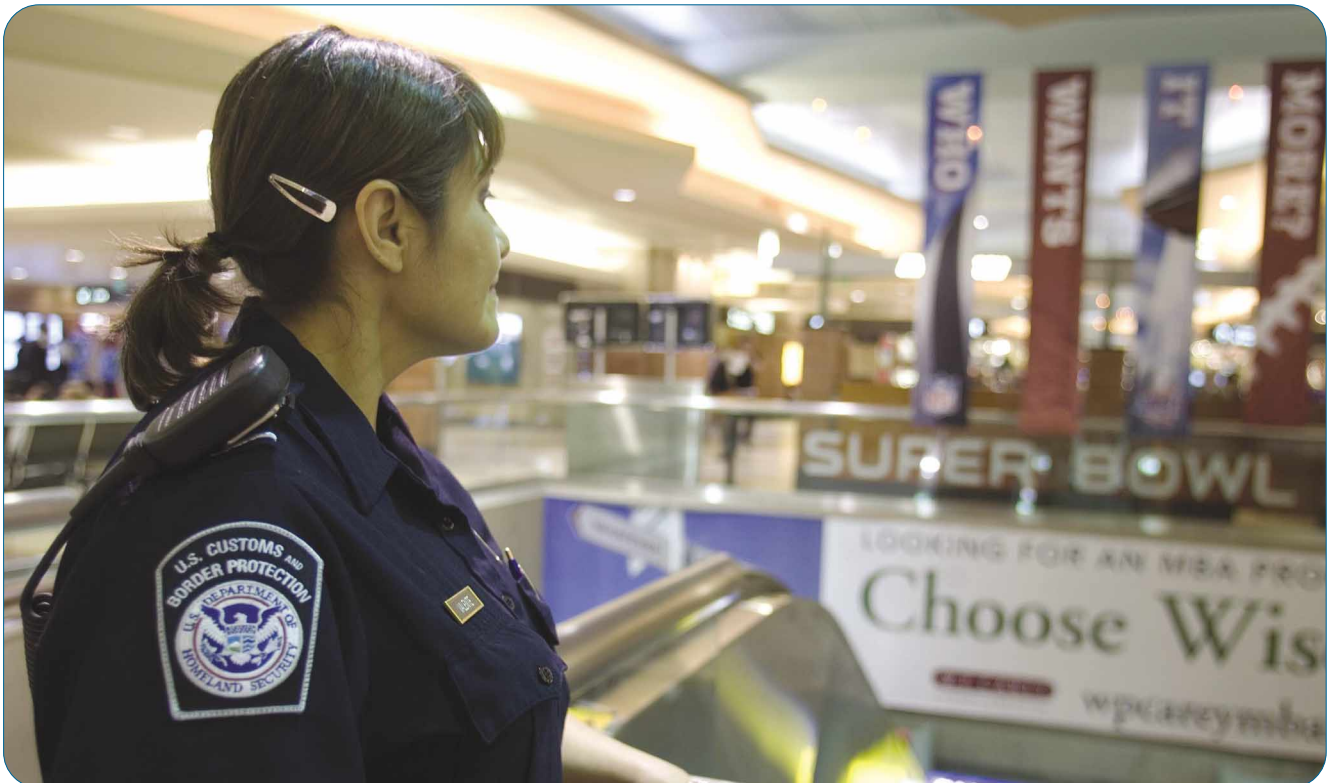


Photo courtesy of the Department for Homeland Security.