ENGINEERING A DIGITAL FUTURE

Indigo Welcomes EU Recommendations For More Resilient Marine Infrastructure As It Advances Its Own Subsea Security Services

Magor, Monmouthshire — 15th May 2024: Indigo, a leading provider of engineering and support services for subsea cabling, welcomes EU recommendations for member states to map submarine infrastructure and to assess risks and vulnerabilities as part of a drive to make subsea cables more secure and resilient.

The Commission Recommendation, published in February 2024, is concerned that networks and services are “a prime target for cyberattacks”, something that Indigo has been addressing for some time in partnership with hyperscale subsea infrastructure providers. A number of initiatives have already advanced Indigo’s capabilities, including the appointment of William Rendle as Head of Information Security. Rendle’s previous experiences include directing technology GRC (Governance, Risk and Compliance), digitisation, cyber and information security change programmes within highly regulated environments globally

Ian Duggan, CEO of Indigo, said, “William brings two decades of experience in technology risk management and delivery to Indigo as we look to build on our leadership position as a network support and security provider. His skills will be particularly relevant for our continued growth in the US and in the subsea market, where cybersecurity is a priority for the hyperscale tech companies we support.”

William Rendle commented, “I’m looking forward to further developing Indigo’s cybersecurity capabilities, building on the great work of a team that has security embedded in its culture.”
.

Since entering the subsea support market in 2021, Indigo has opened a second Network Operations Centre(NOC) in the States, emulating the original NOC in South Wales in being ‘security aware’, providing clients with a combination of fault and threat identification capabilities.

Duggan said about the strategy, “A modern NOC must be able to cross-reference data when tracking an incident and ascertain if there are any security implications. It is increasingly important that network monitoring capabilities can identify early indicators of a cyberattack.”

Aware that service providers themselves are a potential target for cyber criminals, Indigo has narrowed its own threat surface by ensuring full ownership of all connectivity around its remote monitoring service. Its carrier-grade IP-based Data Communication Network (DCN) has advanced security features for high availability and redundancy. The Indigo NOC teams have a forensic level of understanding of the equipment they use, which is always procured as new, direct from the factory.

A Salesforce-driven system is key to the model, integrating APIs from multiple vendor platforms to capture all events and alerts through a single pane of glass for lightning-fast incident management. At the same time, the Salesforce system is gathering incident data for root cause and trend analysis to inform a more proactive approach to security and maintenance. Indigo ensures its team's processes conform to international critical infrastructure requirements by meeting stringent NIST, ISO 27001 and NSA standards.

To find out more, please contact Liz Edwards, Marketing and Communications Director.
liz.edwards@indigotg.com +353 86 817 1512

About Indigo
Indigo provides design, deploy and support engineering services to fixed and mobile carriers, tech companies, and the enterprise sector since 1998.

Indigo collaborate, challenge, research, and develop to enable their customers to stay ahead of emerging and expanding technologies. With the brightest minds and leading technical insights in the business, they design to innovate, deploy to evolve, and support to enhance the performance of digital infrastructure better, faster, and safely.

www.indigotg.com