# Sharing intelligence and expertise with U.S.

News story

In support of the security of both nations and our allies, the Ministry of Defence maintains a strong relationship with the US Department of Defense.

Honorable Ron Moultrie with General Sir Jim Hockenhull

Strategic Command, which leads on cyber activity for Defence, plays a key role in sustaining and advancing this relationship.

Recently UKStratCom hosted Honorable Ron Moultrie, U.S. Under Secretary for Intelligence and Security, during his visit to the UK for a series of engagements with Defence personnel.

Defence Intelligence facilitated a series of discussions between Hon Ron Moultrie and UK officials on the operational use of intelligence, including with newly appointed Chief of Defence Intelligence Adrian Bird CB.

Hon Moultrie also visited several Strategic Command sites to understand more about how the organisation uses digital capabilities and intelligence to benefit operations and military effectiveness.

Speaking on the visit, Commander Strategic Command General Sir Jim Hockenhull said

> At Strategic Command our aims of accelerating the digitisation of Defence go hand in hand with the effective use of intelligence and data.
>
> The U.S. is our foremost ally and partner in this area, and our working relationship in various domains, including cyber, helps to protect us from an array of threats.

Published 9 November 2022

---

# Putin’s failures are becoming apparent to the Russian people: UK statement to the OSCE

Thank you, Mr Chair. It is now over 250 days since we, along with the rest of the world, witnessed the start of President Putin’s unprovoked, premeditated and barbaric attack on Ukraine. Throughout this time, we have highlighted the truth in the face of Russia’s disinformation and propaganda. In addition to the horrendous violence Russia has and continues inflict on the Ukrainian people, there has been an enormous cost to the people of Russia too. Thousands of young Russian lives have been lost on land, at sea and in the air; fighting in an illegal war of choice based on contrived rationales, confused narratives and shifting goals. This is not conjecture, this is not opinion, it is fact.

The failures of Putin’s horrendous adventurism are becoming increasingly apparent to the Russian people. They are becoming increasingly aware that their recently mobilised family members, neighbours and friends are being badly trained, badly equipped and then sent to the battlefield to reinforce poorly equipped, poorly led and demoralised professional soldiers. It is perhaps no wonder then that so many Russians have chosen to flee their own country to avoid mobilisation.

Meanwhile, on the battlefield, Russian military leaders continue to commit more and more Russian troops to the war in an attempt to overcome their failures. Due to low morale and a reluctance to fight, Russian forces have now reportedly started to deploy “barrier troops” or “block units”. These units threaten to shoot their own retreating soldiers in order to compel offensives.

Low morale, indiscipline and dysfunction continues to reach the highest levels of Russia’s military leadership too. On 3 November, Major General Alexander Linkov was reportedly appointed acting commander of Russia’s Central Military District. Linkov replaces Colonel General Alexander Lapin who was purportedly removed from office at the end of October. If confirmed, this is just the latest in a series of dismissals of senior Russian military commanders since the onset of the invasion last February, including the Commanders of the Eastern, Southern, and Western Military Districts. A pattern of blame against senior Russian military commanders for failures to achieve President Putin’s objectives on the battlefield.

It is worth noting that Colonel General Lapin had been widely criticised for poor performance on the battlefield in Ukraine by both Chechen leader Ramzan

Kadyrov and Wagner head Yevgeny Prigozhin.  The latter appears to be gaining increasing influence in the Kremlin, with his private military company being increasingly relied upon to provide fundamental security tasks normally expected of the Russian State.

For example, on 6 November, Prigozhin announced the creation of centres for the training and management of “people’s militias” in Belgorod and Kursk oblasts in

Russia. These “people’s militias” probably function outside the Russian MOD’s structure and chain of command. Their stated intent is to establish units to help defend Russia’s borders.

Meanwhile, as Russia scrambles to fortify its defensive lines throughout eastern Ukraine, Prigozhin announced the construction of a fortified ‘Wagner Line’ of defences in Luhansk oblast. The construction represents a significant effort to prepare defences in depth behind the current Russian front line and protect a key logistics line of communication.

However, as we noted last week, Wagner’s recruitment of Russian convicts including individuals suffering from serious diseases and medical conditions, is a sign of desperation to recruit numbers not fighters.  According to the Ukrainian Centre for Researching and Combating Hybrid Threats, 500 Wagner recruited convicts had died fighting in Ukraine by mid-October. In total, the centre assesses 800-1000 Wagner recruits have likely died in Ukraine. Wagner numbers have been further depleted by substantial non-fatal casualties.

That Wagner, a private military company linked to human rights abuses, is being increasingly relied upon to conduct roles normally expected of a government’s security and military apparatus is itself a telling indicator of the parlous state of Putin’s war machine: more defeats; more Generals sacked; more demoralised troops; more discontent amongst the Russian population; and more critique from Russia’s elites.

Mr Chair, Putin and the Russian military leadership have consistently underestimated the will, determination and courage of the Ukrainian military and civilians to defend their homeland from a brutal and barbaric invader. They continue to fail to understand that every horrendous attack strengthens the Ukrainian resolve and that of its friends, like the UK, who remain steadfast in our support – for however long it takes – to ensure that the sovereignty, territorial integrity, and the independence of Ukraine is fully restored.  Thank you.

---

# Civil news: Interim tender for

# Dartford HPCDS now open

News story

Tender opens 9 November 2022 to deliver services under the Dartford Housing Possession Court Duty Scheme (HPCDS) and closes 5pm 30 November 2022.

We are inviting tenders from 2018 Standard Civil Contract holders currently delivering housing and debt services to deliver services in the following HPCDS:

This opportunity is open to all 2018 Standard Civil Contract holders currently delivering housing and debt services.

When awarding the Dartford HPCDS contract preference will be given to organisations:

- with recent and relevant experience of delivering HPCDS services
- with an office in the corresponding housing and debt procurement area
- able to start delivering work on the contract start date

The Legal Aid Agency (LAA) is seeking to award one contract for Dartford HPCDS.

## Length of contracts

Contracts will be offered from 19 December 2022 until 29 April 2023.

## How do I tender?

Tenders must be submitted using the LAA's e-Tendering system.

## Tender deadline

The tender opens on 9 November2022 and closes at 5pm on 30 November 2022.

## Further information

Civil tender activity 2022 – to find out more and download the 'Information

For Applicants' document

e-Tendering system – to submit your tender

Published 9 November 2022

---

# How Cyber Essentials is helping to improve the cyber resilience of the UK

## Introduction

Good afternoon everyone, and thank you for joining us at this Cyber Essentials showcase event. I'm very excited to be here today, and it is great to see so many people here from a range of organisations including large and small businesses, government departments, trade bodies and charities. I would like to thank everyone for taking the time to attend and celebrate this fantastic event with all of us here at DCMS.

It has been great to hear about the Cyber Essentials journey from Chris [Pinder, IASME] and Lindy [Cameron, CEO, National Cyber Security Centre], and some of the noteworthy milestones of the scheme over the past 8 years. It is amazing to be able to say that the 100,000th certificate was awarded a few months ago, and I know that many of you here today are Cyber Essentials certified and are counted in that number.

The UK government is working to make the UK the safest place to live and work online. DCMS plays a critical role in strengthening the UK's cyber ecosystem and building a resilient and thriving digital UK, in line with our £2.6 billion National Cyber Strategy. As part of that strategy, we are committed to increasing the uptake of standards such as Cyber Essentials. To date, Cyber Essentials has had a profound impact in driving improved cyber security across a wide range of organisations. It is becoming increasingly embedded within our economy and it is playing a vital role in driving a more resilient and prosperous UK.

We regularly hear from organisations that are benefitting from the scheme – from large blue chip companies to small organisations and local charities, helping the most vulnerable in society – a small managed service provider in Northern Ireland, a nursing home in Liverpool, a domestic abuse charity in the Midlands and a charity supporting those with visual or hearing loss in Scotland – are just a few organisations that have gone through the Cyber Essentials scheme recently.

We have heard a lot about growth today, not just of the Cyber Essentials scheme itself but of the entire ecosystem that surrounds it. It is also

helping improve all organisations' productivity and growth as they securely embrace digital technologies. The government's vision is for this growth to continue, especially in the face of economic adversity. We want to raise awareness of the scheme, to see an exponential increase in the number of Cyber Essentials certifications and to raise the baseline of cyber resilience across the economy. We want all organisations in the UK to be working towards Cyber Essentials. To do this, we need organisations to be asking their suppliers, partners and other third parties they engage with to have it. Most suppliers to government need to have Cyber Essentials and we believe that organisations across the wider economy should be asking their own suppliers to do likewise and that is our ask of you today – to promote and use Cyber Essentials as a key tool when assessing the security of your suppliers.

## Supply chains

I know a lot of you are grappling with cyber security challenges in your supply chains. Worrying incidents have shown us that exploiting supply chain vulnerabilities can have severe, far reaching consequences. In the supply chain call for views we published last year, 46% of organisations said a lack of tools is a severe barrier to managing their supplier risk.

I believe Cyber Essentials has an important role to play here. It is not a silver bullet and does not guarantee organisations won't fall victim to a cyber attack, but it does provide protection and resilience for so many. In our engagements with industry, including many of you, we are seeing an increasing number of organisations use Cyber Essentials as a tool to assure themselves that third parties, including suppliers, have implemented minimum cyber security controls.

For example, the NHS recently introduced a requirement for IT suppliers to have Cyber Essentials, thus raising the bar for those organisations that wish to do business with the NHS. Other organisations have seen reduced costs and increased efficiency in their due diligence processes by requiring suppliers to have Cyber Essentials. A well known property website recently told us that asking for Cyber Essentials from suppliers has reduced their due diligence process from days to hours. For them, Cyber Essentials has a commercial benefit and is saving them money.

In a similar vein, we are delighted to announce that DCMS is now working in partnership with St James's Place, a large financial services firm, who have recently required all of their partners to become Cyber Essentials Plus certified. We will hear more from them in our panel discussion in just a few minutes, but this is a great example of an organisation proactively driving improved security practices in those organisations they work so closely with.

## Cyber Essentials Pathways

Now, it would be remiss of me to not recognise the fact that for some organisations, especially those with large and complex IT infrastructures, it is a struggle to comply with all aspects of Cyber Essentials. As Lindy

mentioned, we are looking forward to seeing the results of the Cyber Essentials Pathways pilot and anticipate this will provide a further opportunity for organisations to attain Cyber Essentials. We want to ensure that being Cyber Essentials certified is accessible for all organisations. To this end, we are also in the process of launching an evaluation of the scheme, to help us identify and address any barriers that organisations face when going through the Cyber Essentials process.

## Conclusion

On that note, I wanted to close by saying that my officials and I would love to hear from you, to better understand how DCMS and industry can work together to ensure Cyber Essentials is an effective certification scheme. I invite you to collaborate with us, to join us on the journey to improve Cyber Essentials and ensure it continues to raise the baseline level of cyber security across our supply chains.

The new government remains intent on improving cyber security across our economy. Our Product Security and Telecoms Infrastructure Bill is close to completing its passage through Parliament and when it becomes law, this will ensure much better security in consumer IoT products. We are also working to improve our cyber resilience legislation and expand the number of skilled people working in cyber security. We're continuing to build our digital identity framework, which will help the public and businesses verify identities in an easy, secure and trustworthy manner.

Together we can reduce the social and economic harm that we continue to see from cyber security attacks and drive a more resilient and prosperous UK. Thank you once again for working with us on this amazing scheme.

---

# Change to maximum Plan 2 and Postgraduate student loan interest rates

From 1 September 2022 to 30 November 2022, the maximum Plan 2 and the Postgraduate loan (PGL) interest rate was set at 6.3% for all Plan 2 and PGL borrowers, in line with the prevailing market rates available at the time of setting the cap.

Following this, the Government has confirmed that the maximum Plan 2 and the Postgraduate loan interest rate will be 6.5% between 1 December 2022 and 28 February 2023, to take into account an increase in the prevailing market rates.

From 1 March 2023 to 31 August 2023 the maximum Plan 2 and the Postgraduate loan interest rate will be capped at the forecast prevailing market rate for the 2022/23 academic year. This is 7.3%, in line with the Government announcement dated 13 June 2022. Should the actual prevailing market rate turn out to be lower than forecast, a further cap would be implemented to reduce student loan interest rates accordingly.

- The prevailing market rate is not defined in law, nor does any product on the market offer a direct “market rate” comparison to student loans. The most appropriate market rate comparators for student loans are the effective interest rates available on unsecured personal loans, with the Bank of England’s effective interest rate data (series CFMZ6LI (existing loans) and CFMZ6K9 (new loans)), being the most appropriate benchmark for student loan interest rates. To determine the “prevailing” market rate, a 12-month rolling average is taken. As such, the prevailing market rate has been defined as **the minimum of the 12-month rolling averages of the Bank of England’s effective interest rate data series’ CFMZ6LI and CFMZ6K9.**
- Where the Government considers that the student loan interest rate is too high in comparison to the prevailing market rate, it will reduce the maximum Plan 2 and Postgraduate Loan interest rate by applying a cap for a set period of three months (or longer, if the prevailing market rate remains below the student loan rate at the next monitoring point). This is done by amending Education (Student Loan) (Repayment) Regulations 2009. The prevailing market rate used for setting a cap in a given quarter is based on the latest CFMZ6LI and CFMZ6K9 data available, which is the data going up to 2 months prior to the start of the quarter, e.g. the cap set for between September and November 2022 was based on the end-July 2021 to end-June 2022 data.
- Plan 2 borrowers will continue to repay 9% of their earnings over the repayment threshold. The repayment threshold for Plan 2 ICR loans is £27,295 for FY22-23.
- Plan 2 ICR loans are those loans taken out for a course starting after 1 September 2012 (England and Wales).
- Postgraduate loan borrowers will continue to repay 6% of their earnings over the repayment threshold. The repayment threshold for Postgraduate loans is £21,000 for FY22-23.
- Postgraduate loans are those loans taken out for Postgraduate level study.
- Plan 1 ICR loans, those loans taken out for a course starting before 1 September 2012 are not affected.

Published 9 November 2022
Last updated 17 November 2022 + show all updates

1. 17 November 2022

   Added updated announcement from the Department of Education (DfE). Interest rates for date ranges 1 September 2022 to 30 November 2022 added.

2. 9 November 2022

   First published.