



Exercise Granite Resolve

Report

Final
October 2026

Acknowledgments

In preparing the exercise, OEUK gratefully acknowledges the contribution of members and stakeholders, namely:

- Mark Wilson, OEUK
- Graham Skinner, OEUK
- Iylia Lavatelli, Restrata
- Craig Menzies, Restrata
- Liam Thom, Restrata
- Botan Osman, Restrata
- Martin Smith, CyberPrism
- David Fisher-Holt, CyberPrism
- The State Threats Team at the Department of Energy Security and Net Zero

While every effort has been made to ensure the accuracy of the information contained in this publication, neither OEUK, nor any of its members will assume liability for any use made of this publication or the model agreement to which it relates.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Copyright © 2026 The UK Offshore Energies Association Limited trading as OEUK

PUBLISHED BY OEUK

London Office:

2nd Floor, Cannongate House, 62-64 Cannon Street, London EC4N 6AE
Tel: 020 7802 2400

Aberdeen Office:

4th Floor, Annan House, 33-35 Palmerston Road, Aberdeen, AB11 5QP
Tel: 01224 577250

info@oeuk.org.uk

www.oeuk.org.uk

Contents

1	Summary	6
2	Key findings and Actions	7
2.1	OEUK Actions	7
3	Exercise Overview	9
3.1	Scenario	9
3.2	Exercise Groups	10
3.3	Overview of Injects	11
4	Detailed findings	12
4.1	Safety Practice Supports Security Incident Response	12
4.1.1	People, Environment, Asset and Reputation (PEAR) decision making framework	12
4.2	Incident Ambiguity	12
4.3	Installations not designated Critical National Infrastructure	13
4.3.1	Situational awareness of threat landscape	13
4.4	Incident reporting pathways	13
4.5	Government Response to incidents	14
4.6	Risk of silos	14
4.7	Integrated security planning is required	14
4.8	Co-located offshore sectors	14
5	OEUK & Industry Actions	15

List of Abbreviations

Abbreviations	Definitions
C2C	Control & Command
CCR	Central Control Room – however, for the scenario the term Main Control Room (MCR) may also be used
CMT	Crisis Management Team
CNS	Central North Sea
DESNZ	Department for Energy Security and Net Zero
DMZ	Demilitarized Zone – the section of Network between the Enterprise and Industrial networks.
ERT	Emergency Response Team
EXCON	Exercise Controllers
DoS	Denial of Service
FPSO	Floating Production, Storage and Offloading
GPA	General Platform Alarm
HMI	Human Machine Interface (e.g. Operator screens in the control)
IMT	Incident Management Team
IT	Information Technology (the Enterprise network and everything that sits on it)
JMSC	Joint Maritime Security Centre
LOS	Line of Sight in our instance it's the line-of-sight radio between the assets.
NUI	Normally Unattended/ Unmanned Installation
O&G	Oil and Gas
OEUK	Offshore Energies UK
OT	Operational Technology (the Industrial network and everything that sits on it)
PA	Public announcement (system)
PAPA	Prepare to Abandon Platform Alarm

Abbreviations	Definitions
PEAR	People, Environment, Asset, Reputation
PEARL	As above and includes Liability
POB	Persons/ Personnel on Board
SCADA	Supervisory Control and Data Acquisition
UKCS	United Kingdom Continental Shelf
VOIP	Voice Over Internet Protocol – most modern phones use this. It's difficult to find ones that don't use it.

1 Summary

On 21st April 2026 Offshore Energies UK (OEUK) delivered exercise Granite Resolve, a joint security and resilience exercise in Aberdeen ahead of the OEUK Security and Resilience Conference 2026. The exercise was developed and facilitated by OEUK with expert technical support from Restrata and CyberPrism. The Department for Energy Security and Net Zero (DESNZ) participated and contributed.

The exercise convened over 60 participants from across the UK energy sector, including energy operators, supply chain companies, emergency responders, regulators, government representatives, Police, Coastguard and government security services. The objective was to test and challenge the industry's ability to respond to a complex evolving security incident affecting offshore energy infrastructure within the UK Continental Shelf (UKCS).

Granite Resolve marks a departure from traditional emergency response exercises by combining multiple threat vectors within a single scenario. Each threat within the scenario represented a reasonably foreseeable escalation based on real world security incidents, occurring in a coordinated pattern, again, representing patterns of ambiguous sophisticated attacks seen in other European countries. Participants were required to respond to a blend of suspicious maritime activity, drone incursions, protestor action, operational technology (OT) cyber compromise, communications disruption and heightened geopolitical tensions all within the context of maintaining energy security and safe operations.

The exercise identified:

- Significant strengths in safety related incident management response practices across industry but highlighted a level of uncertainty in responding to security incidents including clarity on escalation threshold triggers.
- Where there is significant ambiguity about the source and intent of system disruption it can mask identification of coordinated hostile activity, especially in the early stages of an incident.
- Vulnerabilities of installations not designated Critical National Infrastructure were clear, creating issue from a lack of situational awareness of the magnitude of threat faced, clarity of in-incident reporting pathways, and level of government response expected during incidents.
- Risk of silos between physical and cyber security requiring integrated security planning and risk of silos between energy sectors requiring domain focussed cross sector security planning at all levels.

2 Key findings and actions

Exercise feedback demonstrated that all participants gained organisation specific actions to enhance security and policy planning within their own response arrangements.

2.1 OEUK findings

Key themes that were captured are:

- There are significant strengths in the response arrangements for safety related incident management across industry, however the exercise highlighted a level of uncertainty in responding to security incidents including a requirement for further clarity on the escalation threshold triggers.
 - The incident consideration of People, Environment, Asset and Reputation (PEAR) as a decision-making framework is effective in supporting prioritisation in security incidents across operational, tactical and strategic levels, however consideration could be given to increasing the scope to include Liability (PEARL) given the experiences from the Crisis Management Team (CMT).
- During the exercise there was significant ambiguity about the source and intent of system disruption and this was identified as being able to mask the identification of coordinated hostile activity across multiple assets, especially in the early stages of an incident.
- The exercise discussion identified that the vulnerabilities of installations not designated Critical National Infrastructure were clear and it was felt that this can create issues that include
 - Lack of situational awareness of the magnitude of threat faced,
 - Reduction in clarity of in-incident reporting pathways,
 - The level of government security response expected during incidents.
- The exercise provided a scenario that impacted multiple assets in the UKCS and the risk of creating a siloed approach brought out:
 - Gaps between physical and cyber security practice requiring a greater level of integrated security planning.
 - Gaps between security and incident management practices between energy vectors especially in relation to co-located offshore oil and gas and wind farms requiring domain focussed cross sector security planning at all levels.

2.2 OEUK actions

As a result of the findings of the exercise OEUK has taken forward the following actions:

- Extend invites for the OEUK Industry Security Threats and Response Action security group to wind farm operators in addition to existing O&G operators, pipeline operators and terminal operators.
- Increase awareness of benchmark cyber expectations via the OEUK Quarterly Security Webinar Series.
- Engage members to sign up to the Government Cyber Security Pledge

- Provide greater visibility to OEUK Board members of security threats and benchmark good practice.
- Develop further security exercise for 2027 that further tests cross sector response action.
- Develop a sector Security Strategy for 2027.

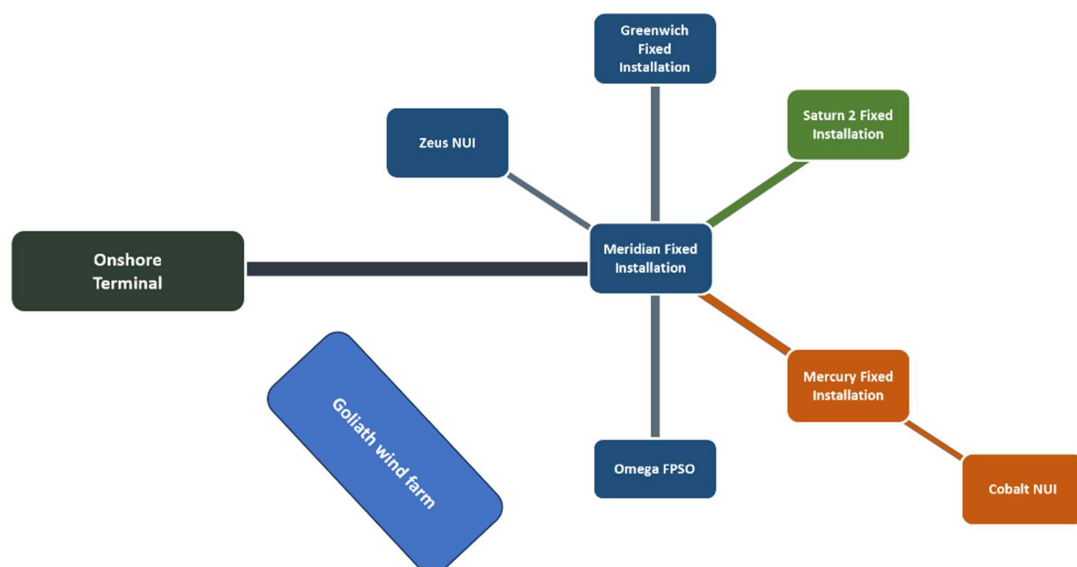
3 Exercise Overview

The exercise involved industry participants undertaking an analysis of response arrangements during a one-day exercise, with the scenario covering a one-week period.

The exercise was designed to immerse participants in a realistic physical and cyber security threat environment linked to onshore and offshore energy infrastructure. It included levels of ambiguity and uncertainty that participants were required to explore as part of the scenario and its associated injects, enabling the identification of improvement areas and future actions.

3.1 Scenario

The exercise was based on seven offshore assets in the Central North Sea (CNS): four fixed attended installations, two normally unattended installations (NUIs) and one floating production, storage and offloading (FPSO) vessel. The assets operated across three duty holders. Collectively, five of the assets fed into one pipeline through a hub-and-spoke arrangement to an onshore terminal and a tanker offload facility for oil. The collective production represented 35% of the UK's gas supply. The light oil was exported directly to Europe and contributed to 20% of the UK's diesel supply via imports, with a direct oil pipeline running to another onshore terminal for refining into petrol and providing 22% of the UK's fuel supply.



Oldenburg Energy was a publicly listed company on the London Stock Exchange and was an exploration and production operator. It was the duty holder for the Meridian and Greenwich fixed attended platforms, as well as the Zeus unmanned installation and Omega FPSO. The Meridian platform served as the hub and gathering platform for the field.

Also operating in the field hub was Shift Energy, which was the duty holder for the Mercury fixed attended installation and the Cobalt normally unattended installation. The final duty holder in the field hub was Axis Energy, which had the Saturn 2 fixed attended installation in its portfolio.

In addition to the hub duty holders, the adjacent area included the Goliath wind farm, which was operated by Stream Winds.

3.2 Exercise Groups

The exercise participants were asked to self-select into groups representing the offshore emergency response teams, the onshore incident management teams and the corporate crisis management functions. The groups were separated from each other and asked questions of the other groups and exercise coordinators (EXCON) throughout the exercise to provide a realistic separation of responsibility.

Group	Role & Focus	Key Responsibilities
Exercise Controller (EXCON)	Represent the external stakeholders that would be called upon in the event of an incident.	Provide external stakeholder input to the exercise and respond to questions asked from exercise players
Emergency response	Input for the asset perspective via the offshore emergency response team (ERT) led by the offshore installation manager. Represents ERT, aviation, marine and other offshore stakeholders such as supply chain.	Management of the initial event to minimise escalation. Also includes the update of offshore personnel and onshore incident management team.
Incident management	Central support to the offshore emergency response team via the onshore support team, also known as the incident management team (IMT), including specialist support. Could see representation from the parent organisation, supply chain, regulators, Police, Coastguard, etc.	Connection to the offshore ERT and the onshore crisis management team. Included in this is the engagement with external stakeholders to ensure updates/ support in a timely manner to prevent escalation. Management is via the PEAR model (people, environment, asset, reputation) to provide a prioritised approach.

Crisis management	Business continuity support via a crisis management team (CMT) in the event of an incident that also includes engagement with strategic stakeholders. Could include representation from Government, Police, other industry organisations, etc.	Direct connection with onshore incident management team (IMT) to support response and recovery aspects linked to local/ national resilience and provide strategic direction to prevent minimise escalation.
-------------------	---	---

3.3 Overview of Injects

INJECT 1 – DAYS (0-1)

The first turn of injects introduces the suspicious vessel activity moving from one asset to another within the North Sea. There is limited information about the vessel and in tandem there is protestor activity reported in relation to ongoing dialogue around highly sensitive marine protected areas.

INJECT 2 – INCIDENT DAYS (2 – 3)

The second turn of injects sees an increase of suspicious activity around several assets and pipelines. Although no 500-metre zone has been infringed the 1,000-metre zone has and on a few occasions drones have been sighted. On one occasion a drone had a failure and ditched to sea although no damage occurred to any other object.

Protestors have peacefully boarded a normally unattended installation operated by duty holder B only for them to realise that it was an unmanned installation.

INJECT 3 – INCIDENT DAYS (4+)

The third turn of injects sees an escalation in activity with blatant non-threatening activity in the local area. Reports of one drone dropping onto a helideck have caused some concern amongst the social media sites by the workforce and the increase in activity is causing aviation problems.

The vessels appear to have backed away from the UK waters and are predominantly active around the meridian line between UK, Norway and the Netherlands. In a number of cases the vessels have entered the 500-metre zone to test response arrangements.

Protestors have maximised the increase in media attention and have boarded an asset in the Southern North Sea. This is being managed by the duty holder, and at present is a peaceful protest.

The key issue is the asset control room have reported a number of alarms being activated on the SCADA system with some high-high levels being reported with no immediate fail-safe action being taken. cyber security attack in Denmark has materialised in a plant shutdown and a number of UK assets.

4 Detailed findings

Individuals attending on behalf of their organisations have taken significant actions to their organisations to progress internally. Common findings were captured via exercise feedback, observations and are discussed below.

4.1 Safety Practice supports Security Incident Response

The offshore energy industry has long standing good practice on incident response, offshore installation managers (OIM) have high levels of competence in emergency response and are required to demonstrate decision making under pressure. In the UK over 60 years of energy production in the North Sea and UK Economic Area has resulted in the development of comprehensive emergency response guidance including those documents published by OEUK. This practice ensures that the offshore emergency response teams can address the initial impact of the incident effectively despite the source of the incident.

General awareness of suspicious activity and subtle signs of early development of cyber incidents could be improved for all personnel, for example failures in communication systems, operating technology or IT systems may initially be addressed with troubleshooting technical issues rather than immediately isolating systems, that could result in more severe impacts that necessary.

The general precautionary approach to limit risk was implemented broadly by ERT teams ensuring that risk to the installations was limited by shutting in production and venting of hazardous inventories once threats were identified or control of systems deemed to be lost. This limits the risk to individual installations but may present system wide risk if a coordinated ambiguous attack was to impact multiple installations at the same time.

Scenarios for drills and exercises should be reviewed to ensure that security incidents are included in scenarios either as standalone or hybrid incidents, this may include demonstration that operational teams can put installations into island mode and retain control to ensure safe operations.

4.1.1 People, Environment, Asset and Reputation (PEAR) decision making framework

The application of PEAR decision making framework in incident response has been confirmed as effective in supporting prioritisation during security incidents across operational tactical and strategic levels. In decision making escalation between ERT, IMT and Crisis Management Teams. Senior leadership of companies should be involved in exercises to ensure they are prepared to respond to security incidents.

4.2 Incident ambiguity

The reasonable escalation scenarios identified are all incidents short of a 'war like incident' this is a legal threshold currently being considered by the UK courts in relation to insurance on the Nordstream pipeline but in general terms is a situation where deliberate intent can reasonably assume and be attributed. In the scenarios selected for Granite Resolve all threats are assumed to be non-attributable or indirectly attributable, certainly attribution is unlikely during the timescale of the incident.

The ambiguity is likely to mask early identification of the developing incident (4.1 above) but may also mask aspects related to coordination. In the scenario the coordinated nature of the incident was not initially identified by ERT and IMT despite the scenario being a single company incident response. Communication of developing incidents across offshore energy infrastructure operators is limited and reporting paths with security services who may have such an overview are not well established.

4.3 Installations not designated Critical National Infrastructure

Most offshore energy infrastructure is not designated Critical National Infrastructure (CNI) resulting in operators being excluded from the established security framework, this includes the vetting of key personnel. The lack of designation and vetting creates challenges for government security services sharing threat intelligence with non-CNI companies impacting the companies' ability to proactively prepare for those threats. The in-incident communication paths, with the exception of Police ILOs, are currently one way, creating uncertainty in the support that may be available hindering response and impacting the speed of recovery. For example, once a drone lands on an offshore energy installation it is unclear how the company should evaluate the threat it poses and therefore the level of response required.

4.3.1 Situational awareness of threat landscape

Offshore energy companies have a long history of proactive protection against safety threats and clarity on the major hazards their activities pose and the barriers they maintain to prevent incidents. In the security space, the intent of threat actors and how quickly the threat could develop is unclear. The business case for protective measures is hard to make when the threat is ambiguous, and clarity on how sector wide threat should be addressed is missing. OEUK look forward to the publication of the Subsea and Offshore Sector Security Strategy by government later in 2026.

The National Protective Security Agency are unable to share a sector threat assessment with OEUK and its members. It is unclear if that is because there is not a sector threat assessment or because security clearances currently do not allow this.

4.4 Incident reporting pathways

At the time of the exercise OEUK had recently published their Suspicious Activity Offshore Guidance for OIMs document and not all participants were aware of it. Further it was clear that participants were not all aware of the DESNZ guidance on drones. The promotion of both has been accelerated since the exercise. There remains significant reporting complexity between JMSC, Police and Coastguard and multiple secondary reports across government and stakeholders. OEUK welcome the ongoing development of a reporting portal to increase the ease of reporting suspicious activities and incidents.

There are limited feedback loops into industry and sharing of information remains a challenge due to security clearances. OEUK welcome the visibility of JMSC monthly reports in relation to suspicious vessel activity near subsea infrastructure and recognise its broad focus covering the whole maritime domain both cables and pipelines. OEUK would welcome its expansion to include all suspicious activity including drones

4.5 Government response to incidents

Throughout the exercise all parties were unclear of the government response expected at each level of escalation. Discussions were had around military support, military support to civil contingencies in addition to Police and Coastguard capabilities. Concerns were raised in relation to what could be expected in regard expected response action from JMSC. The exercise conclusion was that companies' response plans should be developed as standalone responses, with a similar approach to safety response plans.

4.6 Risk of silos

The exercise was attended by O&G and wind emergency response experts and lessons learned are relevant to both sectors, however it is important to recognise that the scenario is heavily focussed on O&G operations. The inclusion of a windfarm on the perimeter of the gas field was deliberate to reflect current and future realities. In most cases the ERT and IMT teams considered near-neighbours in their own sector, but had not considered the interaction with the wind farm operators in advance and did not initially consider informing them of the on-going incident.

Developing sub-sector guidance independently of co-located sectors may result in policy gaps and blind spots. Doing so can miss opportunities for cross sector learning and efficiencies. Equally focussing too narrowly on a single threat vector can undermine the requirement for integrated security plans.

4.7 Integrated security planning is required

The exercise demonstrated that focussing on a single threat vector can result in hostile and criminal actors finding new pathways to direct threat. As cyber security increases across organisations alternative routes into networks may become a focus of hostile actors such as via insider threat or by overcoming physical security to gain entry to systems. Equally an overlap between OT security practices and IT security practices are required. Emergency response may rely on records and data contained within IT systems and risks should be assessed.

4.8 Co-located offshore sectors

Near neighbours should consider each other in response planning to ensure developing incidents are communicated and mutual support can be achieved. More broadly the mutual assistance in relation to security incidents should be developed across sectors following similar models to safety and environmental practice. Mutual assistance is established formally either through legislation, in the case of safety, or by contractual agreement, in the case of environmental response.

Future exercising should feature scenarios that emphasis co-location and interdependence of offshore energy vectors.

5 OEUK & industry actions

OEUK has an important convening role on industry wide actions where collective response, or guidance is required. Equally OEUK has a role in supporting industry workgroups through secretarial and technical support to those groups.

Action	Responsible	Date
Extend invites for the OEUK Industry Security Threats and Response Action security group to wind farm operators in addition to existing O&G operators, pipeline operators and terminal operators.	OEUK HSS Manager	July 2026 - COMPLETE
Include National Energy System Operator and DESNZ representatives onto OEUK industry Security Threats and Response Action group.	OEUK HSS Manager	July 2026 - COMPLETE
Increase awareness of benchmark cyber expectations by through the OEUK Quarterly Security Webinar Series.	OEUK HSS Manager	July 2026 - COMPLETE
Encourage OEUK members to sign up to the Government Cyber Security Pledge.	OEUK HSS Manager, OEUK CEO, OEUK Board	2027
Provide greater visibility to OEUK board members of security threats and benchmark good practice through engagement at board meetings and joint council meetings.	OEUK HSS Manager	2026 – through 2027
Develop a sector Security Strategy for 2027	OEUK HSS Manager	End-2026
Develop further security exercise for 2027 that further tests cross sector response action.	OEUK HSS Manager	April 2027



OEUK.org.uk

OGUK Technical Notes

Member companies dedicate specialist resources and technical expertise in providing technical notes in collaboration with OGUK, demonstrating a commitment to continually improving and enhancing the performance of all offshore operations.

Technical Notes are part of the OGUK suite of Guidelines, free for our members.

OEUK.org.uk

info@OEUK.org.uk



@OEUK_



Offshore Energies UK

œUK