In the United States, The Department of Homeland Security was given a mandate to deal with the concerns for national homeland defense and security after the terrible events of 9/11. As one of its roles it has the explicit target of providing more efficient integration and exchange of intelligence data. Other NATO government organizations exist around the world with the same basic remit of securing national borders, transport utilities and communications systems without restricting or burdening the quality of life and free flow of people, trade goods and services.

However, there are a number of tactical and logistical problems to be resolved, not least that of ensuring the validity of such intelligence data, but also providing standard methods for data acquisition, formatting, storage, sharing, secure distribution and integration with existing military and law enforcement data sets. One of the most challenging problems is that of ensuring consistency of technical and operational standards between the various groups within the respective defense communities, not just within the USA and other nation states, but between them as part of coalition operations. With recent world events there are further pressures to provide for interoperability between former closed military C4I systems and those of national intelligence and law enforcement agencies to provide for Homeland Security operations. Such systems are required at secure installations (e.g. airports, seaports and railways).

Currently in the U.S.A. there are approximately 15 government agencies, offices and federal government organizations all focused on the security of the US homeland, its infrastructure and the US population. The U.S.A. is not alone in having numerous national agencies that ‘touch’ their intelligence data. The Countries of Europe, the Middle East and Asia are all buckling under the pressure to be effective (pseudo real-time) in meeting the challenge formed by the new threat. The systems that are put in place need to share, query and integrate their data with that of external countries and effectively extend the homeland security borders of each country involved.

The main thrust of this JACIC Special Issue is on COTS and military (air, land, sea) technologies that can enhance the homeland security of national transportation infrastructure in the form of airports, seaports, rail, road and mass transit. Moreover, controlled human access to government and secure areas will be examined through use of bio-authentication and spatial tracking techniques. Submissions are invited from industry and National government representatives who can share experiences and expertise in the quest for a coherent set of internationally acceptable technical standards.
Proposed topics include but are not limited to:-

Airport Security technologies
Structural Security Assessment and Blast Risk Mitigation
Hazards Detection
Emergency Response Tools
Intelligent IP-based Sensor Networking for Homeland Security
Real-time intelligence data validation and verification mechanisms
Efficient Data integration and Mining techniques for NATO countries
International standards for data schema and levels of data aggregation
Secure distributed storage and data pinning
SATCOM for HLS
Critical Aerospace Communications Systems
Bio-authentication sensors and tools
HLS for Air, Land and Sea Operational Environments
Airborne Real-time spatial tracking techniques
Cyber and Physical Security of key Infrastructure and Operations
Real-time Resilient Communications Network Infrastructures

For those that are interested in making a technical submission please respond in the first instance with an abstract to the Senior Guest Editor, Professor Gerard Parr at the following address:-

gp.parr@ulster.ac.uk

Notes: Indicative Dates

1. 26th June 2006- Draft Papers should be submitted to any of the Guest Editors in accordance with JACIC format:
   http://www.aiaa.org/content.cfm?pageid=563

2. November 6th 2006- After initial screening and review process a final set of papers will be invited for submission

3. January 29th 2007- Final Papers due

4. Spring 2007 Special Issue Publication Date

Senior Guest Editor:-
Professor Gerard Parr
Chair in Telecommunications Engineering
Internet Technologies Research Group
School of Computing and Information Engineering
Faculty of Engineering
University of Ulster Coleraine Campus
Northern Ireland
United Kingdom BT52 1SA
gp.parr@ulster.ac.uk

Co Editors:-

Professor Lyle N. Long
Professor of Aerospace Engineering
The Pennsylvania State University
lnl@psu.edu
Professor Petre Dini
Senior Research Scientist
Cisco Systems, Inc.
San Jose
California, USA
pdini@cisco.com

Dr. Raymond Bittel
Manager, Advanced Concepts
Prog. Dev. Analysis & Integration
Airport Security Programs
The Boeing Company
Richardson
Texas, USA
raymond.h.bittel2@boeing.com

Professor Laurie Cuthbert
Head of Department of Electrical Engineering
Queen Mary
University of London, UK
laurie.cuthbert@elec.qmul.ac.uk