Your Excellency, Ambassador of the State of Israel to Cyprus, Dear Oren

Permanent Secretary of the Shipping Deputy Ministry, Dear Stelios,

Director General of the Israel National Cyber Directorate (INCD), Dear Gaby,

Chief Scientist, Dear Demetris

Distinguished Guests, Ladies, and Gentlemen,

It is my great pleasure to warmly welcome you all to this groundbreaking event in Cyprus, focused on the critical issue of cybersecurity within the maritime sector. This gathering, jointly organized by the Digital Security Authority (DSA) and the Shipping Deputy Ministry, marks an important milestone in our collective efforts to enhance maritime cybersecurity.

Allow me to extend our heartfelt gratitude to our esteemed colleagues and friends from the Israel National Cyber Directorate for their invaluable assistance in organizing this event. Their expertise and unwavering support have been instrumental in bringing this important event into a reality.

I would also like to thank our distinguished guests from Mandiant, a global leader in cybersecurity, specializing in threat intelligence and incident response. We are honored by your presence and look forward to the insights you will share on safeguarding the maritime domain.

Further it is with great pleasure that I welcome distinguished guests from the U.S Embassy and British High Commission.

Finally, I express my sincerest appreciation to all of you, in attendance today. Your valuable insights and active participation will not only enhance our nation's cybersecurity posture but also contribute to shaping a more secure maritime industry for the Eastern Mediterranean region.

The maritime industry, a cornerstone of global trade and the Eastern Mediterranean economy, faces an escalating cyber threat landscape. The statistics are alarming: in 2023 alone, 64 cyber incidents were reported wordwide, and this number surged dramatically in 2024, with over 1,800 incidents, with vessels targeted. The financial toll has also grown significantly, with the average cost of a cyberattack rising to $550,000—nearly three times the cost in previous years.

This trend demands immediate and decisive action. Cyber threats pose severe risks to operational continuity, financial stability, safety, and even the environment. As such, we must act collectively to address these challenges head-on.

The European Union, through the European Union Agency for Cybersecurity (ENISA), has made significant steps in maritime cybersecurity. Frameworks like the Network and Information Systems (NIS) Directive and its successor, NIS2, provide invaluable guidance for enhancing resilience, mitigating cyber risks, and safeguarding operations and reputation. We encourage all maritime organizations to leverage these frameworks, regardless of their formal classification under the NIS Directive.

In addition, the Digital Security Authority (DSA) has been actively working to strengthen the sector's resilience through participation in European projects and international collaborations. For example:

- **CY-TRUST**: This project focuses on establishing Sectorial Security Operations Centers (SOCs), including one dedicated to the maritime sector. It aims to enhance Cyprus's capacity to defend against cyber threats by emphasizing situational awareness, incident response, and preparedness.
- **SecAwarenessTruss**: This project enhances cybersecurity training for critical infrastructure sectors, including maritime, energy, and healthcare, through hands-on simulation environments (cyber ranges) that foster collaborative incident response capabilities.

The DSA also engages in the **3+1 Cybersecurity Working Group (CSWG)**, bringing together Cyprus, Greece, Israel, and the United States to address maritime and energy sector cyber risks. Furthermore, our collaboration with the U.S. Department of Energy’s Sandia National Laboratories has yielded a series of workshops, concluding in the white paper, called *“A Regional Approach to Maritime Cybersecurity Governance and Risk Management.”*

This paper outlines a vision for a Maritime Cybersecurity Center of Excellence (MCCE), which we aspire to establish. This center would serve as a hub for training, information exchange, security enhancement, innovation, and policy development while aligning with global regulations and addressing the unique needs of our region.

Today, we gather to explore how we can make this vision a reality, leveraging your insights and expertise to identify the needs of your organizations and craft effective defense mechanisms.

As we move forward, we will delve into the critical role of cyber threat intelligence and open the floor for discussions aimed at enhancing our collective resilience.

In closing, I would like to extend my deepest gratitude to all participants and speakers. Your engagement and perspectives are vital to shaping a secure future for the maritime sector. Let us seize this opportunity to work together, share knowledge, and develop robust, innovative solutions.

Before I conclude, I would like again to express my special thanks to our friends from Israel. Despite the challenges they face, their presence here today demonstrates their unwavering commitment to our shared goals.

Thank you.