# 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.