AAIB achieves Silver Investors in People Accreditation

News story

The AAIB has once again achieved the coveted Investors in People Silver Accreditation.

Crispin Orr, Chief Inspector of Air Accidents said: “This is a great achievement for the Branch and we have much to celebrate. Further significant progress has been made since the last assessment, with an additional three indicators rated as ‘Advanced’. The report notes that Silver accreditation is a good result, especially within these challenging times. Achievement of Gold accreditation is a realistic ambition.

“The report contains many encouraging observations and some good pointers where further improvements can be made. It is highly relevant and important feedback in our journey to create a dynamic and inclusive working environment in which all staff can flourish.”

Published 19 July 2021

Royal Statistical Society Award

A cross-organisation team, which included 2 actuaries from the Government Actuary’s Department (GAD), has won a Royal Statistical Society Award.

The 2021 Florence Nightingale Award for Excellence in Healthcare Data Analytics has gone to The Covid-19 Population Risk Assessment, powered by QCovid. It is a predictive model used to estimate the risk of serious health outcomes due to COVID-19 for individuals.

The award, supported by the Health Foundation charity, celebrates data analysts in the UK health and care sector. It is for people whose work has demonstrably delivered better outcomes for patients and the healthcare system.

Cross organisational team

The team included GAD actuaries Nazmus Haq as a senior analyst, and Dhanisha Sanghrajka as a deputy director. The actuaries worked as part of the Department of Health and Social Care (DHSC).

The rest of the team included experts from the NHS, NHS Digital, the Office for National Statistics, NERVTAG, as well as Cambridge and Oxford Universities.

Predictive model

They produced a predictive model, QCovid. This combines information from several datasets to estimate a person's risk of catching and subsequently being hospitalised or dying from COVID-19. It did this by focusing on demographic factors such as age, ethnicity, gender, and body mass index. The model also examined economic factors such as deprivation, pre-existing medical conditions and ongoing treatments.

This technique meant at-risk adults in England could be identified, prioritised for vaccination, and added to the national shielded patients list.

Ingenuity and collaboration

Actuary Nazmus Haq says he is very proud to be part of this successful project: "The fact that our team has been given the top award in this category is a testament to the ingenuity, hard work and collaborative spirit of everyone involved. I am especially pleased too as it shows how our data analytics expertise has made a real difference to people's lives."

For more on his experiences working at DHSC on this project, read Nazmus Haq's blog. In GAD and COVID-19 he reflected on his year of being part of the team supporting the government in its ongoing fight against the pandemic.

FCDO statement: Venezuela gold case in Supreme Court and legal arguments

News story

FCDO Legal Counsel is presenting arguments on behalf of the Foreign Secretary in the Supreme Court hearing over the rights of access to gold held by the Bank of England and owned by the State of Venezuela.

The illegitimate Maduro regime has claimed rights of access over gold held in the Bank of England on behalf of the State of Venezuela.

The UK government is clear that Juan Guaido has been recognised by HMG since February 2019 as the only legitimate President of Venezuela.

An FCDO spokesperson said:

> The UK government has the right to decide who to recognise as the legitimate head of a foreign state. The UK recognises Juan Guaidó as President of Venezuela and consequentially he is the only individual recognised to have the authority to act on behalf of Venezuela as its head of state.
>
> Venezuela needs a peaceful transition to democracy with free and fair elections, both legislative and presidential.

Published 19 July 2021

Recovery funding for the light rail sector

Light rail is a lifeline for many communities across the UK. During the pandemic, the government has provided significant levels of financial assistance to the light rail sector through the Light Rail Revenue Grant and the Light Rail Restart Revenue Grant, supporting 6 light rail operators and local transport authorities in England, outside of London, with over £200

million in funding since March 2020.

To date, the Light Rail Restart Revenue Grant has funded up to 100% of pre-COVID-19 service levels, ensuring key workers have continued to be able to travel easily and safely, as well as ensuring the public could access necessary amenities.

Critically, as restrictions are lifted and passengers return, the light rail sector is important in helping local economic recovery, thereby supporting the government's 'levelling-up' agenda.

To encourage passengers back, light rail services should be as available as they were prior to the pandemic. Without support, however, it may not be possible for operators to maintain the services they have provided up until now.

I can, therefore, announce that a further £56 million in financial support in the form of recovery funding has been made available for the light rail sector. Funding operators and local authorities from 20 July 2021 until the end of this financial year, this will succeed the Light Rail Restart Revenue Grant, which ends on 19 July 2021.

This funding will support operators in adapting their commercial offerings to ensure the longer-term viability and self-sustainability of the sector and is intended to be the final tranche of COVID-19-related support.

UK and allies hold Chinese state responsible for a pervasive pattern of hacking

Press release

UK joins likeminded partners to confirm Chinese state-backed actors were responsible for gaining access to computer networks via Microsoft Exchange servers.

The UK is joining likeminded partners to confirm that Chinese state-backed actors were responsible for gaining access to computer networks around the world via Microsoft Exchange servers.

The attacks took place in early 2021, affecting over a quarter of a million servers worldwide.

Foreign Secretary Dominic Raab said:

> The cyber attack on Microsoft Exchange Server by Chinese state-backed groups was a reckless but familiar pattern of behaviour.
>
> The Chinese Government must end this systematic cyber sabotage and can expect to be held account if it does not.

The attack was highly likely to enable large-scale espionage, including acquiring personally identifiable information and intellectual property. At the time of the attack, the UK quickly provided advice and recommended actions to those affected and Microsoft said that by end of March that 92% of customers had patched against the vulnerability.

Today the UK is also attributing the Chinese Ministry of State Security as being behind activity known by cyber security experts as “APT40” and “APT31”.

Widespread, credible evidence demonstrates that sustained, irresponsible cyber activity emanating from China continues.

The Chinese government has ignored repeated calls to end its reckless campaign, instead allowing its state-backed actors to increase the scale of their attacks and act recklessly when caught.

This coordinated action today sees the international community once again urge the Chinese government to take responsibility for its actions and respect the democratic institutions, personal data and commercial interests of those with whom it seeks to partner.

The UK is calling on China to reaffirm the commitment made to the UK in 2015 and as part of the G20 not to conduct or support cyber-enabled theft of intellectual property of trade secrets.

Notes to editors

- As part of a cross-Government response, the National Cyber Security Centre (NCSC) issued tailored advice to over 70 affected organisations to enable them successfully to mitigate the effects of the compromise.
- In 2018, the UK government and its allies revealed that elements of the Chinese Ministry of State Security (MSS) were responsible for one of the most significant and widespread cyber intrusions stealing trade secrets. [link]
- The European Union has also made an announcement today [link].

The National Cyber Security Centre has assessed that:

Actors	Activity	NCSC Assessment
HAFNIUM	Compromising Microsoft Exchange gave the perpetrator a foothold to pivot further into the IT networks of victims.	NCSC is almost certain that the Microsoft Exchange compromise was initiated and exploited by a Chinese state-backed threat actor. NCSC judge it highly likely that HAFNIUM is associated with the Chinese state. The attack was highly likely to enable large-scale espionage, including acquiring personally identifiable information and intellectual property.
APT40, TEMP.Periscope, TEMP.Jumper. Leviathan	Targeting maritime industries and naval defence contractors in the US and Europe. Targeting regional opponents of the Belt and Road Initiative. Targeting multiple Cambodian electoral entities in the run up to the 2018 election.	NCSC judge it is highly likely that APT40 is linked to the Chinese Ministry of State Security and operates to key Chinese State Intelligence requirements. NCSC judge that APT40 is highly likely sponsored by the regional MSS security office, the MSS Hainan State Security Department (HSSD).
APT31, Judgement Panda, Zirconium, Red Keres	Since 2020 targeting government entities, political figures, contractors and service providers. European countries. Targeting Finnish Parliament in 2020.	NCSC judge it is almost certain that APT31 is affiliated to the Chinese State and likely that APT31 is a group of contractors working directly for the Chinese Ministry of State Security.

Published 19 July 2021