**Minister of Communication & Works of the Republic of Cyprus**

**Mr Tasos Mitsopoulos**

**Curriculum Vitae (C.V.)**

Personal info:
Place of origin and date of birth: Larnaka, 30 May 1965.
Marital status: Married to Katerina Vati; has one son and one daughter.
Studies: Law (National and Kapodistrian University of Athens).
Profession: Professional executive of the Democratic Rally Party (DISY).
Foreign languages: English, French.

Parliamentary tenure/activity
· Representative of Larnaka constituency under the banner of DISY, 2006-2013.
· Deputy Chairman of the House Standing Committee on Legal Affairs.
· Parliamentary Spokesman of DISY.
· Member of the Committee of Selection.
· Member of the House Standing Committee on Legal Affairs, of the Ad Hoc House Committee on Rules of Procedure and full member of the Special House Committee on Declaration and Examination of Financial Interests.
· Member of the COSAC (Conference of Parliamentary Committees for Union Affairs)
· Member of the delegation of the House to the Parliamentary Assembly of the Mediterranean (PAM).

Political career:
· Member of the DISY Youth Organisation and of the Protoporia Student Union (NEDISY) (1978-2000).
· Member of the Youth Party of Nea Dimokratia (1998-1990)
· Vice-chairman and General Secretary of the Youth Organisation of the European People's Party (EPP) (1989-1993).
· Special Advisor to the Hellenic Foreign Ministry (1989-1993).
· Director of Dimitris Avramopoulos' Office, currently Greek Foreign Minister (1993-1995).
· Assistant of C. Hatzidakis-Member of the European Parliament (1995-1997)
· Director of the Office of the President of DISY (1997-2005).
· Spokesman of DISY (1999-2008).
· DISY Commissioner for European Affairs and Secretary of the Party's Political Planning.
· Head of the Middle East Observatory of the European People's Party.
· Member of the DISY Executive Bureau and of the DISY Political Bureau.

# Opening Address by the Minister of Communication and Works Mr Tasos Mitsopoulos

It is with great pleasure that I welcome the initiative of the organizers to host this conference in Cyprus. The conference addresses the very important issue of securing oil and natural gas infrastructures and systems from cyber threads and cyber-attacks which have transitioned from the theoretical level to the inevitable. I would like to warmly welcome you to this event which addresses this important issue that must be taken into account in developing the critical for the economy of Cyprus, oil and natural gas infrastructure.

Last summer, one of the world's largest oil and natural gas producers discovered that a virus had infiltrated more than 30,000 of its computer workstations. The company's immediate reaction was to isolate all of its computer systems from outside access.

While the infiltration had no immediate impact on the company's production operations, employees were cut off from e-mail and corporate servers for several days. Furthermore, the virus erased significant data, documents, and e-mail files on about 75% of corporate computers. Another example is the "stuxnet" worm which affected nuclear plans in an Asian country with significant damage to the affected infrastructure. Considering that some of the infected systems were not even connected to the internet makes the issue more alarming. It is estimated that a 10% probability of a major critical information infrastructure breakdown is realistically possible in the next ten years.

These are clear signals to all energy companies worldwide. These messages show that the infrastructure of even the biggest, best-prepared organizations are vulnerable to attack.

Today's cyber threats are persistent, well organized, constantly evolving and often successful. Many incidents appear within the information technology (IT) ecosystem in a manner that is all but impossible to distinguish them from legitimate activity.

Security is only as strong as the weakest link. Many times the infrastructure alone is not the weakest element. Employees and executives who are not adequately trained in security threats appear to be a major security risk. The far-flung geographic locations of energy producers also present a huge challenge, which means that connected technology assets are necessary to assure a wide range of essential services.

The consequences can be serious and wide-ranging. Depending on the target and size of the organization, the financial impact alone can reach millions of euros. Furthermore cybercrime can seriously damage brands, compromise customer confidence, violate compliance mandates, and weaken the ability to generate revenue. The energy sector play's a crucial role in the global economy and is expected to play even more important role in Cyprus economy. Cyber-attacks in this field can endanger public safety by disrupting communications, exploration, energy refining, power, and utility services. Cyber-attacks can be used to leverage IT integration in oil and gas exploration, production, refining, and distribution and transmission.

An effective security strategy is a critical element to achieving innovation and growth. The government of Cyprus is recognising the importance of the effective implementation of a national cyber-security strategy. The Cybersecurity Strategy of the Republic of Cyprus has been recently adopted by the Council of Ministers, and since last March we are exercising an intensive implementation phase. The Ministry of Communications and Works, which has the supervisory role in the Information Society and Cyber security fields in Cyprus, is working with the other competent Ministries of the Republic in security standards in our country.

The new national Cybersecurity strategy covers further to network and information security and resilience, the fields of cybercrime, cyberdefence and international cooperation in the field of cybersecurity. The activities are coordinated by the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR).

Since many other sectors rely on ICT as an enabler, all should therefore be concerned about network and information security and more widely cyber security. As explained before, a number of specific infrastructure and service providers are particularly vulnerable, due to their high dependence on correctly functioning network and information systems. These sectors play an essential role in providing key support services for our economy and society, and the security of their systems is of particular importance to the functioning of the market. These sectors include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, internet services and public administrations. These sectors are covered under the actions of the Cyber security strategy and more particularly under the national Critical Information Infrastructure Protection (CIIP) framework. The work in this field is underway and will cover the energy sector which is considered to be critical.

Ladies and Gentlemen,

In a country which is an island, where the economy depends heavily on the supply of services and where the successful exploitation of the opportunities from oil and natural gas exploration is evident, a high level of network and information security and cybersecurity is important and will contribute to the development of the required market environment and trust, to enable the progress of our society. The active implementation of the national strategy on Cybersecurity shows the government's will to work closely with all stakeholders and to help all critical sectors, including the energy sector, to lead our society to progress and economic prosperity.

Finally, I would like to wish every success in this event and I hope that this initiative will be of benefit to all the stakeholders in the oil and natural gas industry that are present at the conference today.

See more at:
http://www.cyprus.gov.cy/moi/pio/pio.nsf/All/EFF8884468F6B890C2257C2900301CEC?Opendocument