The Institution of Engineering and Technology

150
1871 - 2021

IET Codes and Guidance:
Cyber Security case study

Helping the Department for Transport (DfT) manage cyber security threats at UK ports

theiet.org

The problem

A number of incidents at ports across Europe have significantly raised the profile of cyber security in this area. The risks associated with the complex systems used by port owners and operators need careful management.

The DfT and Defence, Science and Technology Laboratory (Dstl) contracted the IET to commission guidance to help those responsible for ports around the country manage the threat from cyber attacks.

Our process

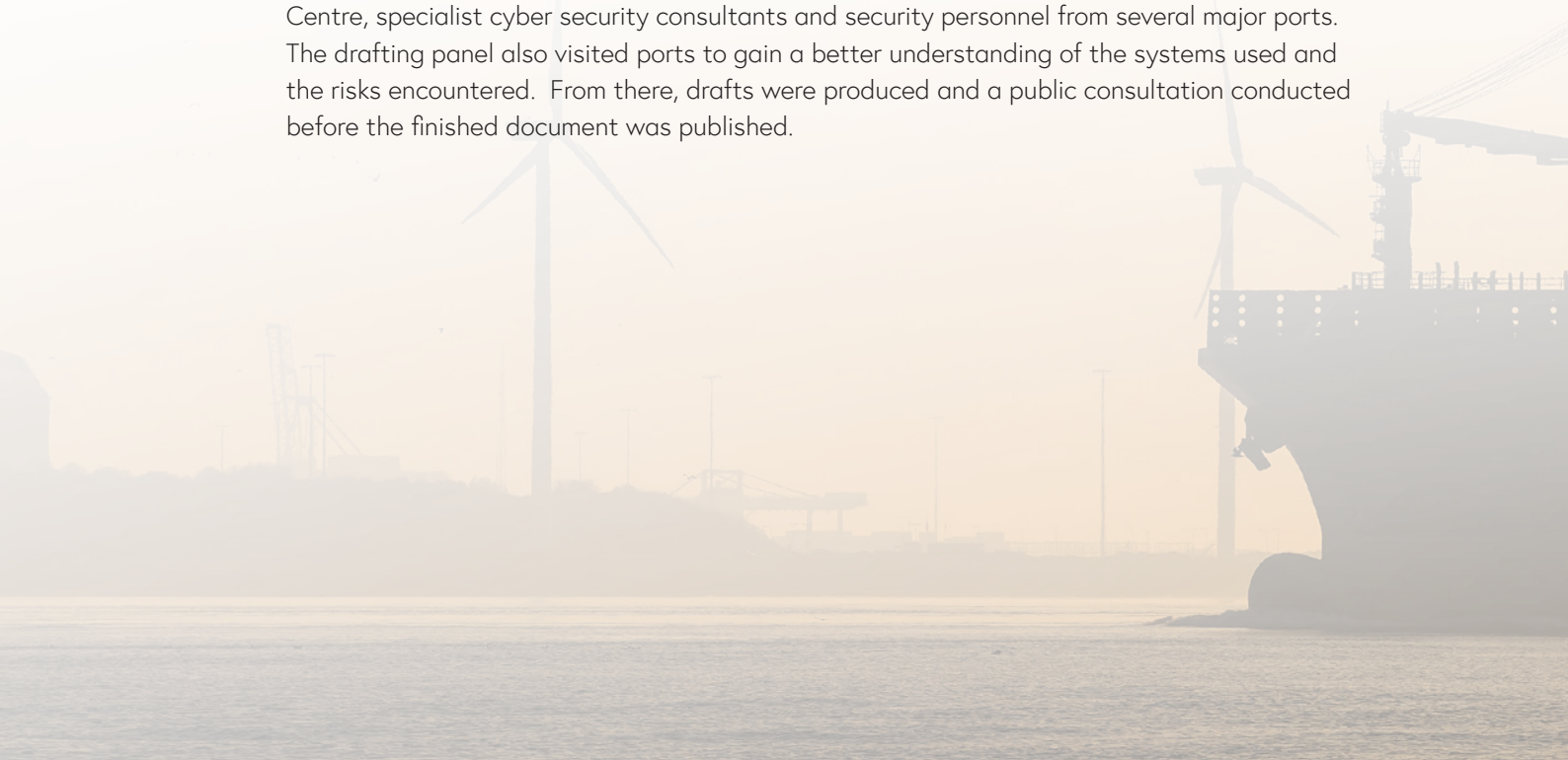
We work collaboratively with our clients to identify their requirements, appoint a technical committee containing industry experts and stakeholders, and draft actionable, practical guidance. To ensure the end result is robust, and fully meets the expectations of our clients and the wider industry, we release a draft for public comment towards the end of the process. This provides valuable feedback from industry stakeholders, which is carefully reviewed and considered before the final document is published.

For this guidance, the requirements included creating a document to help port owners, operators and security staff to:

- develop a cyber security assessment and plan,
- devise the most appropriate mitigation measures,
- have the correct structures, roles, responsibilities and processes in place, and
- handle security breaches and incidents.

The document also needed to highlight the key national and international standards and regulations to be reviewed and followed by anyone using the guidance.

We involved stakeholders throughout the process from DfT, Dstl, the National Cyber Security Centre, specialist cyber security consultants and security personnel from several major ports. The drafting panel also visited ports to gain a better understanding of the systems used and the risks encountered. From there, drafts were produced and a public consultation conducted before the finished document was published.



What was the outcome?

The initial Code of Practice was published in July 2016 and has proved to be an important briefing document for port security personnel. To keep the guidance up to date with ever evolving security threats, it was revised in 2019 to the *Good Practice Guide: Cyber Security for Ports and Port Systems*. The Guide is of real value to all those responsible for security and business continuity in ports and can be used as an integral part of an organisation's overall risk management system.

Jim Spooner, Head of Maritime Resilience at the Department for Transport was very pleased with the outcome.

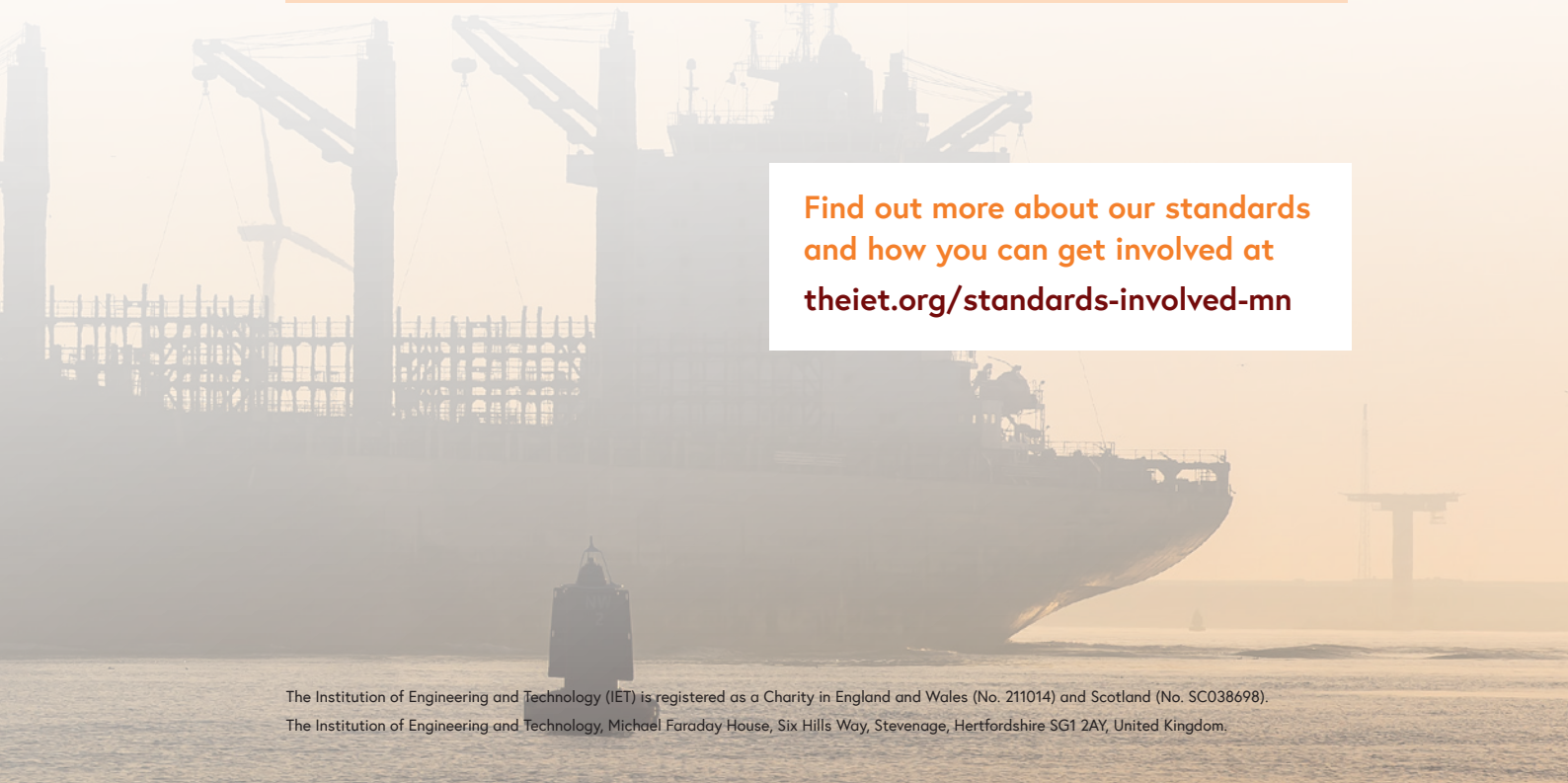
> ***"It has enabled ports to stay abreast of cyber security guidance thereby decreasing the likelihood of an unfortunate event impacting on the port. This improves overall UK resilience in the maritime sector."***

Working with the IET Codes and Guidance team

The DfT and Dstl chose the IET to create this standard for them. Our reach into the engineering industry, expert members and contacts in specialist areas, and experience publishing practical guidance makes us the natural choice for creating engineering standards. Our robust development and consultation processes provide peace of mind to our clients that the documents they commission will be of a high quality and meet their bespoke requirements.

Jim concluded that he would happily work with the IET again in the future.

> ***"IET has a professional approach and valuable expertise across the board."***



Find out more about our standards and how you can get involved at

theiet.org/standards-involved-mn