Joint statement from COP26 President Alok Sharma and Italian Ecological Transition Minister Roberto Cingolani

Press release

In a joint statement, COP26 President, Alok Sharma and Italian Ecological Transition Minister, Roberto Cingolani, show the UK and Italy's commitment to COP26 and international collaboration on climate change.



COP26 President Alok Sharma and Italian Ecological Transition Minister Roberto Cingolani met on 11 May 2021 in Rome. They released the following statement:

During this year of the UK-Italy COP Presidency, we stand together on the need to build back better following the devastating impact of COVID-19.

The UK and Italy are committed to putting climate and nature at the heart of the multilateral agenda in 2021, including through the G7, G20 and COP26 Presidencies. Through our Presidencies, we will work closely to achieve progress on the most vital issues of our age, and encourage countries to take concrete actions towards our shared climate goals.

We are pleased that all G7 countries have now committed to net zero by 2050 at the latest, providing a vital step forward towards reducing global emissions. We now urge all countries to do their part and to take the steps needed to keep the 1.5 degree Celsius temperature limit within reach, including through setting ambitious nationally determined contributions and long-term strategies to cut emissions and reach net zero.

Together, we recognise the importance of working with the world's most vulnerable, to support them to adapt and respond to climate impacts and to scale up finance and private investment for both mitigation and adaptation, including the greater use of nature based solutions.

We reaffirm our strong and steadfast commitment to strengthening

implementation of the Paris Agreement and to unleashing its full potential. We look forward to working with all countries, businesses and civil society both at the pre-COP and the COP26 Climate Conference, to help build momentum towards a successful outcome. We stress the importance of raising awareness on climate action, especially among the youth.

We are firmly committed to working together to advance the climate agenda, and are pleased to reaffirm the strength of our partnership.

Published 11 May 2021

New 'We Offer Testing to our Staff' scheme launched

- New sticker scheme launched allowing UK businesses to display their offer of free testing for staff alongside materials promoting use of the NHS COVID-19 app to check in customers and visitors
- Alongside the vaccine rollout and checking in with the NHS COVID-19 app, regular testing is at the heart of plans to reopen society and the economy, helping to prevent the spread of variants

A new scheme for businesses offering workplace testing for staff through NHS Test and Trace has been launched across the UK. It will show customers, employees and the wider public the businesses that are going the extra mile to keep their staff and the public safe.

In addition to workplace testing, business owners and staff should all follow essential behaviours such as 'Hands, Face, Space, Fresh Air' and, where applicable, checking customers and visitors in using the NHS COVID-19 app.

Businesses that offer rapid workplace testing to staff, either through onsite testing or workplace test collection, will be able to download posters and stickers to demonstrate their offer for free, regular testing to their employees keeping people safe.

More than 122,000 businesses have signed up for free workplace testing already, using free government-supplied rapid test kits from NHS Test and Trace. All organisations that registered before 12 April and self-declared their involvement are eligible for the scheme.

Participating firms will be able to access digital assets including stickers and posters from Tuesday 11 May, and can be accessed by participating firms online via the online ordering platform.

Health Minister Lord Bethell said:

Through this new scheme participating businesses can proudly display their contribution to our national recovery and their support to public health, while also reassuring staff and customers in the process. Around 1 in 3 people with coronavirus do not show any symptoms so every day rapid testing is helping us find cases of COVID-19 we wouldn't otherwise know about, breaking chains of transmission and saving lives.

Regaining our lost freedoms depends on all of us getting tested regularly. There are more ways for people to access free rapid tests than ever before, and I'm grateful to all the businesses for their contribution to this scheme and to our national recovery effort.

Business Minister Paul Scully said:

Businesses across the UK have been hard at work ensuring they are reopening safely, in line with public health guidance, and more than 120,000 firms have gone even further by answering our call to sign up for free workplace testing.

Today's announcement means people can work and shop with the peace of mind that more rapid tests are being taken, more cases are being detected, and more lives are being saved.

Jenny Harries, CEO of the UK Health Security Agency (UKHSA), said:

Businesses participating in the workplace testing scheme can now demonstrate that the health of their staff, customers and the communities they serve is a key priority by prominently displaying these stickers.

Alongside 'Hands, Face, Space, Fresh Air' and, where applicable, checking customers and visitors into their premises, workplace testing has a crucial role to play in safely taking the next step out of lockdown.

By prominently displaying the stickers on their websites or on their premises, alongside existing materials which promote checking customers and visitors in, businesses will be able to demonstrate to their customers that the health of staff, customers and their local communities is a key priority.

Around 1 in 3 people with COVID-19 do not experience any symptoms and may be spreading the virus unwittingly. Rapid testing detects cases quickly, meaning positive cases can isolate immediately. Since rapid testing was introduced, over 152,000 positive LFD results have been returned, detecting asymptomatic cases of COVID-19 that may not otherwise have been found and potentially saving lives. By making rapid tests available to everyone, more cases will be

detected, helping to break chains of transmission and save lives.

Alongside the rollout of the vaccine, regular testing is likely to be an essential part of the easing of restrictions as it will help quickly find cases and suppress the spread of variants. Through associated new testing technology, positive cases of variants of concern are being detected faster than ever before. Greater volumes of testing make it easier to identify and control variants.

Getting a rapid test

Getting a rapid test is quick and convenient. In addition to the free workplace testing offer, anyone in England can now access free, twice-weekly rapid testing through the following channels:

- a home ordering service, which allows people to <u>order lateral flow tests</u> <u>online</u> to be delivered to their home
- community testing, offered by all local authorities
- collection at local PCR testing sites during specific test collection time windows
- testing on-site at schools, colleges and other educational settings
- a new 'Pharmacy Collect' service, where people aged over 18 without symptoms will be able to visit a participating local pharmacy and collect a box of 7 rapid tests to use twice a week at home

If testing at home, individuals will need to <u>register their results online</u> or by calling 119. They should self-isolate if positive and order a confirmatory PCR test.

Anyone with symptoms of COVID-19 should book a test online or by calling 119.

Background information

NHS Test and Trace is part of the UKHSA.

Read the guidance on 'We Offer Testing to our Staff'.

Health is a devolved matter and eligibility to access these 2 different types of asymptomatic testing differs across the 4 nations. Please check and follow your nation's guidelines.

James Webb Space Telescope/MIRI

The UK in the James Webb Space Telescope

Looking back in time

NASA's James Webb Space Telescope (JWST) will look further back in time than any other telescope — to 400m years after the Big Bang. JWST is a collaboration between ESA, NASA and the Canadian Space Agency, due for launch in late 2021 as the replacement for the Hubble Space Telescope.

The four key goals of the JWST are:

- to search for light from the first stars and galaxies that formed in the Universe after the Big Bang
- to study the formation and evolution of galaxies
- to understand the formation of stars and planetary systems
- to study planetary systems and the origins of life

These goals can be accomplished more effectively by observation in near-infrared light rather than light in the visible part of the spectrum. For this reason, the JWST's instruments will not measure visible or ultraviolet light like the Hubble Telescope, but will have a much greater capacity to perform infrared astronomy.

JWST will also study the atmospheres of exoplanets identified by the European Space Agency PLATO science mission — necessary to understand their potential for hosting life. Securing a leading role on this prestigious NASA mission ensures that UK scientists remain at the forefront of global space science research. As the successor to Hubble, Webb is expected to generate even more astonishing images of our Universe, inspiring the next generation of UK researchers and engineers.

What will the JWST do?

To study these distant objects the telescope will use infrared light and must be cooled to within a few tens of degrees above Absolute Zero or -273°C. This is to prevent radiation from the telescope and its instruments swamping the astronomical signals. To achieve this Webb will have a huge multi-layer sunshield which is the area of a tennis court.

The below time-lapse video reveals NASA's James Webb Space Telescope under construction. (Credit: NASA Goddard)

JWST time-lapse

To capture the very faint signals Webb's main telescope mirror is 6.5 metres in diameter, the largest ever flown in space, and is gold-coated to optimise its ability to reflect infrared light. Its 18 segments will fold up inside the rocket for launch, then unfold in space.

Webb's Integrated Science Instrument Module (ISIM) will house four instruments, which are:

UK leading the build

The UK leads the European Consortium to build the Mid InfraRed Instrument (MIRI). MIRI will 'see' faint infrared (IR) light invisible to the human eye and will peer far into the past observing very distant galaxies and newly forming stars and planets. MIRI uses IR because unlike visible light, it can penetrate the dense dust clouds which surround newly forming stars and planets.

The UK provided the scientific leadership on MIRI and the instrument design and managed the overall project. The UK was also responsible for the overall construction of the instrument and the quality control to ensure that MIRI would operate as intended and cope with the harsh conditions of space.

MIRI was the first instrument to be delivered to NASA, in May 2012. Since delivery, it has been integrated and tested with the other science instruments and the telescope.

MIRI was built for ESA by a European Consortium of 10 countries, led by Principal Investigator Prof Gillian Wright at the Science and Technology Facilities Council's UK Astronomy Technology Centre. The European Consortium works in partnership with a team at NASA's Jet Propulsion Lab, who have contributed the detectors and cryo-cooler for MIRI.

Mission facts

The UK (UK Space Agency since 2011 and STFC) has invested almost £20 million in the development phase of MIRI and has continued to support essential post-delivery testing, integration, calibration and characterisation activities by the UK MIRI team at NASA's Goddard Space Flight Centre, Johnson Space Centre and more recently at prime contractor Northrop Grumman in California.

This work is critical to understanding the instrument behaviour in operations and optimising the interpretation for the science data which will eventually be returned from the mission.

<u>STFC's UK Astronomy Technology Centre</u> contributes the Instrument Science Leadership though Prof Wright, along with the optical design/engineering and calibration sources.

Other UK institutes involved in MIRI are:

A full list of people from across the UK that are playing an active role in the JWST can be found on this page.

In March 2021 Space Telescope Science Institute (STScI) announced the selected JWST General Observer programs for Cycle 1. The selected proposals were prepared by more than 2,200 unique investigators from 41 countries, including 43 US states and territories, 19 ESA member states, and 4 Canadian provinces. More detailed information about the approved proposals can be found here.

The NASA/ESA/CSA James Webb Space Telescope successfully launched on an Ariane 5 rocket from Europe's Spaceport in French Guiana on 25 December 2021.

For more information, visit the NASA, ESA and JWST UK websites.

Response to commissioning letter

We use some essential cookies to make this website work.

We'd like to set additional cookies to understand how you use GOV.UK, remember your settings and improve government services.

We also use cookies set by other sites to help us deliver content from their services.

Home Secretary Priti Patel speech to CyberUK Conference

Good afternoon,

Let me start by thanking Lindy and the whole National Cyber Security Centre team for inviting me to join you today.

Today we are discussing many of the most challenging and important issues we face as a country. In light of the seriousness of these topics it is a privilege for me, as Home Secretary, to outline my priorities and observations on cyber security with you.

The efforts of the NCSC and the work you all do to protect our country in cyberspace are simply outstanding.

These efforts may not always be front page news, but in my role I know what you do here is at the forefront of defending our nation and keeping our people safe.

British businesses and the public are safer because of these efforts and the way in which you work to bring together intelligence and technology to protect people and our institutions.

Cyber continues to revolutionise the way we all live.

The last year has brought that home more than ever before.

Online communications, traffic and the volume that we see on online platform continues to grow.

And that impacts how we guard our own national security and brings new challenges while highlighting new threats, often exposing many new gaps that we have to close.

Cyber is now a core component of our homeland security mission, with effective cyber defences critical to making the UK a responsible Cyber Power, as set out in our recently published Integrated Review.

We are taking a new, comprehensive approach to strengthen our position as a democratic cyber power.

Protecting and promoting our interests in cyberspace, while also detecting, disrupting and deterring our adversaries.

While continuing to shape, influence and unlock tomorrow's technologies and opportunities so they are safe, secure and open.

We want to make the United Kingdom, and the lives and livelihoods of our people, stronger and more resilient to the threats we face and ready for the opportunities ahead.

As Home Secretary, it is my responsibility and duty to keep our citizens safe and the country secure, while protecting economic prosperity.

Cyber security and resilience are increasingly important and integral parts of my job. This includes our domestic response to all kinds of cyber threats, whether they be from states with hostile intent, organised criminals, terrorists, or from elsewhere.

Throughout the last year, we responded to new threats, including working with the pharmaceutical industry and the NHS to help protect them from the cyber threats they faced while working to develop vaccines to beat COVID-19.

As all of you in this audience will be aware, the threats facing the UK in the cyberspace — to our citizens, our businesses, academia and to the government — are real and significant.

The picture is diverse, spanning state and state-sponsored actors, organised crime groups, and criminals seeking to profit by defrauding citizens and businesses online.

The scale of this type of criminality is truly shocking. In the year ending September 2020, there were an estimated 1.7 million cyber dependent crimes experienced by adults in England and Wales.

The overall cost of computer misuse incidents against individuals, including hacking into personal computers and email accounts and stealing of personal data and imagery, has been estimated at over £1 billion.

And nearly 2 out of every 5 businesses in the UK identified at least one

cyber security breach or attack in the last 12 months.

These are not just statistics. The impact of these breaches and attacks have a profound and lasting impact on people and their lives and livelihoods.

These crimes are not victimless. They cause real harm to people and businesses.

One of the biggest challenges we face in tackling these threats is the breadth of ways in which they can manifest themselves, often causing both financial suffering and long term damage.

The use of networked cameras to spy on and harass individuals...

The operation of criminal websites that sell compromised details, fuelling further cyber crimes and fraud...

The attack by criminals on services essential to the economy, such as the attack on fuel pipelines in the US last week...

And as you will have heard earlier from the CEO of Solar Winds, cyber operations are often highly sophisticated, and many are very likely to be state sponsored.

The hack on Solar Winds has shown that state actors have significant capability. We need to be able to understand that threat, protect ourselves from it, and bolster our cyber resilience.

While addressing the danger from state and state-sponsored actors, it is rightly a key priority.

We also know that criminal groups have the intent and technical means to operate in cyber space.

The NCSC Annual Report sets out that ransomware incidents handled by the Centre have been increasing.

Cyber criminals have increasingly focused on companies and organisations. Taking the time to research their target so they can maximise their chances of releasing higher sums of money through extortion.

In the face of such complex and often inter-linked threats, it is crucial that we join ourselves up, and have a clear and effective response so that our citizens and businesses are safe and can operate safely and securely online.

Government has a strong position against paying ransoms to criminals, including when targeted by ransomware. Paying a ransom in response to ransomware does not guarantee a successful outcome.

It will not protect networks from future attacks, nor will it prevent the possibility of future data leaks. In fact, paying a ransom is likely to encourage criminals to continue to use this approach.

There is action that organisations can take.

Be as prepared and engage with the NCSC and law enforcement as soon as you can, so they can assist with understanding and mitigating the incident.

Understand the consequences of an incident and how it will affect your organisation in the future. This is not just about loss of data; there can be real disruption and significant impacts.

Learn from incidents - prepare and exercise your response.

Ransomware, like other cybercrime types, has no boundaries. The challenge of investigating and identifying those responsible is one we share with our international partners.

Recently, Five Eyes interior ministers have agreed to work together to prevent, discourage and counter the threat of ransomware.

The threats we face are significant and evolving. But just as our adversaries are continually developing their tactics, we are always seeking new ways to bolster our defences.

And we are making progress. Funding from the National Cyber Security Programme has completely transformed our capability — from improving the response of local police forces through bringing the most sophisticated organised crime groups to justice.

We have also created the National Cyber Force to help transform the UK's ability to counter and deter adversaries, and further our interests and promote our values.

We are also taking action to tackle the truly horrific levels of online child sexual abuse and exploitation, with law enforcement agencies, making an estimated 800 arrests and safeguarding or protecting over 1,000 children every month.

The key in all of this is to increase our resilience; from the most critical and important systems right through to PCs, tablets and smartphones — the very tools and devices used every single day — but to put the right protections in place to deliver on our ambition of making the UK the safest place to be online.

As a world-leading organisation in its field, the NCSC has a pivotal role to play, working across government and with industry to drive improvements in cyber security.

We have also set up the cyber Protect Network and Cyber Resilience Centres to boost the support provided by police to the public and businesses.

These are, of course, international issues. And that means the relationships we have with partners around the world, including our Five Eyes allies, are more important than ever before.

As I have set out, we are making progress. But we cannot stand still — this work is simply too important.

So we will, as promised in the Integrated Review, develop a comprehensive cyber strategy that will set out how we will maintain the UK's competitive edge and counter the threats from cyberspace.

In line with this ambition, it is critical that government has all the right levers available to ensure that those who commit criminal acts in cyberspace are effectively investigated by law enforcement, and prosecuted by our criminal justice system.

Including those perpetrating the most heinous and appalling crimes against children or those committing serious fraud.

The Computer Misuse Act has proved to be an effective piece of legislation to tackle unauthorised access to computer systems, and it has been updated a number of times to take account of changes we now face.

Alongside the Act, there is also separate legislation that provides powers for law enforcement agencies to investigate both cyber-dependent and cyber-enabled crimes.

As part of ensuring that we have the right tools and mechanisms to detect, disrupt and deter our adversaries, I believe now is the right time to undertake a formal review of the Computer Misuse Act.

And today I am announcing that we will be launching a call for information on the Act this year.

I would urge you all to provide your open and honest views on ensuring that our legislation and powers continue to meet the challenges posed by the threats in cyberspace.

Before I finish, I want to thank you again for the opportunity to speak to you today — and for all of the work that you do.

These are complex challenges, these are difficult issues, so it is absolutely vital that we work together closely to confront them.

We have made great strides, and we all know there is more to do.

My message to all of you working across the public and private sector to fend off cyber criminals and hostile state actors is simple: keep it up.

Your contributions and work are crucial if we are to stay one step ahead of our adversaries.

Ultimately, this is about keeping our citizens, our businesses, and our national security safe, and as Home Secretary that will always be my number one priority.

Thank you.