

[Press release: Highways England appoints interim Major Projects Director](#)

Highways England has today (Monday 21 August) announced the appointment of Peter Mumford as Exec Director to lead major projects until a permanent successor is appointed.

Peter is a senior director with a breadth of experience across all aspects of professional technical and management services, including the leadership of significant programme management teams and major project teams across global locations.

He joins the Highways England Executive team from HKA (formally Hill International) where he was Vice President. Prior to that Peter held senior positions within a number of construction industry related organisations including, Aecom, EC Harris LLP and Turner & Townsend.

The appointment of Peter will allow for a seamless transition of the major projects directorate without any impact on our ability to deliver the government's £15bn road investment strategy.

Highways England Chief Executive Jim O'Sullivan said:

I am really pleased to have Peter join the executive team. It is important that we continue to have the right mix of individuals to lead the company as we deliver the challenging target we have been set by government.

General enquiries

Members of the public should contact the Highways England customer contact centre on 0300 123 5000.

Media enquiries

Journalists should contact the Highways England press office on 0844 693 1448 and use the menu to speak to the most appropriate press officer.

Press release: Highways England urges motorists to check their vehicles this bank holiday

Highways England is lifting more than 98 per cent of roadworks to help people travelling over the August bank holiday – and motorists are being urged to make sure their vehicles are ready for the journey.

Last year more than 20 motorists broke down each day during July and August because they had run out of fuel. Almost half of all breakdowns are caused by simple mechanical problems which could be avoided with simple checks and nearly a quarter are caused by tyre problems.

Highways England will be removing some 445 carriageway miles of roadworks from motorways and strategic A roads over the bank holiday and today joined forces with leading safety group IAM RoadSmart (IAM) to remind motorists to do their bit before setting off to cut the number of breakdowns.

Highways England operations director, Nick Harris, said:

We're lifting more than 98 per cent of roadworks this bank holiday to help people get where they need to as safely and quickly as possible. If you're driving out to enjoy the late summer bank holiday, make sure you take a few vital minutes to check your vehicle, especially if you haven't done so for a while.

IAM RoadSmart Policy & Research Director, Neil Greig, added:

It's excellent news that most roadworks will be lifted over the bank holiday. The onus is now on drivers to minimise the number of preventable incidents by driving safely and preparing themselves and their vehicles properly.

With tens of thousands of motorists set to travel across England, Highways England traffic officers will be working around the clock to deal with incidents on motorways and A-roads.

And before they set off, Highways England is urging motorists to:

- check fuel: Make sure you have enough to get to your destination.
- check tyres: Prior to setting off on a long/significant journey, check your tyre pressure and the condition of your tyres, including the spare – look out for cuts or wear and make sure the tyres have a minimum tread depth of 1.6mm, which is the legal limit
- check engine oil: Use your dipstick to check oil before any long

journey, and top up if needed – take your car back to the garage if you're topping up more than usual

- check water: To ensure you have good visibility, always keep your screen wash topped up so you can clear debris or dirt off your windscreen
- check your lights: If your indicators, hazard lights, headlights, fog lights, reverse lights or brake lights are not functioning properly, you are putting yourself at risk – in addition, light malfunctions can be a reason for your vehicle to fail its MOT

Highways England has also launched a series of specialist videos to help carry out basic vehicle checks before they set off on their travels. The videos [can be viewed on the Think! website](#)

[View a map](#) showing the locations of lifted and completed schemes.

By suspending or completing roadworks, more lanes will be open and many speed restrictions will be lifted. The roadworks will be removed by 6am on Friday 25 August 2017 and will not be put back before 00:01 on Tuesday 29 August 2017.

Those wishing to find out more about driving on smart motorways can [view our webpage](#) for further information.

Drivers planning to use the Dartford Crossing are reminded to pay Dart Charge in advance or by midnight the day after crossing.

More information can be found on our [website](#) or by calling our information line (0300 123 5000) they can keep up to date with conditions on the roads.

For more detailed information on how to carry out your vehicle checks, search Think!

General enquiries

Members of the public should contact the Highways England customer contact centre on 0300 123 5000.

Media enquiries

Journalists should contact the Highways England press office on 0844 693 1448 and use the menu to speak to the most appropriate press officer.

[Press release: Chief Trade Negotiation Adviser starts at the Department for](#)

International Trade

An internationally recognised trade expert with over 25 years of experience, Crawford will lead trade policy and the development of trade negotiation capability at DIT, following a global recruitment campaign by the department.

As Chief Trade Negotiation Adviser and Second Permanent Secretary, Crawford will be the UK government's expert on trade negotiation and strategy, and the principal adviser to the International Trade Secretary on striking trade agreements and market access deals with the UK's global trading partners.

Crawford will serve as an ambassador for DIT, engaging with international partners and trade counterparts to develop key strategic relationships, and will personally oversee pivotal trade negotiations on behalf of ministers.

Crawford will also act as the new head of profession for trade negotiators within the UK Civil Service, building, recruiting for and strengthening the department's specialist trade and negotiation capability.

Crawford Falconer brings over 25 years of public service in trade and foreign affairs to DIT. A New Zealand/UK dual-national, he was previously Professor of Global Value Chains and Trade at Lincoln University. This follows a long career at the heart of New Zealand's Foreign Office, as Deputy Secretary (Vice Minister) for International Trade and Foreign Affairs. He has also served in the OECD, as New Zealand Ambassador to the World Trade Organization, and been a judge on over 15 WTO international trade disputes.

International Trade Secretary, Dr Liam Fox said:

Crawford Falconer brings a wealth of international trade expertise to our international economic department, ensuring that as we leave the EU, the UK will be at the forefront of global free trade and driving the case for international openness.

His direct experience in global trade will prove invaluable as we build our future trading arrangements with the rest of the world.

Crawford Falconer said:

As the UK prepares to leave the EU we have a huge opportunity to be a world innovator, striking trade deals outside of Europe, and to be an ambassador for free trade across the world.

With 90% of new trade to come from outside the EU in the next decades, this is an immensely exciting time to join the Department, and I look forward to preparing for the important negotiations ahead.

[Press release: UK Public Health Rapid Support Team \(UK-PHRST\) deploys to Sierra Leone](#)

Following natural disasters, outbreaks of water borne diseases such as cholera can occur, particularly where there is a lack of access to clean water and sanitation. Given the scale of the disaster in Freetown, the local capacity to detect and control a disease outbreak is limited and the Government of Sierra Leone has requested international support.

The UK-PHRST team deploying includes experts in tracking the progress of an outbreak (epidemiologists) and diagnosing its cause (microbiologists), as well as a logistician.

The team will be working alongside Sierra Leone health system professionals and other experts in disaster relief to support the Sierra Leone government's response.

UK-PHRST is jointly run by Public Health England and the London School of Hygiene & Tropical Medicine and is funded by the UK government. It continually monitors infectious diseases and other hazards globally, identifying situations where the deployment of specialist expertise could prevent these threats from turning into a global outbreak.

Professor Daniel Bausch, Director of the UK-PHRST said:

Sierra Leone is working to stop a tragedy becoming a major public health issue. Our team of specialists will support its health professionals with enhanced surveillance for water-borne diseases, such as cholera, which often appear in the wake of extreme rainfall and flooding. The people of Sierra Leone have shown extraordinary resilience since the Ebola outbreak and we are working alongside them as we tackle this latest disaster together.

Health Minister Philip Dunne said:

This disaster is a tragedy for Sierra Leone and I am pleased our new rapid support team is helping to protect lives.

In this first bilateral deployment our specialists will save lives on the ground working with local professionals to prevent disease outbreaks. By assisting to halt the spread of disease at the

source, not only do we protect those in Sierra Leone but also citizens across the world, including the UK.

International Development Secretary, Priti Patel said:

The UK stands by Sierra Leone in its time of need, stepping up with new emergency support to get food, water and medicine to people who have lost everything.

British expertise is also leading the fight against global health threats ensuring that disease doesn't take hold in the aftermath of disasters.

The Rapid Support Team is just one way we are helping ensure that countries and the international system are better prepared to effectively tackle the preventable and treatable diseases that still plague countless people today. This will build a safer and healthier world which benefits us all.

As the UK-PHRST's deployment progresses, it will continue to provide support and share expertise with our partners in Sierra Leone to strengthen the health system beyond the immediate response.

The UK government has remained in Sierra Leone throughout the post-Ebola period, with Public Health England helping to strengthen health systems and further developing the ability to respond to such disasters and prevent outbreaks.

The London School of Hygiene & Tropical Medicine is a world authority in public and global health research, and has been conducting Ebola vaccine trials in Sierra Leone since the outbreak of the virus in West Africa.

UK-PHRST

UK-PHRST consists of public health experts, scientists, academics and clinicians ready to respond to urgent requests from countries around the world within 48 hours to support them in preventing local disease outbreaks from becoming global epidemics.

Informed by surveillance data, the UK-PHRST deploys on behalf of UK Government in response to requests from low- and middle-income countries, as well as with the WHO (World Health Organization) and the Global Outbreak and Response Network (GOARN).

The UK-PHRST has previously deployed members to Ethiopia (outbreak of Acute Watery Diarrhoea) and Nigeria (Meningitis outbreak). These deployments were under the World Health Organization's Global Outbreak and Response Network (WHO GOARN).

The core team consists of:

- epidemiologists (experts in tracking the progress of an outbreak)
- clinical researcher (developing the best clinical response measures)
- social scientist (community responses to outbreaks)
- microbiologist (diagnosing the cause of an outbreak)
- data manager, analyst, systems expert
- infection prevention and control expert (advising on outbreak control measures)
- logistician

The consortium of research institutions includes the University of Oxford and King's College London as academic partners.

Public Health England

[Public Health England](#) exists to protect and improve the nation's health and wellbeing, and reduce health inequalities. It does this through world-class science, knowledge and intelligence, advocacy, partnerships and the delivery of specialist public health services. PHE is an operationally autonomous executive agency of the Department of Health.

London School of Hygiene & Tropical Medicine

[The London School of Hygiene & Tropical Medicine](#) is a world-leading centre for research and postgraduate education in public and global health, with more than 4,000 students and 1,000 staff working in over 100 countries. The School is one of the highest-rated research institutions in the UK, is among the world's leading schools in public and global health, and was named University of the Year in the Times Higher Education Awards 2016. Our mission is to improve health and health equity in the UK and worldwide; working in partnership to achieve excellence in public and global health research, education and translation of knowledge into policy and practice.

[Press release: Two in three bosses at Britain's biggest businesses not trained to deal with a cyber attack](#)

- New reports highlight scale of the cyber security and data protection challenge
- One in ten FTSE 350 companies operate without a response plan for a cyber incident
- Only six per cent of businesses completely prepared for new data protection rules
- Separate new research finds charities are as susceptible to attacks as businesses Undertaken in the wake of recent high profile cyber attacks, the survey of the UK's biggest 350 companies found more than two thirds

of boards had not received training to deal with a cyber incident (68 per cent) despite more than half saying cyber threats were a top risk to their business (54 per cent).

One in ten FTSE 350 companies said they operate without a response plan for a cyber incident (ten per cent) and less than a third of boards receive comprehensive cyber risk information (31 per cent).

Minister for Digital Matt Hancock said:

We have world leading businesses and a thriving charity sector but recent cyber attacks have shown the devastating effects of not getting our approach to cyber security right.

These new reports show we have a long way to go until all our organisations are adopting best practice and I urge all senior executives to work with the National Cyber Security Centre and take up the Government's advice and training.

Charities must do better to protect the sensitive data they hold and I encourage them to access a tailored programme of support we are developing alongside the Charity Commission and the National Cyber Security Centre.

There has been progress in some areas when compared with last year's health check, with more than half of company boards now setting out their approach to cyber risks (53 per cent up from 33 per cent) and more than half of businesses having a clear understanding of the impact of a cyber attack (57 per cent up from 49 per cent).

The Government is fully committed to defending against cyber threats and a five-year National Cyber Security Strategy (NCSS) was announced in November 2016, supported by £1.9 billion of transformational investment. This includes opening the National Cyber Security Centre and offering free online advice as well as training schemes to help businesses protect themselves.

The 10 Steps to Cyber Security guide sets out a comprehensive framework to help company boards manage cyber risks, from getting the basics right through to protecting their most critical assets, and the Cyber Essentials scheme sets out the technical basics all companies should have in place.

Earlier this week, Government also announced proposals on how to help the nation's essential industries be more resilient to cyber threats through the NIS Directive.

Alex Dewdney, NCSC Director for Engagement, said:

The NCSC is committed to making the UK the safest place in the world to live and do business online.

We know that we can't do this alone – everyone has a part to play. That's why we're committed to providing organisations with expert advice through our website and direct engagement.

We also urge organisations to follow the guidance in the Government's Cyber Essentials Scheme.

Separate new research looking at the cyber security of charities has also been published today.

It found charities are just as susceptible to cyber attacks as businesses, with many staff not well informed about the topic and awareness and knowledge varying considerably across different charities. Other findings show those in charge of cyber security, especially in smaller charities, are often not proactively seeking information and relying on outsourced IT providers to deal with threats.

Where charities recognised the importance of cyber security, this was often due to holding personal data on donors or service users, or having trustees and staff with private sector experience of the issue. Charities also recognised those responsible for cyber security need new skills and general awareness among staff needs to raise.

Helen Stephenson CBE, Chief Executive at the Charity Commission for England and Wales, said:

Charities have lots of competing priorities but the potential damage of a cyber-attack is too serious to ignore. It can result in the loss of funds or sensitive data, affect a charity's ability to help those in need, and damage its precious reputation. Charities need to do more to educate their staff about this threat and ensure they dedicate enough time and resources to improving cyber security.

We want to make sure charities are equipped to do this, and we encourage them to use the advice on our Charities Against Fraud website. We also continue to work closely with the Department for Digital, Culture, Media and Sport to help charities protect themselves online.

The FTSE 350 Cyber Governance Health Check is the Government's annual report providing insight into how the UK's biggest 350 companies deal with cyber security.

The Government will soon be introducing its new Data Protection Bill to Parliament. With this coming into effect next May, implementing the General Data Protection Regulation (GDPR), the report for the first time included questions about data protection.

The new data protection law will strengthen the rights of individuals and

provide them with more control over how their personal data is being used.

The report found:

- Awareness of GDPR was good, with almost all firms (97 per cent) aware of the new regulation
- Almost three quarters (71 per cent) of firms said they were somewhat prepared to meet the GDPR requirements, with only 6 per cent being fully prepared
- Just 13 per cent said GDPR was regularly considered by their board
- 45 per cent of Boards say they are most concerned with meeting GDPR requirements relating to an individual's right to personal data deletion

The Information Commissioner's Office has produced guidance for organisations on implementing the regulation, including a checklist for businesses on the actions they need to take; and a series of interactive workshops and webinars.

The ICO will also produce guidance for organisations about the responsibilities under the GDPR and individuals on their rights under the GDPR. The Department for Digital, Culture, Media and Sport will continue to work closely with the Information Commissioner's Office (ICO) during this transitional period.

Note to editors:

Media enquiries – please contact the DCMS News and Communications team on 020 7211 2210 or out of hours on 07699 751153.

The FTSE 350 Cyber Governance Health Check is carried out in collaboration with the audit community, including Deloitte, EY, KPMG and PWC:
<https://www.gov.uk/government/publications/cyber-governance-health-check-2017>

The Cyber Security Among Charities report covers the findings from qualitative research undertaken with UK registered charities:
<https://www.gov.uk/government/publications/cyber-security-in-charities>

The Department for Digital, Culture, Media & Sport (DCMS) has commissioned the [UK Cyber Security Sectoral Analysis Survey](#) to provide statistics about the size, scale and future opportunities for the UK's Cyber Security industry.

The reports are part of the Government's £1.9 billion investment to significantly transform the UK's cyber security. The National Cyber Security Strategy sets out how the UK Government will deliver a UK that is secure and resilient to cyber threats; prosperous and confident in the digital world. The National Cyber Security Programme managed by the Cabinet Office coordinates the work undertaken to implement the UK's National Cyber Security Strategy. Further information is available at www.gov.uk/cybersecurity

Annex

Paul Taylor, UK head of Cyber Security at KPMG, said:

“Cyber-attacks continue to pose a growing threat to business. While cyber security has cemented itself onto the board’s agenda, they often lack the training to deal with incidents. This is hugely important as knowing how to deal confidently with an incident in the heat of the moment can save time and money. The aftermath of a cyber-attack, without the appropriate training in managing the issue, can result in reputational damage, litigation and blunt competitive edge.”

Zubin Randeria, cyber security leader at PwC, said:

“The report’s findings echo those of the PwC CEO Survey, which found that three-quarters of UK CEOs consider cyber risks to be a significant threat to their business and 97% are addressing cyber incidents. It’s positive that cyber security is now front of mind for boards and business leaders, but concerning that many still are not equipping themselves with the right knowledge to respond when the worst does happen. Cyber security attacks are now an everyday reality and it’s the responsibility of business leaders to make sure they’re prepared.

“The most successful leaders will be those who take an active involvement in cyber security governance and set the tone from the top – this is not an issue just to delegate to more technical teams. Investors, customers, the media and the general public all routinely scrutinise companies’ responses to cyber security incidents, as we’ve seen from the recent ransomware attacks. Companies that fail to prepare to respond to a breach also leave themselves exposed to a damaging commercial and reputational backlash.”

Phill Everson, head of cyber risk services at Deloitte, said:

“This year’s report marks a clear improvement in board level awareness of cyber risks and their impacts, driven in large part by high profile, cross-sector incidents. There is still some way to go, though, as the findings show that many boards still do not have a defined role to lead a company-wide response. This corroborates with recent Deloitte analysis of FTSE 100 annual reports, which found that just 5% disclose having a board member with specialist technology or cyber experience.

“As well as greater awareness of the financial and reputational impact of a cyber breach, preparedness is also key to a successful response. From May next year, cyber breaches will have to be reported within 72 hours under General Data Protection Regulation (GDPR). This is significantly sooner than the period that many companies have historically alerted customers, which often runs into many months. As hackers become increasingly more sophisticated, companies will have to ensure that staff training and technology stays ahead of the evolving cyber threat to respond in a timely and effective manner.”

Stuart Whitehead, UKI Head of Cybersecurity, Privacy & Resilience at EY said:

“Cyber is an ever increasing threat to the UK economy and although we are glad to see that this latest survey of the UK’s largest organisations illustrates that cyber is increasingly a board level priority, there is still some way to go to best prepare organisations for a potential breach. With the current backdrop, the cyber agenda is evolving into a conversation about organisations’ resilience to cyber-attacks. This is not only how organisations protect themselves but how they respond to an incident, recover business processes and limit the impacts to revenue and reputation. The increase in Board level attention is encouraging, but greater emphasis will be required over the coming years to truly improve the security posture of organisations across the UK.”