Public Document Pack

Digital Services Committee

Date: **THURSDAY, 10 JULY 2025**

Time: **11.00 am**

Venue: **COMMITTEE ROOMS - WEST WING, GUILDHALL**

Members:
James Tumbridge (Chairman)
Deputy Dawn Wright (Deputy Chair)
Simon Burrows
Deputy Timothy Butcher
Lesley Cole
Susan Farrington (Ex-Officio Member)
Deputy Caroline Haines (Ex-Officio Member)
Philip Kelvin
Alderman Sir William Russell (Ex-Officio Member)
Deputy James Thomson CBE (Ex-Officio Member)

Enquiries: **Rhys Campbell**
Rhys.Campbell@cityoflondon.gov.uk

Accessing the virtual public meeting
Members of the public can observe all virtual public meetings of the City of London Corporation by following the below link:
https://www.youtube.com/@CityofLondonCorporation/streams

A recording of the public meeting will be available via the above link following the end of the public meeting for up to one civic year. Please note: Online meeting recordings do not constitute the formal minutes of the meeting; minutes are written and are available on the City of London Corporation's website. Recordings may be edited, at the discretion of the proper officer, to remove any inappropriate material.

Whilst we endeavour to livestream all of our public meetings, this is not always possible due to technical difficulties. In these instances, if possible, a recording will be uploaded following the end of the meeting.

Ian Thomas CBE
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**

3. **MINUTES**

To agree the public minutes and non-public summary of the previous meeting held on 15 May 2025 as a correct record.

For Decision
(Pages 5 - 12)

4. **DIGITAL INFORMATION TECHNOLOGY SERVICE (DITS) - SERVICE DELIVERY SUMMARY**

Report of The Chamberlain.

For Information
(Pages 13 - 18)

5. **QUARTERLY PROGRAMME SAPPHIRE (ERP) UPDATE REPORT - Q2 2025**

Report of The Chamberlain and The City Surveyor.

For Information
(Pages 19 - 26)

6. **OLA AGREEMENT UPDATE**

Report of the City of London Police.

For Information
(Verbal Report)

7. **IMPACT OF THE NEW CYBER SECURITY AND RESILIENCE POLICY STATEMENT**

Report of The Chamberlain.

For Information
(Pages 27 - 64)

8. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

9. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

10. **EXCLUSION OF THE PUBLIC**

MOTION - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

For Decision

Part 2 - Non-Public Items

11. **NON-PUBLIC MINUTES**

To agree the non-public minutes of the previous meeting held on 15 May 2025 as a correct record.

For Decision
(Pages 65 - 68)

12. **FUTURE NETWORK PROGRAMME**

Report of The Chamberlain.

For Decision
(Pages 69 - 116)

13. **QUARTERLY PROGRAMME SAPPHIRE (ERP) UPDATE- NON-PUBLIC REPORT - Q2 2025**

Report of The Chamberlain.

For Decision
(Pages 117 - 120)

14. **PHISHING SIMULATION RESULTS - APRIL**

Report of the Director of Digital Information and Technology.

For Information
(Pages 121 - 132)

15. **MANAGED PRINT SERVICES, PROCUREMENT STAGE 2 AWARD REPORT**

Report of The Chamberlain.

For Information
(Pages 133 - 140)

16. **CYBER SECURITY**

Report of The Chief Information Security Officer.

For Information
(Pages 141 - 190)

17. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

18. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

DIGITAL SERVICES COMMITTEE

Thursday, 15 May 2025

Minutes of the meeting of the Digital Services Committee held at Guildhall, EC2 on Thursday, 15 May 2025 at 1.45 pm

Present

Members:
James Tumbridge (Chairman)
Deputy Dawn Wright (Deputy Chair)
Simon Burrows
Deputy Timothy Butcher

Observing Virtually:
Deputy Caroline Haines
Susan Farrington

Officers:

Caroline Al-Beyerty	-	The Chamberlain
Sam Collins	-	Chamberlain's Department
Zakki Ghauri	-	Chamberlain's Department
Simon Grey	-	Chamberlain's Department
Christopher Bell	-	City of London Police
Gary Brailsford-Hart	-	City of London Police
Matthew Cooper	-	Town Clerk's Department
Kate Doidge	-	Town Clerk's Department

1. **APOLOGIES**
Apologies were received from Alderman Sir William Russell and Deputy James Thomson.

Deputy Caroline Haines and Susan Farrington observed the meeting virtually.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
There were no declarations.

3. **COURT ORDER**
The Committee received the Order of the Court of Common Council dated 25th April 2025, appointing the Committee and setting its Terms of Reference.

4. **ELECTION OF A CHAIRMAN**
The Committee proceeded to elect a Chairman in accordance with Standing Order No. 28. The Town Clerk informed the Committee that James Tumbridge, being the only Member expressing their willingness to serve, was duly elected

Chairman of the Digital Services Committee for the ensuing year and took the Chair for the remainder of the meeting.

RESOLVED – That James Tumbridge be elected Chair of the Digital Services Committee for the ensuing year.

5. **ELECTION OF A DEPUTY CHAIRMAN**

The Committee proceeded to elect a Deputy Chairman in accordance with Standing Order No. 29. The Town Clerk informed the Committee that Dawn Wright, being the only Member expressing their willingness to serve, was duly elected Deputy Chair of the Digital Services Committee for the ensuing year.

RESOLVED – That Dawn Wright be elected Deputy Chair of the Digital Services Committee for the ensuing year.

James Tumbridge moved a Vote of Thanks to Deputy Dawn Wright, the past Chair of the Committee.

RESOLVED UNANIMOUSLY - That - at the conclusion of her three year term of office as their Chair, of the Digital Services Committee, the Committee wish to extend to:

Deputy Dawn Wright

their sincere thanks and appreciation for the manner in which she has presided over their deliberations and the detailed care and interest she has shown in all aspects of the work of the Digital Services Committee.

DAWN'S UNWAVERING COMMITMENT began with the then-Digital Services Sub (Finance) Committee, serving as a Member of the Sub Committee. Following the transformation of the Sub Committee into a Grand Committee, Dawn was elected as its first-ever Chair in 2022 and has since consistently provided excellent leadership and support to colleagues during an exciting and frequently challenging period of digital transformation.

AS CHAIR, Dawn has been instrumental in the development and approval of the City Corporation's first-ever Digital, Data and Technology Strategy. This comprehensive strategy encompasses the entire City of London Corporation, including the City of London Police, Barbican Centre, GSMD and City Schools and Freemen's School. It has set a solid foundation for the City of London Corporation's digital transformation journey, moving toward a data-driven organisation and hopes to drive greater automation and responsible use of AI.

UNDER DAWN'S CHAIRSHIP, the successful insourcing of the IT Managed Service has transitioned to a model where 90% of the service is managed in-house, a strategic move which not only results in an impressive £900k per annum saving but has also improved the quality, flexibility and delivery of the Digital, Information, and Technology Service, allowing the organisation to shape the service offering and allow for greater collaboration.

WITH DAWN'S SUPPORT, the first-ever AI Policy was approved, in conjunction with the rollout of Copilot for Microsoft 365 to over 300 staff members across the City of London Corporation. This initiative has resulted in the organisation taking over 4,000 Copilot actions and benefitting from 250 Copilot-assisted hours every week.

DAWN HAS PLAYED A PIVOTAL ROLE in the approval of the Future Network Strategy and the initiation of the Future Network Programme, which aims to transform the IT Network by moving to a WiFi-first, cloud-based solitons, providing seamless access to resources from anywhere, providing greater resilience for the organisation. Further, Dawn's support has also mitigated a significant corporate risk posed by the decommission of the Public Switched Telephony Network by 2027 and ensuring that the Corporation is well-prepared for this transition.

DAWN WAS INSTRUMENTAL in the installation of the Technology Support Desk at Guildhall, and requested a similar desk be installed and set up for the City of London Police's New Street office – a highly visible support desk looking after the technology needs of Police colleagues, which was very well received.

UNDER DAWN'S CHAIRSHIP, the City of London Corporation has appointed an award-winning Director of Digital, Information, and Technology, bringing in expertise and innovation and further strengthening the City of London Corporation's digital capabilities. Dawn has also been fully supportive of the promotion of 'Women in Tech', an initiative which brings together women to discuss how to attract more representation from women in senior technology roles.

FINALLY, THE COMMITTEE WISHES TO PLACE ON RECORD its recognition and sincere thanks to Dawn for her great passion and commitment as Chair of the Digital Services Committee, which has been greatly appreciated by the Members and staff alike, recalling her substantial body of achievements over the past three years, and convey to her their very best wishes for the future.

6. **MINUTES**

RESOLVED: - That the public minutes and non-public summary of the meeting held on 30th January 2025 be approved as an accurate record.

7. **APPOINTMENTS TO OTHER COMMITTEES**

The Committee received a report of the Town Clerk relative to the Committee's appointments to other Committees.

The Committee considered the appointment of one Member to the Projects and Procurement Sub-Committee. The Town Clerk informed the Committee that no expressions of interest were received ahead of the meeting and invited any expressions of interest to the position. Simon Burrows, being the only Member willing to serve was duly appointed to serve on the Sub-Committee for the ensuing year.

RESOLVED – That Simon Burrows be appointed to the Projects and Procurement Sub-Committee.

8. **DRAFT CHAMBERLAIN'S BUSINESS PLAN FOR 2025/26**

The Committee received a report of the Chamberlain, for the approval of the Business Plan for the Chamberlain's Department for 2025/26.

RESOLVED: - That the Digital Services Committee:

- Note the factors taken into consideration in compiling the Chamberlain's Department Business Plan; and
- Approve the parts of the Chamberlain's Business Plan for 2025/26 referring to the Digital, Information and Technology Service subject to the incorporation of any changes sought by the Committee (all other parts are to be approved by the Finance Committee).

9. **DIGITAL, INFORMATION AND TECHNOLOGY SERVICE (DITS) - SERVICE DELIVERY SUMMARY**

The Committee received a report of the Chamberlain, concerning the service delivery summary for the Digital, Information and Technology Service.

RESOLVED: - That the report be received, and its contents noted.

10. **DIGITAL, INFORMATION, AND TECHNOLOGY SERVICE (DITS) - BUSINESS PLAN END OF YEAR UPDATE**

The Committee received a report of the Chamberlain, concerning an end of year update on progress against the 2024/25 Business Plan for the Digital, Information and Technology Service.

A Member queried the procurement of the Managed Print Solution. The Committee heard that the initial procurement exercise was for a single tender, but following concerns raised on the solution being fit for purpose, a new procurement exercise with the Print Room and Managed Print Service being split into two lots.

RESOLVED: - That the report be received, and its contents noted.

11. **QUARTERLY PROGRAMME SAPPHIRE (ERP) UPDATE REPORT - Q4 2024/25**

The Committee received a report of the Chamberlain, concerning the quarterly update on Programme Sapphire (ERP).

A Member raised a query relating to Wave 2 (HR & Payroll), which was received in non-public session.

Questions were raised on lessons learned in the post-implementation review, following the go live of the Learning Management System. The response was that officers had identified that communications on the changes to staff needed to be sharper, which would be incorporated into upcoming milestones. On the Learning Management System, initial data demonstrated the number of

escalated queries had been fewer as it was now a self-serve system, which could indicate an improved user experience. The next steps were to identify the level of user expectations, and measure this against feedback on user experience to track progress to report back to Members.

The Chairman requested that the Chamberlain share their thoughts on how the Committee and the Finance Committee work together to ensure the delivery of Programme Sapphire. The Chamberlain responded that the governance of the Programme needed to balance swift decision making and informing the interested stakeholders. There was a working party for the Programme, which discussed issues and challenges, which Members were encouraged to join. There was also a close working relationship between the Chamberlain and the Chairman and Deputy Chairman of Finance Committee to manage and run the delivery of the Programme concurrently with the Digital Services Committee.

The Chairman requested that future updates on Programme Sapphire track lessons learned and capture position impacts to understand the value of the new system.

RESOLVED: – That the report be received, and its contents noted.

12. **CO-PILOT PROOF OF VALUE REPORT**

The Committee received a report of the Chamberlain, concerning a report that summarised the findings of a recent discovery exercise completed by Pheonix Software Limited into the use of Copilot for M365 across several City of London Corporation departments.

Members queried the purpose of the report and whether it demonstrated value for money for the Copilot license, such as departmental cost savings. Officers responded that it had taken a departmental funded approach for Copilot licenses, and thus each department funded its own Copilot license. These departments may have been careful in its selection of roles that would benefit from the use of AI. The report itself sought the possibility and value for the wider organisation in the future.

Members requested more quantitative data on the benefit for Copilot, especially in future reports, as this would be useful for Members understand how success was being measured. The Committee heard that data was available which broke down use of Copilot, such as Copilot assisted hours, but again the report concerned itself was a more qualitative-based assessment and discussed the difference it has made to various roles across the City Corporation.

Following a concern raised, it was confirmed that Power BI formed part of the license with Microsoft and thus was not an additional cost.

Lastly, the Committee heard that, in relation to Copilot being used for FOIs and document discovery, officers in the Comptroller & City Solicitor's Department were trialling using Copilot, the outcomes of which were yet to be understood.

RESOLVED: – That the report be received, and its contents noted.

13. **REPORT OF ACTION TAKEN**
The Committee received a report of the Town Clerk, concerning details of decisions taken under urgency between Committee meetings.

The Chairman queried the Comptroller and City Solicitor's reasoning for the insertion of the word 'appropriate' into the Committee's Terms of Reference. It was agreed that this would be followed up with the Chairman outside of the meeting.

RESOLVED: - That the report be received, and its contents noted.

14. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no public questions.

15. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
There were no public items of urgent business.

16. **EXCLUSION OF THE PUBLIC**

RESOLVED: - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of the Schedule 12A of the Local Government Act.

17. **NON-PUBLIC MINUTES**
RESOLVED: - That the non-public minutes of the previous meeting held on 30th January 2025 be approved as an accurate record.

18. **QUARTERLY PROGRAMME SAPPHIRE (ERP) UPDATE REPORT - Q4 2024/25**
The Committee received a report of the Chamberlain, concerning the quarterly update on Programme Sapphire (ERP), in non-public session.

19. **DIGITAL, INFORMATION AND TECHNOLOGY SERVICE (DITS) - RISK UPDATE**
The Committee received a report of the Chamberlain, concerning an update on the risks faced by the Digital, Information and Technology Service (DITS).

20. **CYBER SECURITY UPDATE**
The Committee received a report of the Chief Information Security Officer, concerning an update on cyber security.

21. **PHEONIX SOC SERVICE**
The Committee received a report of the Chamberlain, concerning the Pheonix SOC Service.

22. **CITY OF LONDON POLICE ORGANISATIONAL LEVEL AGREEMENT**

The Committee heard a verbal report concerning an update on the City of London Police (COLP) Organisational Level Agreement (OLA).

23. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no non-public questions.

24. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There were two items of other non-public business.

The meeting ended at 3.10 pm

Chairman

Contact Officer: Kate.Doidge
Kate.Doidge@cityoflondon.gov.uk

This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Digital Services Committee	**Dated:** 10/07//2025
Subject: Digital Information Technology Service (DITS) –Service Delivery Summary	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes**	**Providing Excellent Services**
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	N/A
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	The Chamberlain
Report author:	Dawn Polain – Head of Service Delivery (CoL/CoLP)

Summary

This is an overview of the current service provision as managed by DITS. Performance is measured monthly therefore for the purposes of this report, the most recent reporting month is May 2025.

The services managed by DITS for the City of London (CoL) and City of London Police (CoLP) have been stable.

Recommendation(s)

No recommendations to advise during this reporting period.

Main Report

Background

1. General performance across all CoL/CoLP Incident Response and Resolution KPIs remains consistent with previous months.
   .
   May performance figures for CoL and CoLP were:

   CoL: Incident Response 94% Met, Incident Resolve 95% Met
   CoLP: Incident Response 84% Met, Incident Resolve 93% Met

Current Position

2 There were no P1 Incidents reported for CoL/CoLP during this reporting period which were within the responsibility of DITS Resolver groups.

Key service provider status:

4. Barracuda experienced 1 x P1 incident which affected CoLP
   77370 – User reports that cameras were down in the Control Room
   Resolution – Barracuda restarted the VPN tunnel

5. No other Priority 1 incidents recorded by Service Providers for this reporting period.

Service improvements and highlights

6. 90% of CoL/CoLP Users scored DITS with a Customer Satisfaction score of >8 in May.

7. Service Management continue to support CoLP SCP CCTV to enable a stable service. Work is continuing to review and refine the current Support Model to better support the SCP operational service.

8. Service Management have supported the evaluation and moderation of bids submitted for the Future Network Programme (FNP).

9. KPI performance across all Priorities continues to be monitored by the Service Management team, and areas for improvement have been highlighted to Resolver Groups.

Service Metrics

10. The COL and COLP P4 Resolution KPI continues to be achieved across CoL and CoLP, with a performance KPI of 96% and 95% respectively.

11. Resolver Teams have been requested to focus on the P3 Incident performance as improvement is required in this area.
    The DITS Service Management team chair twice weekly KPI review sessions with all Resolvers, and particular attention will be levied against the P3 target until an improvement can be reported.

Options

12. None to advise this reporting period.

Proposals

13. None to advise this reporting period.

Key Data

14. As detailed in Appendix 1

Corporate & Strategic Implications - None

Conclusion

15. The DITS Service Management team continue to support Resolver Teams in order to improve KPI performance figures.

    The team is also continuing to evaluate the effectiveness of our ITIL processes, and it is expected that a revised Release Management and Continual Service Improvement process will soon be introduced to complement our existing ITIL functions.

Appendices

- Appendix 1 – CoL and CoLP Performance Stats

Dawn Polain
DITS Head of Service Delivery

T: 07895 330693
E: dawn.polain@cityoflondon.gov.uk

Appendix 1 – Current Performance against Service Metrics COL/LC In House Incident Performance

Executive Performance Metrics | COL/LC In House

CoL/LC	KPI Metrics	December 2024			January 2025			February 2025			March 2025			April 2025			May 2025		
		Total	KPI%		Total	KPI%		Total	KPI%		Total	KPI%		Total	KPI%		Total	KPI%	
Service Performance Measure (In House)	Total Incidents (Logged)	353	-		509	-		473	-		522	-		555	-		470	-	
	Total Incidents (Closed)	419	-		441	-		464	-		510	-		548	-		516	-	
	98% of all P1 Incidents responded < 15 minutes	1	0%	↓	0	-	↑	0	-	→	0	-	→	0	-	→	0	-	→
	98% of all P2 incidents responded to < 15 minutes	1	100%	↑	0	-	→	3	0%	↓	0	-	↑	0	-	→	1	0%	↓
	95% of all P3 incidents responded to < 2 hours	26	88%	↑	37	84%	↓	28	79%	↓	26	81%	↑	18	50%	↓	8	62%	↑
	95% of all P4 incidents responded to < 8 hours	391	92%	→	404	95%	↑	433	92%	↓	483	93%	↑	530	96%	↑	478	95%	↓
	98% of all P1 Incidents resolved < 2 hours.	1	100%	↑	0	-	→	0	-	→	0	-	→	0	-	→	0	-	→
	98% of all P2 Incidents resolved < 4 hours	1	100%	→	0	-	→	3	0%	↓	0	-	↑	0	-	→	1	100%	↑
	90% of all P3 incidents resolved < 8 hours	26	88%	↑	37	92%	↑	28	79%	↓	26	81%	↑	18	78%	↓	6	46%	↓
	90% of all P4 incidents resolved < 5 business days	391	99%	↑	404	96%	↓	433	98%	↑	483	97%	↓	430	97%	→	482	96%	↓

Data does not include COL Service Desk, LC Service Desk, COL Revenues, COL Horizon Support, COL CSD Performance & Services Te am, COL Mosaic Support, 3rd parties, CoL Housing Team

Executive Performance Metrics | COLP In House

COLP	KPI Metrics	December 2024			January 2025			February 2025			March 2025			April 2025			May 2025		
		Total	KPI %		Total	KPI %		Total	KPI %		Total	KPI %		Total	KPI %		Total	KPI %	
Service Performance Measure (In House)	Total Incidents (Logged)	554	-	-	634	-	-	624	-	-	627	-	-	632	-	-	534	-	-
	Total Incidents (Closed)	592	-	-	633	-	-	527	-	-	684	-	-	653	-	-	564	-	-
	98% of all P1 Incidents responded < 15 minutes	2	0%	↓	0	-	↑	0	-	→	1	0%	↓	0	-	↑	0	-	→
	98% of all P2 incidents responded to < 15 minutes	1	100%	→	1	0%	↓	2	100%	↑	2	100%	→	1	0%	↓	3	0%	→
	95% of all P3 incidents responded to < 2 hours	28	61%	↑	51	63%	↑	30	43%	↓	47	70%	↑	39	56%	↓	34	44%	↓
	95% of all P4 incidents responded to < 8 hours	561	91%	↓	581	92%	↑	495	88%	↓	634	88%	→	613	89%	↑	527	87%	↓
	98% of all P1 Incidents resolved < 2 hours.	2	50%	↓	0	-	↑	0	-	→	1	0%	↓	0	-	↑	0	-	→
	98% of all P2 Incidents resolved < 4 hours	1	100%	→	1	0%	↓	2	100%	↑	2	100%	→	1	100%	→	3	67%	↓
	90% of all P3 incidents resolved < 8 hours	28	75%	↑	51	78%	↑	30	77%	↓	47	66%	↓	39	64%	↓	34	59%	↓
	90% of all P4 incidents resolved < 5 business days	561	98%	→	581	98%	→	495	98%	→	634	95%	↓	613	95%	→	527	95%	→

This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Finance Committee – For Information Digital Services Committee – For Information	**Dated:** 01/07/2025 10/07/2025
Subject: Quarterly Programme Sapphire (ERP) Update Report – Q2 2025	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes** • **provides statutory duties** • **provides business enabling functions**	Providing Excellent Services
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	N/A
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Caroline Al-Beyerty, Chamberlain
Report author:	Simon Gray, Chamberlain's Department

Summary

1. The Programme has delivered Wave 1 deliverables
   - Learning Management (LMS) April
   - Performance Management and Goal Management (PMGM) – May
   - Recruitment – June

2. The principle of "Adopt not Adapt" is being maintained and there have been minimal changes proposed

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. The Programme Sapphire - Enterprise Resource Planning (ERP) Programme is the project for the City of London Corporation to replace its current legacy systems; City People (Midland i-Trent) for HR & Payroll and Oracle R12 for both strategic and operational finance.

2. The new ERP Solution will modernise the technology we rely upon to deliver back-office services.

3. A vital component of the new ERP Solution is that it will support the City of London Corporation's culture change. It will promote and enable self-service for all employees to access their information, provide access to real-time information and enable informed business decisions.

4. The change workstream will be key to driving the success of the programme over and above the technology, this is driven by the 'adopt not adapt' principle.

5. The Programme is delivering in 3 waves (see Appendix 3 for further details):

Wave 1	Leaning Management System (April 2025) Performance & Goals (May 2025) Recruitment (June 2025)	Q1 2025
Wave 2	Core HR & Payroll	Q3 2025
Wave 3	Finance & Budget Management / Forecasting	Q1 2026

Wave 1

6. Learning Management Solution

- The LMS solution was delivered in April 2025. The data as of 11th June 2025 is shown in Appendix 1, highlights include 649 employees accessing the solution and 656 hours of training content consumed.
- The reporting function has been a key benefit – providing the ability to track completion of mandatory training such as Cyber Ninja for corporate compliance.
- The Learning team are now looking to expand the course offerings within the solution, which will provide considerable advantage for people in their learning and development plans.

7. Performance Management and Goal Management (PMGM)

- PMGM went live in May 2026 – the initial focus is on entering Goals for the 2025/26. Reviews for 24/25 were completed in the previous solution.
- As at 11th June 2025 – 730 goals had been created by 100 users. The deadline for people to enter their goals for the civic year is 15 July 2025.

8. Recruitment Go-Live

- The recruitment module was the final element to go live in June 2025 and at the time of the report there was less than 1 week of operational data to support the new solution. These will be provided at the next quarterly update but will be available verbally in the meeting.

Wave 2 Update

9. Progress is Green. The plan is on track, there are risks to delivery being tracked with mitigating work in progress to maintain Green status. The design for SuccessFactors (the Core HR & Payroll solution which is part of SAP ERP Product) is complete with the following exceptions:

Module	Progress Update
Occupational Health (December 2025)	• Workshops are planned in line with the project plan.
HR Service Desk (December 2025)	• SAP have sunset their existing product and the Corporation will need to evaluate the alternative product to ensure compliance with requirements. • Confirmation is being escalated to the System Integrator (HCL) and the software vendor (SAP) to confirm the delivery for December 2025 • This is a critical items for the planned launch in December 2025 and is being tracked as a key risk for that reason.
Employee Health & Safety (April 2026)	• The workshops are underway. There has been a challenge with the compliance / alignment to UK Health and Safety legislation which being worked through with the SAP Product owner. • This is a Wave 3 deliverable (April 2026) • At this time the decision has been made to hold the delivery of this module until business assurance is in place that the requirements will be met – a decision is expected in July on this module with the business owner
Payroll (December 2025)	• The plan is being evaluation to ensure that December 2025 is achievable with contingency plans in the event of delays during the parallel run process and alignment with the Ambition 2025 programme

10. The Corporation leads are now focused on data collection/ cleansing in preparation for the first data migration wave which is due to commence on the 20th June 2025.

11. The level of change management / stakeholder management needs to increase significantly with a focus on driving the transformation from the service delivery teams (HR / DITS).

Wave 3 Update

12. Progress against the overall plan is currently logged as Amber with the following status updates:
    - Resource gaps from the system integration partner (HCL) were escalated by the Board / SRO and have now been resolved and the delays logged.
    - Key decisions on the enterprise structure have been made that have supported strong progress and unlocked the remaining design decisions to support the April 2026 go-live. These principles will be demonstrated in playback sessions planned for Jun- Aug.
    - The workstream is currently being re-planned and the expectation is still to deliver for 1st April 2026 once the replan is complete. The focus is on mapping the dependent activities between the system integrator and Corporation resource to complete the plan
    - The level of change management / stakeholder management needs to increase significantly with a focus on driving the transformation from the service delivery teams (Finance / DITS). The change management resource to focus on Finance is now in place to drive this

Change Management

13. The change team is now fully resourced with a specific lead in place for the Change Champions network and Finance Workstream
14. The Training Needs Analysis (TNA) was completed and details are included in Appendix 2. Further work is required to agree the training strategy / approach
15. Mini-Roadshows were delivered

Digital Services Update

16. The data migration activities are progressing with support for Wave 1 complete and the focus now on preparing for Wave 2 testing cycles
17. Changes from the build cycle are being managed against the data migration needs

Budget Update

18. The overall budget forecast is unchanged at £19.4m
19. The costed risk provision is £8.6m – a recommendation was made in the June Board which is detailed in the non-public section for £21k.

Look ahead

20. The build for Wave 2 (HR and Payroll) will be completed and commencement of System Integration Testing. 2 playback waves have been delivered at the time of the report and are progressing well to evidence the build.

Corporate & Strategic Implications

Strategic implications - The ERP Programme supports the Corporate Initiatives to deliver brilliant basics and mitigates the risk of unsupported legacy systems.

Financial implications – Digital Services Committee, Finance Committee and Court of Common Council have approved the budget envelope to bring in the relevant resources including backfills.

Resource implications - The requirement of resourcing is detailed in this paper.

Legal implications - All staff resourcing, and employment contracts will comply with statutory requirements and be in line with best practice.

Risk implications - Failure to baseline the programme roles would place a risk on the organisation.

Equalities implications - An Equalities Impact Assessment was done initially and is currently being updated and will be brought back for review. This will be routinely updated throughout the life of the programme.

Climate implications - None

Security implications - None (other than standard vetting requirements)

Conclusion

21. The programme is tracking to plan on deliverables and budget and no use of costed risk. The key principle of adopt not adapt is being adhered to with minimal change. Risk and issues will continue to be monitored / reported with the focus on robust planning for Wave 2 & 3. The levels of change management / stakeholder engagement need to ramp up to support the transformation journey over the next quarter and will be reported on at the next stage report.

Appendices

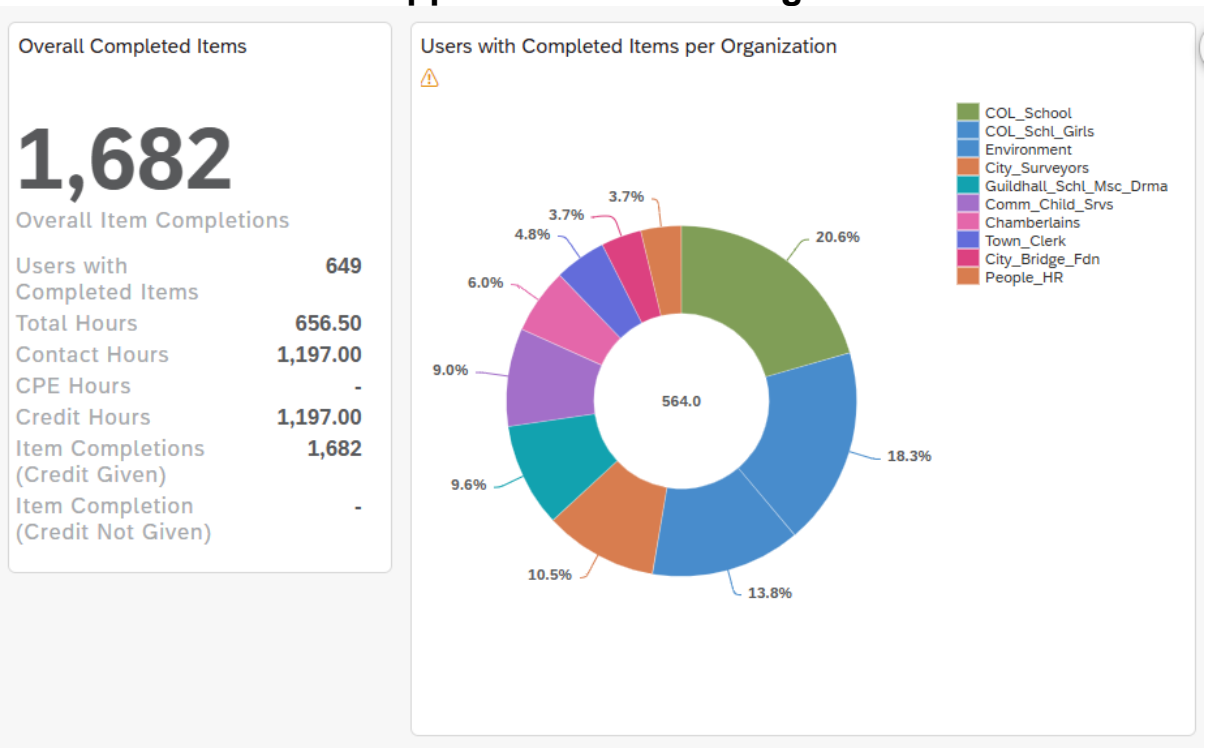
Appendix 1 – LMS Usage

Appendix 2 - Learning Journeys

Simon Gray
Programme Director, Chamberlain's Department

T: 07557 568016
E: simon.gray@cityoflondon.gov.uk

Appendix 1 – LMS Usage



Appendix 2

Learning Journeys – SuccessFactors

Audience	Course Name / Course Duration (Minutes) / Recommended Delivery Method											
HR (16 hours of training)	Overview for HR teams	Position Management	Manage New Hires / Onboarding	Maintain Personal Information	Maintain Employment Information	Absences	Manage Leavers	Management Information	Manage Timesheets	Succession and Career Development		
	60	120	90	60	180	180	60	60	90	60		
	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom		
Manager Self Service (2 hours of training)	MSS- Delegation	MSS- Occupational Health	MSS- My Team Personal Information	MSS- My Team Employment Information	MSS- My Team Absences	MSS- Leavers	MSS- Approvals/Rejections	MSS- Learning	MSS- Reporting	MSS- Timesheets	Perf.Mgmt. - Goal Mgmt. (Managers)	MSS- Succession and Career Development
	15	15	10	15	15	10	6	15	10	15	45	10
	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eClassroom	eLearning
Employees with PC Access (2 hours of training)	ESS- ECSC (AskHR)	ESS- Basics and Navigation	ESS- Personal Information	ESS- Employment Information	ESS- Absences	ESS- Learning	ESS- Timesheets	ESS- Perf.Mgmt. - Goal Mgmt.	ESS- Recruitment for Internal Candidates	ESS- Succession and Career Development		
	10	10	15	10	15	15	15	30	10	10		
	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning	eLearning		
Employees with NO PC Access (3 hours of training)	Manage your HR Information (Employee)	Learning	Timesheets (Employee)	Perf.Mgmt. - Goal Mgmt. (Employee)								
	60	45	45	45								
	Drop-in (Phys and Virtual)	Drop-in (Phys and Virtual)	Drop-in (Phys and Virtual)	Drop-in (Phys and Virtual)								

Learning Journeys – S/4HANA

Audience	Course Name / Course Duration (Hours) / Recommended Delivery Method					
Accounts Payables (17.5 hours of training)	SAP Overview & Navigation	AP: Business Partner Master Data	AP: Invoice Capture - Non-PO	AP: Invoice Capture - PO Invoice	AP: Payment Processing	AP: Reporting & Month End
	.5 hour	3 hours	4 hours	2.5 hours	4.5 hours	3 hours
	eLearning	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom
Accounts Receivables (15 hours of training)	SAP Overview & Navigation	AR Receipting	AR: Business Partner Master Data	AR: Invoicing and Down Payments	AR: Month End	AR: Reporting
	.5 hour	3.5 hours	2.5 hours	2 hours	4 hours	2.5 hours
	eLearning	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom	Physical / Virtual classroom
Purchasing	Purchase Requistionners	Capital Purchasing	PO Approvers	Goods Receiving Only	Purhasing & Invoice Enquiries	
	4 hours	6.5 hours	.5 hour	2 hours	2 hours	
	Physical / Virtual classroom	Physical / Virtual classroom	eLearning	Physical / Virtual classroom	Physical / Virtual classroom	

This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Digital Services Committee – For Information	**Dated:** 10/07/2025
Subject: Impact of the New Cyber Security and Resilience Policy Statement	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes** • **provides statutory duties**	**Providing Excellent Services**
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	N/A
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Chamberlains
Report author:	CJ Chapman

Summary

The purpose of this report is to inform about the recently published Cyber Security and Resilience Policy Statement Command Paper and to discuss its implications if any for the Corporation including the proposed actions needed to comply with the new policy.

This policy, presented to Parliament by the Secretary of State for Science, Innovation and Technology, outlines significant changes aimed at enhancing the UK's cyber security and resilience. Key points include the expansion of the regulatory scope to include Managed Service Providers (MSPs), strengthening supply chain security, empowering regulators, and ensuring the regulatory framework can adapt to emerging threats.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

The government first announced it would be bringing a Cyber Security and Resilience Bill before parliament in July 2024. Hostile actors were increasingly exploiting the UKs dependence on online infrastructure, conducting cyber attacks that cause maximum disruption and destruction. Perhaps most notably the June 2024 cyber attack on Synnovis – which impacted critical health services in the UK demonstrating how fundamentally reliant our health services are on online technology.

In April 2025. The Cyber Security and Resilience Policy Statement Command Paper was presented to Parliament by the Secretary of State for Science, Innovation and Technology. The policy aims to enhance the UK's cyber security and resilience by expanding the regulatory framework, empowering regulators, and ensuring adaptability to emerging threats.

As such the Cyber Security and Resilience Bill is designed to strengthen the UK's cyber defences by enhancing the resilience of Critical National Infrastructure (CNI), essential services, and crucially - digital service providers. The Bill builds upon the existing Network and Information Systems (NIS) Regulations 2018 and introduces new regulatory powers, reporting duties, and oversight mechanisms for entities deemed vital to national security and economic stability.

Current Position

As a local council we provide and support essential services to the City of London. Although we are not formally designated as Operators of Essential Services (OES) and therefore do not currently comply to the NIS Regulations which this Bill builds upon.

The Bill targets specific sectors such as energy, transport, health, digital infrastructure, and data centres. These sectors are considered essential to the functioning of the nation and are regulated accordingly. In addition, the expanded scope of the Bill brings into the fold Relevant Digital Service Providers (RDSPs), or Critical Suppliers. Local councils have not been designated under these categories and we are therefore not subject to the regulatory duties imposed by the Bill.

Options

Although we are not in scope for this bill there are some actions we can take forward.

1. **Remain Vigilant to Changing legislation**
2. **Certify with NCSC Cyber Assessment Framework**

Proposals

1. **Remain Vigilant to Changing legislation** - The Bill acknowledges the rapidly evolving cyber threat landscape and the need for the UK's regulatory framework to remain agile and responsive. As the landscape adapts so must we. As legislation changes, we will be first in line to adoption and compliance.
2. **Certify with NCSC Cyber Assessment Framework -** The Bill proposes to formalise the use of the NCSC's Cyber Assessment Framework (CAF) as a benchmark for cyber resilience. The CAF provides structured guidance for assessing and improving cyber security across critical sectors. At the City of London we have already begun our journey to certification and have passed our initial independent assessment.

Key Data

- The policy brings more entities, including MSPs, into the NIS regulatory framework.
- The policy gives the government greater flexibility to update the framework as and when needed, to respond in an agile way to changing threats, for instance by extending the framework to new sectors.

Conclusion

While the principles underpinning the Cyber Security and Resilience Bill—such as improved cyber resilience, incident reporting, and supply chain security—are relevant to all public sector bodies, the statutory provisions of the Bill do not currently extend to local government councils. Unless councils are explicitly designated in future secondary legislation, they remain outside the direct scope of the proposed regulatory framework.

By pursuing voluntary certification with frameworks such as the NCSC Cyber Assessment Framework, councils can benchmark their preparedness, identify vulnerabilities, and demonstrate a commitment to safeguarding vital services. Regularly reviewing internal processes, investing in staff training, and monitoring legislative changes will position the organisation to respond rapidly should regulatory obligations shift.

In conclusion, while local government remains outside the immediate remit of the Cyber Security and Resilience Bill, the fundamental message is clear: cyber security is a shared responsibility. By anticipating change, embracing best practices, and fostering a culture of continuous improvement, councils can play a pivotal role in protecting both their own operations and the wider communities they serve, ensuring ongoing trust and resilience in an increasingly digital world.

Appendices

- Appendix 1 - Cyber_Security_and_Resilience_Policy_Statement_Command_Paper

CJ Chapman
Information Security Manager
E: CJ.Chapman@cityoflondon.gov.uk

Department for
Science, Innovation
& Technology

Cyber Security and Resilience Policy Statement

CP 1299

Cyber Security and Resilience Policy Statement

Presented to Parliament by the Secretary of State for Science, Innovation and Technology by Command of His Majesty

April 2025

CP 1299

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at cybersecurityandresiliencebill@dsit.gov.uk.

ISBN 978-1-5286-5588-0

E03328649 04/25

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

CORRECTION SLIP

Title: Cyber Security and Resilience Bill Policy Statement

Session: 2024–2025

Number (if any): CP 1299

ISBN: 978-1-5286-5588-0

Date of laying: 1 April 2025

Correction:

In the 2024 Cyber Breaches Survey the figure given for the prevalence of cyber security breaches or attacks in businesses was 49.7% (rounded up to 50% in the main body of the Survey report). This correction removes text that suggested that more than 50% of businesses faced cyber security breaches or attacks.

Text currently reads:

The 2024 Cyber Breaches Survey also reveals the significant scale of the challenge we face, with more than half of businesses reporting some form of cyber security breach or attack in the past twelve months.

Text should read:

The 2024 Cyber Breaches Survey also reveals the significant scale of the challenge we face, with half of businesses reporting some form of cyber security breach or attack in the past twelve months.

Date of correction: 4 April 2025

CONTENTS

Ministerial foreword

The first duty of this Government is to keep its citizens safe. To anticipate the threats we face, minimise the risks we take, and make the UK as safe and secure as it can possibly be. That is what making National Security our number one priority means in practice.

The digital revolution is transforming our Critical National Infrastructure and our essential public services. It offers an extraordinary opportunity – to make our people and our country better off. However, it may also bring new and dangerous vulnerabilities.

In an increasingly dangerous and unstable world, we will not hesitate to protect our people from those who seek to do us harm. For too long, successive Governments have failed to properly address the growing risk posed by cyber criminals and hostile states. Last year's cyber-attack on a supplier to NHS hospitals in London caused more than 11,000 acute outpatient appointments and elective procedures to be postponed. Some of those people will have waited months to be seen.

I will not allow this to continue. We must take decisive action to deliver effective and enduring change. That is why, within weeks of entering Government, I announced plans for a Cyber Security and Resilience Bill. In this Policy Statement, I set out legislative proposals for this Bill. I also acknowledge that the cyber landscape moves exponentially – a lot can happen in a short space of time. This statement proposes several additional measures to tackle the threats that we are facing now.

Our legislative proposals reflect the insights we have gathered from our international partners, including valuable lessons from the European Union on the implementation of its NIS2 regime. They are also informed by consultations conducted by the previous Government in 2022 and 2023. However, it is vital that we also recognise the unique threats that the UK faces now and the threats that we cannot yet predict in the decades to come. At the same time, we must ensure that regulation works for businesses and investors, today and tomorrow.

At the core of our proposals is this Government's number one mission: economic growth. Growth is the only route to creating new jobs and putting more money in working people's pockets. But there is no growth without stability. By securing the digital infrastructure upon which a growing number of our businesses depend, we can deliver the stability they need to innovate and invest.

Every business I have spoken to has said the same thing: we need agile, pro-innovation regulation that is designed for the digital world we live in. Change has never been needed more.

Together, we can grow our economy, rebuild our public services, and deliver a more secure, resilient and prosperous digital future for Britain.

The Rt Hon Peter Kyle MP
Secretary of State for Science, Innovation and Technology

Strategic context

We are facing unprecedented threats to our critical national infrastructure, posing a risk to UK citizens.

Hostile cyber activity in the UK has grown more intense, frequent, and sophisticated, with real world impacts for UK citizens. Last year, a ransomware attack on the NHS led to over 11,000 postponed outpatient appointments and procedures. The 2024 Cyber Breaches Survey also reveals the significant scale of the challenge we face, with more than half of businesses reporting some form of cyber security breach or attack in the past twelve months.

The National Cyber Security Centre's (NCSC) Annual Review 2024 describes the threat landscape as 'diffuse and dangerous', with persistent attacks from hostile states and organised crime. This poses a threat to our national security. Chinese state sponsored threat actors have already targeted US critical sectors (e.g. Volt Typhoon) and Russia has launched destructive attacks against the Ukrainian Government. High profile attacks in the UK have affected local and central Government, such as the compromise of the Ministry of Defence's payment network, and attacks on essential providers, like Southern Water, and on the Leicester City Council and St Helens Borough Council, demonstrate a real risk to both our national and economic security and that of our allies.

Richard Horne, NCSC CEO, in a speech to launch the NCSC Annual Review, spoke about the severity of the risk facing the UK as being widely underestimated and the defence and resilience of Critical National Infrastructure, supply chains, the public sector, and our wider economy needing to improve urgently.

Resilience is not improving at the rate necessary to keep pace with the threat and this can have serious real-world impacts. The Government's legislative plan for cyber security will address the vulnerabilities in our cyber defences to minimise the impact of attacks and improve the resilience of our critical infrastructure, services and digital economy.

Cyber criminals are constantly adapting and improving their strategies.

Cyber criminals have continually exploited advances in technology to improve the effectiveness of their malicious activities. Our regulatory framework must keep pace and provide flexibility to respond to future threats as and when they emerge.

Adversaries are exploiting vulnerabilities in critical infrastructure and supply chains, using tools, such as artificial intelligence and commercial cyber capabilities, to enhance their espionage and disruptive activities.

Our growing dependency on technology has made supply chains particularly vulnerable, with ransomware and data extortion emerging as significant threats. Less than one tenth of operators of essential services feel confident in managing the risk from their wider supply chains (NIS 2018 Second Post Implementation Review). As these actors continue to evolve, the risk to supply chains remains a critical concern, necessitating heightened vigilance and robust cyber resilience measures.

Cyber security is a critical enabler of economic growth, fostering a stable environment for innovation and investment.

This Government is focused on kickstarting economic growth to improve the prosperity of our country and living standards of working people.

Secure and robust digital services create a stable and secure environment for businesses to thrive, attracting investment and encouraging the development of cutting-edge technologies. This stability not only enhances the competitiveness of individual companies but also drives overall economic progress by reducing downtime and operational disruptions.

Resilient cyber infrastructure is essential for encouraging innovation by providing a secure foundation upon which new ideas and technologies can be built, thereby maintaining the UK's position at the forefront of global technological advancements.

Our legislative plan for cyber will increase the uptake of essential cyber defences. This will protect more entities from cyber attacks and fostering an environment in which investment and innovation can thrive.

The case for change

In the July 2024 King's Speech, the Government announced it will introduce a Cyber Security and Resilience Bill to strengthen the UK's cyber defences and build the resilience of our essential services, infrastructure, and digital services.

This policy statement sets out more details for this Cyber Security and Resilience Bill's measures, as announced in the King's Speech.

The cyber landscape is consistently changing, with new evidence emerging daily. In recognition of this fact, this policy statement will also set out some additional measures that the Government is considering for an appropriate legislative vehicle, which could be this Cyber Security and Resilience Bill.

Current regulatory framework

The UK defines its most important digital and physical infrastructure assets, systems (including information and operational technology), sites, personnel, and functions through the lens of Critical National Infrastructure (CNI). Last year, the Government introduced the first new CNI sector in almost a decade when it designated data infrastructure, a first step in updating the UK's resilience. However, maintaining the security of essential and digital services, including CNI, in a continually shifting threat and hazard landscape, is an ongoing challenge for the Government as well as the public and private sector stakeholders responsible for managing and operating those services.

The Network and Information Systems (NIS) Regulations 2018 are the UK's only cross sector cyber security legislation. They play an essential role in safeguarding the cyber and physical resilience of much of the UK's CNI by placing security duties on the operators involved in the delivery of essential services.[1]

The 2018 Regulations cover five sectors (transport, energy, drinking water, health, and digital infrastructure) and some digital services (online marketplaces, online search engines, and cloud computing services). Twelve regulators (called 'competent authorities' in the regulations) are responsible for enforcing the regulations. Our regulations need updating to keep pace with the threats faced by regulated entities and we need to take action to bring the UK in line with our counterparts.

[1] Organisations that operate services that are deemed critical to the economy and wider society. They include critical national infrastructure (water, transport, energy) and other important services, such as healthcare and digital infrastructure.

A Cyber Security and Resilience Bill will address the specific cyber security challenges faced by the UK while aligning, where appropriate, with the approach taken in the EU NIS 2 directive. This strategic approach ensures we can be flexible and responsive to cyber threats in a proportionate way that balances the impact on business.

This Bill will make substantial improvements to this existing framework by bringing more entities into scope and putting regulators on a stronger footing so that they can carry out their important duties. The measures acknowledge the need for increased visibility over cyber threats, and the importance of simple and clear reporting requirements across different frameworks, including those under consultation by the Home Office to counter ransomware. The Bill will also allow the Government to act against emerging threats without the need for new primary legislation.

In recognition of the evolving threat landscape, this policy statement will outline several additional measures which will enable the Government to respond decisively to imminent threats to national security. The additional measures recognise the new status of data centres as CNI and the need for Government to set the strategic direction for the increasing variety of sectors in scope of the regulations. The Government will decide the appropriate legislative vehicle for the additional measures in due course.

Cyber Security and Resilience Bill measures, as announced in the King's Speech 2024

1. Bringing more entities into scope of the regulatory framework

In the King's Speech, we announced that we will use a Cyber Security and Resilience Bill to make crucial updates to the NIS Regulations 2018. We will do this by bringing more firms into scope, to better recognise the increasing reliance on digital services and the vulnerabilities posed by supply chains.

The evolving threat landscape and high-profile cyber attacks targeting essential services, as well as the growing dependency on cloud-based and other digital services, necessitates the inclusion of more entities within the regulatory framework.

Supply chains play a crucial role in the wider economy. The complexity of the digital landscape and the interconnectedness of supply chains means that vulnerabilities in one part can have cascading effects on our essential services. It is therefore imperative to recognise the importance of supply chains and develop appropriate measures to manage the risks they pose. Regulating this space will help ensure that all relevant entities adhere to robust cyber security practices, thereby safeguarding the economy and the services upon which society depends.

1.1 Bring Managed Service Providers into scope

1.1.1 Summary of intent

Managed service providers (MSPs) play a critical role in the UK economy by offering core IT services to businesses. These organisations have unprecedented access to clients' IT systems, networks, infrastructure, and data. This makes them an attractive target for malicious actors and subject to cyber attacks, including those that resulted in impacts on clients. This has included the Cloud Hopper attack on MSPs and the attack on the Ministry of Defence's personnel system. These highlight the vulnerabilities of MSPs and by extension, the critical services they support.

This measure will expand the remit of current regulations by bringing entities who provide managed services into the scope of the regulations. Placing duties on MSPs will enable us to protect a broader range of services from cyber attacks and build a better picture of the threats facing our essential services.

1.2.2 How the measure would work in practice

The Bill will define the managed services that will be brought into scope of legislation. The characteristics below reflect the services intended to be included. Exact wording will be subject to final drafting.

A managed service is a service which:

1. is provided to another organisation (i.e., not in-house), and;
2. relies on the use of network and information systems to deliver the service, and;
3. relates to ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, applications, and/or IT networks, including for the purpose of activities relating to cyber security, and;
4. involves a network connection and/or access to the customer's network and information systems.

These firms[2] will be subject to the same duties as those placed on firms that provide digital services, referred to as 'relevant digital service providers' under the 2018 Regulations.[3] The Information Commissioner's Office (ICO) will act as the regulator and have authority to regulate MSPs through information gathering, investigation and enforcement powers.

1.1.3 Impact

Expanding the scope of the regulations to include managed services will enhance the security of IT infrastructure and reduce the risks of cyber attack. This measure is estimated to secure a further 900-1100 MSPs.[4] While we expect this measure to have associated costs related to security improvements and compliance, these investments will position MSPs as trusted and reliable partners in the cyber security landscape.

[2] Firms covered could include but not limited to those offering services such as managed IT services, IT infrastructure and applications management, IT remote support and systems integration and management (SIAM), managed security services such as and managed security service providers (MSSPs), managed security operations centre (SOC), security information and event management (SIEM), incident response and threat and vulnerability management and relevant business process outsourcing.

[3] By "relevant digital service providers" we mean the providers of the kind of digital service defined under NIS Regulations 2018 Regulation 1(2). Currently this refers to online marketplaces, online search engines and cloud computing services. In future, this will also include managed service providers once brought into scope of the regulatory framework through the Bill.

[4] https://www.gov.uk/Government/publications/research-on-managed-service-providers/research-on-uk-managed-service-providers

1.2 Strengthening supply chain security and enabling regulators to designate ‘Critical Suppliers’

1.2.1 Summary of intent

Supply chains underpin the essential services and digital infrastructure that our economy and society rely on. A single supplier’s disruption can have far-reaching impacts on the delivery of essential or digital services. Currently, however, there is no targeted mechanism to address critical supply chain vulnerabilities under the 2018 Regulations.

The Bill will enable the Government to set stronger supply chain duties for operators of essential services (OES) and relevant digital service providers (RDSP) in secondary legislation, subject to consultation. It will also introduce a power for regulators to identify and designate specific high-impact suppliers as ‘designated critical suppliers’ (DCS), bringing them under comparable obligations as OES and RDSP. This will also extend to certain small and micro RDSPs where they play a pivotal role in supporting essential services.

By embedding supply chain security requirements directly into our regulatory framework, we aim to enhance national cyber resilience and reduce the threat of significant disruptions to critical services if a regulated entity is impacted by an attack on their supply chain.

1.2.2 How the measure would work in practice

Supply Chain Duties for OES and RDSP

The Bill will empower the Government to clarify, in secondary legislation, duties on OES and RDSP to manage supply chain cyber risks. These duties will be designed to ensure appropriate and proportionate measures are taken – such as contractual requirements, security checks, or continuity plans – to prevent vulnerabilities in suppliers from undermining essential or digital services.

Designation of Critical Suppliers

Regulators will be able to individually designate a supplier as a DCS if the supplier’s goods or services are so critical that disruption could cause a significant disruptive effect on the essential or digital service it supports. DCS are therefore expected to account for a very small number and percentage of those suppliers providing goods or services to OES and RDSP. Designation will bring such suppliers directly within scope of core security requirements and incident reporting obligations, ensuring consistent standards across the most critical tiers of the supply chain. The threshold criteria for designation are likely to be:

- Supply of goods or services: The supplier provides goods or services (including digital services) to an OES (regulated by that regulator) or to an RDSP (in the case of the ICO).

- Significant disruptive effect: The regulator judges that a failure or disruption in that supplier's goods or services – or an incident affecting the supplier's network and information systems – could have a significant disruptive effect on the provision of the essential or digital service.

- Reliance on networks and information systems: The supplier's goods or services depend on networks and information systems, making them relevant to the scope of the regulatory framework. This is intended to ensure that suppliers only fall within scope if their goods or services involve or rely upon technology (such as IT infrastructure or operational technology) that could be targeted or disrupted.

- Not already regulated: The supplier is not subject to similar cyber resilience regulations elsewhere (e.g., under Part 2 of the Communications Act 2003, as amended by the Telecommunications (Security) Act 2021) or elsewhere under the 2018 Regulations.

Extending Regulation to Certain SME RDSPs

RDSPs

Currently, small and micro RDSPs are exempt from the 2018 Regulations. Under these proposals, regulators may designate a smaller RDSP as a critical supplier if it meets the designation criteria outlined above. This ensures proportionate regulation of high-risk suppliers, regardless of size.

Futureproofing and Consultation

The Bill will provide flexibility to refine these duties and threshold criteria through secondary legislation, subject to appropriate consultation. This ensures requirements can be updated in line with technological changes, emerging threats, and lessons learned from implementation.

1.2.3 Impact

This new regime will create strong incentives for both regulators and regulated entities to ensure effective oversight of supply chain risk. By addressing supply chain vulnerabilities and ensuring that key suppliers meet appropriate security standards, we intend to reduce the risk of significant disruptions to essential and digital services, enhance national cyber resilience, and bolster trust in critical infrastructure.

We remain committed to minimising regulatory burden on small businesses and ensuring only a small number of critical SME RDSPs are eligible for designation under this measure. The narrow designation grounds we are proposing will ensure this.

2. Empowering regulators and enhancing oversight

We can only bolster the UK's cyber security if our regulators are well-prepared to take on their new responsibilities and we as Government have strong data on the cyber threat. That is why, in the King's Speech, we committed to putting regulators on a stronger footing to ensure essential cyber safety measures are being implemented. We also committed to improved incident reporting to improve our understanding of the threats.

The measures outlined in this section are focused on ensuring that regulators have the right tools and the clarity of purpose to deliver on this Government's ambitions.

2.1 Technical and methodological security requirements

2.1.1 Summary of intent

The NCSC Cyber Assessment Framework (CAF) is a resource that supports OES and firms that provide digital services to manage and assess their cyber risks. CAF profiles support the development of target levels of cyber resilience within sectors and for organisations in respect of specified vital functions. Two of the types of CAF profile are the Basic Profile and the Enhanced Profile. These set out principles and objectives that organisations should meet to assess and manage their cyber security.

The Government's intent is to establish these principles and objectives on a firmer footing, making it essential for firms to follow best practice and easier for them to do so. This will ensure that firms can invest in cyber security with greater clarity on what is required and make it simpler for the regulators to oversee the requirements.

While expectations on technical standards and methods were put on a statutory footing in the 2018 Regulations, they only relate to digital services firms. This measure will update those requirements, bringing them into closer alignment with NIS2 as well as, where appropriate, allowing them to be extended to operators of essential services.

2.1.2 How the measure would work in practice

The Bill will provide the Secretary of State with powers to make regulations to update the existing requirements. The Secretary of State would be able to exercise these powers following consultation with appropriate bodies.

Further, this would provide the Secretary of State with powers to issue a code of practice setting out guidance on how the regulatory requirements should be satisfied.

There are often more than one-way outcomes that can be achieved, so businesses and regulators benefit from additional clarity.

The measure will provide the Secretary of State with powers to tailor the requirements for each sector, as appropriate and proportionate.

2.1.3. Impact

This measure will enable the Government to set clear expectations for firms that provide digital services and operate essential services in scope of the Bill, to ensure proportionate and up to date security requirements are in place, while providing a means to update these requirements in response to a changing threat landscape.

2.2 Improving incident reporting

2.2.1 Summary of intent

Reporting of significant cyber incidents provides regulators and NCSC with a better view of the evolving threat landscape, enabling timely assistance where necessary and improved resilience. Many significant events go unreported under the current framework, limiting the ability to identify and assess vulnerabilities.

The Bill will update and enhance the current incident reporting requirements for regulated entities by expanding the incident reporting criteria, updating incident reporting times, streamlining reporting, and enhancing transparency requirements for digital services and data centres. The Government's work on ransomware, currently under consultation (closing 8 April), will complement the Bill, both DSIT and the Home Office will continue to collaborate to ensure that any future frameworks are aligned and do not create duplication. These proposals are intended to put regulators on a stronger footing to address emerging risks, helping to build our overall cyber resilience.

2.2.2 How the measure would work in practice

<u>Expanding the incident reporting criteria</u>

Under the current NIS regulations, for an incident to be reportable, it must have resulted in interruption to the continuity of the essential or digital service. This is too narrow in scope and many incidents of concern are not reported. The Bill will expand this to capture incidents that are capable of having a significant impact on the provision of the essential or digital service, and incidents that significantly affect the confidentiality, availability, and integrity of a system. This will include the compromise of data confidentiality, spyware attacks that use firms that provide digital services (including MSPs) as a vector to access other organisations, or other incidents significantly affecting the integrity of a system.

Updating incident reporting times

The Bill will introduce a two-stage reporting structure which will require regulated entities to notify their regulator and also inform NCSC of a significant incident no later than 24 hours after becoming aware of that incident, followed by an incident report within 72 hours. This initial notification will serve as an ‘early warning,’ bringing the incident to the attention of the regulator sooner than current practice. In practice, we intend for this procedure to be similar to, and no more onerous than, the equivalent requirements under the EU’s NIS2 Directive.

Streamlining reporting

Regulated entities will be required to report an incident to their regulator and also inform NCSC at the same time, ensuring that NCSC receives the same information as the regulator at the same time. This information will contribute to both the regulators' and NCSC's understanding of the threat landscape.

Enhancing transparency requirements

Firms that provide digital services and data centres that experience a significant incident will be required to alert customers who may be affected by that incident. This will encourage openness and accountability among the services in scope.

2.2.3 Impact

This measure is designed to increase the UK’s resilience to cyber attacks by ensuring regulators are promptly informed about incidents in their critical sectors. Transparency requirements will raise standards across service providers and customers will be better informed when the service they rely on could be affected or have a knock-on effect on their business. We are confident these changes will further strengthen the UK’s resilience to cyber threats, balancing the need for increased cyber security with the importance of managing costs effectively for regulated industry.

2.3 Improve the Information Commissioners Office's information gathering powers

2.3.1 Summary of intent

The Information Commissioner's Office (ICO) is the regulator for firms that provide digital services (Relevant Digital Service Providers (RDSPs)), regulating online marketplaces, search engines, cloud services and – once the Bill is implemented – managed services.

The intention is to support the ICO in their ability to proactively identify cyber risks and take appropriate steps to prevent imminent attacks. The increasing threat posed by vulnerabilities in digital services, with the services supplied at scale and across multiple sectors, means the ICO's previous reactive approach is no longer deemed sufficient relative to the risks posed. The primary intent of this measure is to enhance the ICO's capability to identify and mitigate cyber risks before they materialise, thus preventing attacks and strengthening the digital services sector against future threats.

2.3.2 How the measure would work in practice

The Bill will address the current challenges by providing the ICO with more information to enable it to identify the most critical firms that provide digital services. This will enable it to adopt a proactive, rather than reactive, approach to assessing the cyber security capabilities of digital services. The Bill will:

- Enhance the ICO's ability to gather information to assist them in determining the criticality of regulated digital services and their risk-based approach. This includes:
    - an expanded duty for firms that provide digital services to share information with the ICO on registration,
    - expanded criteria for ICO to use their existing current power to serve information notices on firms that provide digital services, and
    - appropriate information gateways for other entities, outside the scope of the NIS Regulations, to share information with the ICO
- Introduce powers for ICO to enforce a failure to register with the ICO.

2.3.3 Impact

In adopting a more proactive supervisory approach for the most critical firms that provide digital services, the ICO will likely incur additional costs associated with the ongoing monitoring of these entities. These will include the cost of evidence collection, review, analysis, and feedback. We recognise that this will be a challenging and complex task and intend to work closely with the ICO to ensure that appropriate support is in place.

2.4 Improve regulators' cost recovery mechanisms

2.4.1 Summary of intent

An effective regulatory regime requires independent, well-equipped regulators that are able to fully carry out all of their functions and help protect the key services our economy relies on. The current regulations need to be updated as they limit regulators' ability to recover costs and creating cash flow challenges.

The Government intends to improve the cost recovery regime and introduce a more modern, comprehensive, and flexible regime in line with other similar legislation in the UK. It will allow regulators to set a fees regime, recover costs, or a mixture of these processes to cover the expenses of this regulation, including enforcement, and reduce the need to pass regulatory costs to the taxpayer.

2.4.2 How the measure would work in practice

The Bill will introduce the ability for regulators to set up new fee regimes, allowing for fees to be levied as well as recovering costs via invoices. It will also clarify the intent and scope of the costs regulations and extend this regime to all activities necessary for the performance of the regulators' functions, including enforcement.

This measure will introduce:

- A power to request information from regulated entities, so that regulators can set appropriate fees, proportionate to the sectors they regulate;
- A duty on regulators to publish a Statement of Charging Principles setting out the principles, methodology, and process for raising these funds, as is the practice across many regulatory frameworks;
- A duty on regulators to consult with their OES and firms that provide digital services when setting fees and a duty to issue an end-of-cycle statement setting out how these funds are being used;
- A duty on regulated entities to pay the fee.

This regime is intended to ensure that regulators operate at cost and are able to carry out the full extent of their functions.

2.4.3 Impact

The proposed measures will ensure that regulators are financially independent and capable of effectively performing their duties, including enforcement, by allowing them to proactively raise funds. In practice, we expect regulators to make varied use of these powers and incorporate them into their existing processes and legal duties.

Overall, we expect this measure will address current cash flow challenges and prevent the financial burden of regulation breaches from falling onto the taxpayer, thereby promoting a more transparent, robust, and reliable regulatory environment.

3.Ensuring the regulatory framework can keep pace with the ever-changing cyber landscape

New technologies and emerging threats require agile regulations. It is important for national security that our regulatory framework is not stagnant. The measure outlined in this section ensures that the Government is not beholden to the timescales of primary legislation if the regulations require updating in the future.

3.1 Delegated powers – ensure the regulatory framework is adaptable to emerging threats

3.1.1 Summary of intent

In light of the rapidly evolving cyber threat and technology landscape, Government must be able to update regulations to mitigate new risks and to capitalise on technological advancements. This measure seeks to grant new powers to the Secretary of State, enabling the legislative framework to be updated to ensure it is current and effective.

3.1.2 How the measure would work in practice

Through the Bill, the Secretary of State will seek powers to update the regulatory framework without requiring an Act of Parliament, subject to certain safeguards. Such powers could be used to bring new sectors and sub-sectors in scope of the regulations and make changes to the responsibilities and functions of NIS regulators. Delegated powers will enable the Government, after any appropriate consultation, to introduce new requirements and duties for regulated entities, as further described above in sections ‘1.2 Strengthening Supply Chain Security and enabling regulators to designate critical suppliers’ and ‘2.1 Technological and methodological security requirements’, where these are considered appropriate and proportionate to impose on digital firms or operators of essential services.

3.1.3 Impact

The proposed measure will ensure that cyber legislation remains relevant and effective by providing a mechanism for timely updates. This will enhance the UK's regulatory framework, particularly in sectors critical to national security and economic stability. It also provides flexibility to these measures to adapt and accommodate changes in the CNI landscape. Ultimately, the measure will support and better maintain proportionality in regulation, and ensure ongoing protection of essential services, thereby benefiting both the Government and the public.

Additional measures under consideration

The cyber landscape is constantly evolving, and cyber actors are changing their tactics to circumvent protections. In recognition of this, we have set out four measures under consideration, which are additional to the commitments made in the King's Speech. The Government will consider the most appropriate legislative vehicle to take forward these measures in due course, which could be this Cyber Security and Resilience Bill.

1. Bring data centres into scope of the regulatory framework

1.1 Summary of intent

Data centres house and support the technology and data that meet the demands of our digital lives. They underpin almost all economic activity and innovation, including the development of AI and other technology, public service delivery, and how we interact with one another. Disruption or compromise of data centre infrastructure can therefore have significant negative impacts on the public, businesses, and national and economic security.

Following the King's Speech, data centres were designated as CNI in September 2024. In recognition of this, the Government is committed to introducing proportionate regulatory oversight. Bringing data centres into scope of the regulations would strengthen and level the consistency of protection across the sector, provide a platform for secure growth and investment, and give Government and a designated regulator the levers to steward the sector in the face of an evolving threat landscape in line with other CNI utilities.

1.2 How the measure would work in practice

Data infrastructure would be classified as a relevant sector and data centres an essential service. Based on feedback to the 2023 consultation, the Government intends to include data centres within the scope of regulations irrespective of the nature of service(s) offered from them and their ownership.

UK data centres would be in scope at or above 1MW capacity unless it is an enterprise data centre which will only be in scope if they are at or above 10MW capacity.[5] The operation of a data centre (that meets the thresholds in the UK) will require duties to be met. This would include notifying and providing certain information, having in place appropriate and proportionate measures to manage risks, and reporting significant incidents.

[5] Enterprise data centres are those operated by a business solely to deliver and manage the IT needs of the business.

The scope would be adjustable over time, under specified conditions, to account for developments in the market and risk landscape.

1.3 Impact

By bringing data centres into scope, the Government aims to strengthen the protection of CNI and all it supports and enables. Externally commissioned research (2024) indicates that there are currently 224 colocation data centres in the UK, managed by 68 operators. Of these, around 182 third-party sites and 64 operators will fall within scope. We expect the number of enterprise data centres within scope of full duties to be relatively low.

This measure is designed to balance security and resilience with the need for growth and investment, recognising that they support each other. We therefore do not intend or expect responsible operators to incur significant compliance costs, but we would provide a full impact assessment upon legislating.

2. Publish a statement of strategic priorities for regulators

2.1 Summary of intent

As this Cyber Security and Resilience Bill will expand the scope of the regulations to bring in new sectors, consistency across different regulators and coherence of approach across sectors becomes increasingly important for regulators and the wider market. That is why we are considering a new measure to provide a clear and coherent framework for cyber security regulation across the twelve regulators and their sectors.

The Government is considering introducing a new power for the Secretary of State to publish a Statement of Strategic Priorities. This measure draws on successful models from other regulatory regimes, such as telecoms and online safety, to establish a unified set of objectives and expectations for the implementation of the regulations.

2.2 How the measure would work in practice

The new measure would include a new duty for regulators, tied to the objectives contained within the statement. The objectives set out in a statement of strategic priorities would be developed in consultation with sectors and regulators periodically.

We propose that the Secretary of State would be required to consult with regulators before publishing a Statement of Strategic Priorities and, once issued, the Statement will need to be laid before Parliament to enable scrutiny.

A published Statement is intended to be updated once every three to five years and will be accompanied by a requirement for regulators to report annually on their progress against the objectives contained within the Statement.

2.3 Impact

The Statement would serve as a crucial instrument to streamline roles, responsibilities, and expectations, ensuring that all regulators, across all relevant sectors are implementing the regulations in a consistent manner. Reporting requirements would reassure ministers, the public, and Parliament that appropriate measures are being adopted across sectors.

3. Powers of direction

We are proposing new executive powers for Government to enable swift and decisive action in response to cyber threats, ensuring rapid and effective protection.

Empowering the Government to respond effectively is crucial for national security. The following powers would enhance our ability to protect critical infrastructure and essential services, strengthening the nation's resilience in a digitally enabled economy.

Empower the Secretary of State to direct a regulated entity to take action, when it is necessary for national security.

3.1 Summary of intent

We are proposing a new power for the Secretary of State to issue directions to regulated entities, requiring them to take action to address threats to and incidents affecting their systems where there is a significant threat to national security.

At present, the Government does not have a power to direct regulated entities to address cyber threats, even where this is judged to be essential for safeguarding national security. The growing threat posed by high capability actors and hostile states means that this is a gap that could be exploited with increasing regularity and impact, putting the operation of the UK's critical infrastructure at risk.

This new measure would ensure the Government can intervene directly to protect networks where necessary for national security.

3.2 How the measure would work in practice

We are considering equipping the Secretary of State with the power to issue a direction to a regulated entity in relation to a specific cyber incident or threat, requiring the entity to take action to remedy the incident or threat. The Secretary of State would only be able to issue a direction where necessary and proportionate for reasons of national security.

Where practicable and provided it would not compromise national security, an entity would be given the opportunity to make representations before it receives a direction.

Once issued, a direction would be laid in Parliament to enable public scrutiny, unless doing so would present a national security risk.

The Secretary of State would be responsible for monitoring and enforcing compliance with directions. We are considering the appropriate enforcement regime for the powers, recognising the importance of complying with a direction for national security reasons. We will also consider the precedents set by the Telecommunications (Security) Act 2021.

3.3 Impact

The power to direct regulated entities would ensure that the Government can respond swiftly to incidents and threats with significant national security risks – protecting critical infrastructure from sophisticated cyber threats.

Empower the Secretary of State to direct a regulator to take action when it is necessary for national security

3.4 Summary of intent

We are considering equipping the Secretary of State with a new power to issue a direction to a regulator on national security grounds, requiring them to exercise their functions to ensure that action is undertaken across their sectors.

The current system requires regulated entities to undertake 'appropriate and proportionate' measures to secure themselves against cyber threats, and regulators issue guidance to their sectors to help them interpret this duty. However, the Government needs the ability to require regulators to, for example, issue guidance stating that 'appropriate and proportionate' security measures are likely to require certain levels of network monitoring and testing. This presents a gap if the Government considers that more stringent security measures are required due to a worsening threat landscape.

This measure is intended to address this gap, by providing the Secretary of State with the power to direct regulators to advise their sectors to adopt more stringent cyber security measures, where this is necessary for national security.

3.5 How the measure would work in practice

Secretary of State would have powers to issue a direction to regulators. The power would only be used where necessary for national security, and where the impact of a direction is deemed to be proportionate.

We would set out requirements for regulators in receipt of a direction to submit reports to the Secretary of State, outlining how they have implemented the direction.

The Secretary of State would not be able to issue directions to other Secretaries of State or Devolved Governments.

3.6 Impact

The power to direct regulators would serve as an essential tool to ensure that whole sectors are more resilient against cyber security threats in periods of heightened risk.

Conclusion

Changes in global politics and developments in technology mean that the UK is facing greater challenges to its cyber security than ever before. The proposals that we have put forward in this statement aim to meet those challenges, providing robust measures to address the evolving threat landscape.

It is clear that this is the right time to update the UK's legacy frameworks, address gaps in the current regulation, and ensure that all relevant entities are brought within scope of the rules. Through these measures, we will make sure that our critical infrastructure and services remain protected – for people across the UK to rely on.

Our proposals will ensure that critical infrastructure is protected from hostile actors – securing essential services, such as the NHS and energy providers. Improved standards and regulation will also foster the secure networks and systems that are essential for business growth and innovation.

This Cyber Security and Resilience Bill is one essential tool in the Government's wider approach to addressing the threat posed by cyber attacks, reflecting our commitment to safeguarding the digital economy through a wider tapestry of measures and initiatives. It reflects the Government's commitment to safeguarding the digital economy through a wider tapestry of measures and initiative.

E03328649

978-1-5286-5588-0

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank