Public Document Pack

Economic and Cyber Crime Committee of the City of London Police Authority Board

Date: **WEDNESDAY, 5 MAY 2021**

Time: 9.00 am

Venue: **VIRTUAL PUBLIC MEETING (ACCESSIBLE REMOTELY)**

Members:

Deputy James Thomson (Chair)
Tijs Broeke (Deputy Chairman)
Deputy Keith Bottomley
Alderman Emma Edhem
Alderman Timothy Hailes
Andrew Lentin (External Member)
Dawn Wright
Graeme Doshi-Smith
Alderman Bronek Masojada
Chair of Policy & Resources (or Nominee)
Policy & Resources Committee Representative

Enquiries: **Chloe Rew - chloe.rew@cityoflondon.gov.uk**

Accessing the virtual public meeting

Members of the public can observe this virtual public meeting at the below link:
https://youtu.be/xQvcJGtPjj0

This meeting will be a virtual meeting and therefore will not take place in a physical location following regulations made under Section 78 of the Coronavirus Act 2020. A recording of the public meeting will be available via the above link following the end of the public meeting for up to one municipal 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.

John Barradell
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. **TERMS OF REFERENCE**

To receive the terms of reference appointing the Committee for the ensuing year, as agreed at the meeting of the Police Authority Board on 16 April 2021.

For Information
(Pages 1 - 2)

4. **MINUTES**

To agree the public minutes and non-public summary of the previous meeting held on 3 February 2021.

For Decision
(Pages 3 - 8)

5. **CHAIR'S PUBLIC UPDATE**

For Information

6. **T/COMMANDER'S PUBLIC UPDATE**

For Information

7. **NATIONAL LEAD FORCE PLAN UPDATE**

Report of the Assistant Commissioner.

For Information
(Pages 9 - 14)

8. **INNOVATION & GROWTH - OVERVIEW OF CYBER & ECONOMIC CRIME RELATED ACTIVITIES**

Report of the Executive Director, Innovation & Growth.

For Information
(Pages 15 - 18)

9. **CYBER GRIFFIN - OVERVIEW**

Report of the Assistant Commissioner.

To be read in conjunction with the non-public appendix at item 22.

For Information
(Pages 19 - 34)

10. **ECONOMIC CRIME ACADEMY UPDATE**

Report of the T/Commander.

For Information
(Pages 35 - 36)

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

12. **ANY OTHER BUSINESS THAT THE CHAIR CONSIDERS URGENT**

13. **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 item(s) 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 Agenda

14. **NON-PUBLIC MINUTES**

To agree the non-public minutes of the meeting held on 3 February 2021.

For Decision
(Pages 37 - 40)

15. **NON-PUBLIC REFERENCES**

Joint report of the Town Clerk and Commissioner.

For Information
(Pages 41 - 44)

16. **CHAIR'S NON-PUBLIC UPDATE**

Chair to be heard.

For Information

17. **T/COMMANDER'S NON-PUBLIC UPDATE**

T/Commander to be heard.

For Information

18. **ECONOMIC CRIME DIRECTORATE PERFORMANCE REPORT Q4 - JANUARY-MARCH 2021**

Report of the Commissioner.

For Information
(Pages 45 - 62)

19. **NATIONAL POLICE CHIEF COUNCILS (NPCC) CYBER CRIME PORTFOLIO**

Report of the Assistant Commissioner.

For Information
(Pages 63 - 88)

20. **STAKEHOLDER ENGAGEMENT AND POLICY UPDATE**

Joint report of the Commissioner and the Town Clerk.

For Information
(Pages 89 - 98)

21. **FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE - NEXT GENERATION AND CURRENT SERVICE UPDATE REPORT**

Report of the Assistant Commissioner.

For Information
(Pages 99 - 102)

22. **NON-PUBLIC APPENDIX TO CYBER GRIFFIN - OVERVIEW**

To be read in conjunction with the Cyber Griffin - Overview report at item 9.

For Information
(Pages 103 - 140)

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

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

Economic and Cyber Crime Committee

Composition

- Up to six Members of the Police Authority Board appointed by the Police Authority Board (in addition to the Chair and Deputy Chair of the Board).
- Up to four co-opted Members to be appointed by the Police Authority Board.
- Chair and one other Member of the Policy and Resources Committee, to be appointed by that Committee.
- Up to one external Member, to be appointed by the Police Authority Board.

Terms of Reference

To be responsible for:

a. *overseeing the force's national responsibilities for economic fraud and cyber crime having regard to the strategic policing requirement in this area;*

b. *monitoring government, and other external agencies' policies and actions relating to economic crime;*

c. *overseeing the delivery of the City of London National Lead Force Plan;*

d. *monitoring the implementation of any external review recommendations related to economic, fraud and cyber crime (including, but not restricted to, Mackey Review, HMICFRS Fraud related inspections, Tori Consultant Review);*

e. *overseeing of the City of London Police's private sector partnerships with regard to the tracking of fraud, cyber-crime & economic crime;*

f. *identifying and oversee opportunities to exploit the synergies between the Corporation's Cyber Security agenda and that of the City of London Police;*

g. *overseeing the business strategy, service and financial performance of the Economic Crime Academy;*

h. *overseeing the Force's national responsibilities as the National Police Chiefs Council (NPCC) lead for the Cyber Portfolio;*

i. *overseeing the work of Cyber Griffin initiative; and*

j. making recommendations to the Police Authority Board in any other matters relating to economic crime.

Frequency of Meetings
Quarterly

ECONOMIC CRIME COMMITTEE OF THE CITY OF LONDON POLICE AUTHORITY BOARD

Wednesday, 3 February 2021

Minutes of the meeting of the Economic Crime Committee of the City of London Police Authority Board held virtually on Wednesday, 3 February 2021 at 10.00 am

Present

Members:

Deputy James Thomson (Chairman)
Nicholas Bensted-Smith
Tijs Broeke
Alderman Emma Edhem
Alderman Timothy Hailes
Andrew Lentin
Deputy Robert Merrett
Benjamin Murphy
Dawn Wright

In Attendance:

City of London Police Authority:

Simon Latham	-	Deputy Chief Executive
Oliver Bolton	-	Deputy Head of the Police Authority Team
Polly Dunn	-	Town Clerk's Department
Chloe Rew	-	Town Clerk's Department
Aqib Hussain	-	Chamberlain's Department

City of London Police Force

Angela McLaren	-	Assistant Commissioner
Clinton Blackburn	-	T/Commander
Christopher Bell	-	City of London Police
Alix Newbold	-	City of London Police

1. **APOLOGIES**
   Apologies were received from Doug Barrow, James Tumbridge and Deputy Philip Woodhouse.

2. **MEMBERS DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
   There were none.

3. **MINUTES**
   RESOLVED, that – the public minutes and non-public summary of the meeting held on 16 November 2020 be agreed as a correct record.

Matters arising:

The Chairman noted that the strategic communication and engagement plan would be addressed in the Assistant Commissioner's Public Update.

4. **CHAIRMAN'S PUBLIC UPDATE**

The Chair provided the following update:

- The Force had been engaging with Police and Crime Commissioners (PCC) around fraud and cyber-crime, and noted the importance of raising awareness of the Force's work in these areas;
- The Home Office had reviewed the strategic policing requirement and recognised that fraud and cyber-crime should be included more prominently;
- The Chair met with the MP for the City & Westminster to discuss supporting fraud and cyber-crime work more publicly.

5. **ASSISTANT COMMISSIONER'S PUBLIC UPDATE**

The Assistant Commissioner provided the following update:

- Given the breadth and ongoing activity related to the Lead Force Plan, it would be beneficial to have a programme to establish a coordination role and report back to the Committee on a quarterly basis;
- The Force had a proactive communication programme to address scams, particularly those related to romance and investment fraud;
- The Communication and Engagement Plan is an integral piece of work related to other policing strategies and would therefore be brought to the Committee at the same time as a refreshed policing plan, to recognise the synergies.

6. **ANNUAL REVIEW OF TERMS OF REFERENCE**

Members considered a report of the Town Clerk in respect of the Annual Review of the Committee's Terms of Reference.

The Chair emphasised the importance of referencing fraud and cyber together in the Terms of Reference, and to emphasises the Committee's role in oversight, rather than scrutiny.

RESOLVED, that – Members agree the following changes:

1. the addition of 'one external Member, to be appointed by the Police Authority Board' in the Committee's composition;
2. the addition of the following responsibilities in the Committee's Terms of Reference:
    - a. overseeing the force's national responsibilities for economic crime, fraud and cyber, having regard to the strategic policing requirement in this area;
    - c. overseeing the delivery of the City of London National Lead Force Plan;

- d. monitoring the implementation of any external review recommendations related to economic crime, fraud and cyber (including, but not restricted to, Mackey Review, HMICFRS Fraud related inspections, Tori Consultant Review);
- e. overseeing of the City of London Police's private sector partnerships with regard to the tracking of fraud, cyber-crime & economic crime as well as the joint Cyber Griffin project;
- f. overseeing the business strategy, service and financial performance of the Economic Crime Academy;
- g. overseeing the Force's national responsibilities of the National Police Chiefs Council (NPCC) lead for the Cyber Portfolio;
- h. overseeing the work of Cyber Griffin initiative; and,
- i. making recommendations to the Police Authority Board in other matters relating to economic crime.

7. **ECONOMIC CRIME ACADEMY UPDATE**

Members considered a report of the T/Commander relative to the Economic Crime Academy (ECA) update. The T/Commander noted that some courses had been postponed due to the pandemic, however courses would resume once restrictions lift. A stronger move to online training would increase capacity per course and have wider national and international reach, and a fully online course was in development in partnership with Coventry University and Lloyds Bank for counter fraud qualifications. 90% of forces across the UK were engaged with the programme, and advertising and branding strategies were being employed to expand the ECA's reach. The T/Commander also reported that discussions were underway with the College of Policing to establish courses for economic crime and policing and this would be reported back to the Committee as discussions progressed.

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

8. **NATIONAL LEAD FORCE (NLF) IMPLEMENTATION PLAN**

Members received a report of the Assistant Commissioner relative to the National Lead Force (NLF) Implementation plan. The Assistant Commissioner emphasised the importance of taking a programmatic approach in delivering the NLF Plan. The plan is a 2020-2022 and would likely be used beyond this. The measures in the plan would be refreshed every year, and the Committee would receive updates on the plan on a quarterly basis.

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

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

There were none.

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

There was no other business.

11. **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 item(s) 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.

12. **NON-PUBLIC MINUTES**
RESOLVED, that – the non-public minutes of the meeting held on 16 November 2020 be agreed as a correct record.

13. **CHAIRMAN'S NON-PUBLIC UPDATE**
The Chair's non-public update was heard.

14. **ASSISTANT COMMISSIONER'S NON-PUBLIC UPDATE**
The Assistant Commissioner's non-public update was heard.

15. **NON-PUBLIC REFERENCES**
Members considered a joint report of the Town Clerk and Commissioner regarding non-public references.

16. **ECONOMIC CRIME DIRECTORATE PERFORMANCE REPORT - Q3 OCTOBER - DECEMBER 2020**
Members received a report of the Commissioner relative to the Economic Crime Directorate Performance for Q3 October to December 2020.

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

17. **NEXT GENERATION SERVICE UPDATE**
Members received a report of the Service Delivery Director relative to the Next Generation Service Update.

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

18. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were none.

19. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There was one item of urgent business.

The meeting ended at 11.19 am

Chair

Contact Officer: Chloe Rew
tel. no.: 020 7332 1427
chloe.rew@cityoflondon.gov.uk

This page is intentionally left blank

Committee: Economic and Cyber Crime Committee – For information	**Dated:** 05/05/2021
Subject: National Lead Force Update	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1,10, 12
Does this proposal require extra revenue and/or capital spending?	**N**
If so, how much?	**NA**
What is the source of Funding?	**NA**
Has this Funding Source been agreed with the Chamberlain's Department?	**NA**
Report of: Assistant Commissioner McLaren	**For Information**
Report author: Alix Newbold	

SUMMARY

This report provides information on key activities delivered as part of the National Lead Force Plan. These activities include:

- progress on establishing a national proactive economic crime capability in four pilot regions
- launch of a North West Police Intellectual Property Crime Unit
- work to embed Project Otello intensification campaigns into sustainable police action
- roll out of a scheme to educate young people about online fraud through schools nationally

Recommendation(s)

It is recommended that members note the contents of this report.

MAIN REPORT

BACKGROUND

1. The National Lead Force Plan was approved by Police Authority Board in October 2020. The plan is structured around 5 key outcomes / aims with milestones and performance measures attributed to each milestone. This report will be a standing agenda item in future and will provide an overview of ongoing activity.

CURRENT POSITION

2020/21 Annual performance summary

2. 2020/21 has proven to be an extremely challenging year. We have experienced rising demand coupled with the need to quickly implement changes to working practices due to Covid19. Performance within the Action Fraud reporting service has been variable throughout the year and a drive to improve the service is a key focus in 21/22.

3. A number of areas of wider NLF performance have seen improvement in 20/21 this includes significant increases in confirmed funds repatriated to victims through partnership working with the banking sector, increased compliance across forces in relation to reporting compliance, and sustained delivery of training by the Economic Crime Academy through the use of an online platform.

Outcome 1: The public has confidence in the Action Fraud reporting service

4. Action Fraud is the National Fraud and Cybercrime Reporting Service delivered by COLP. Responsibilities include providing a first point of contact for victims of fraud, crime reporting and triage. We constantly seek opportunities to improve the quality of service delivered informed by user feedback. A number of activities are in progress including changes to staffing and recruitment models and technological improvements. One example of this is the chatbot rollout.

Website improvements

5. Recent improvements include:

    a. implementation of pop-ups and banners to inform victims in Scotland to report

    b. automatic prompts advising victims to request help via chat while reporting where there is any doubt regarding fraud type

    c. roll out of phase one of a chatbot which quickly directs victims to the right response and information freeing up call handlers to deal with the most vulnerable of victims

6. Chatbot is a virtual assistant application which complements and provides additional functionality to the current chat service. It is an automated platform that will be integrated with the current chat service provided. The chatbot delivers a virtual assistant to offer both menu assisted guidance and provide natural language understanding of the victim chat text offering appropriate information to better understand the service and how to submit a crime report. The three main functions of the chatbot in relation to user experience will mirror that of a live advisor:

    a. Accessibility for all including enhancing the digital self-service journey by providing guidance alongside self-serve

    b. Providing preventative information and education

c. Supporting users of the service to report as appropriate

7. Phase one was delivered on 31 March. It provides a parallel menu to the live advisor chat service driven by options to access the most common activities of visitors to the website. This includes new reports, scams, and providing and receiving updates. While providing the public with a guided digital service for these common activities, phase one also provides initial data to support the development of phase two.

8. Initial data shows the chatbot was accessed 57, 821 times in the first few weeks since deployment. In capacity terms, this equates to potentially freeing up the equivalent of 2-3 live advisor (in excess of 300 hours) to allow live advisors to focus on handling the significant demand the service is experiencing and providing live support to those who need it most. The initial data is encouraging and is in line with the expectations of capacity savings at the outset of the project, taking into account this is phase one data only.

9. Phase two is currently under design and will be ready for deployment at the end of May, subject to testing and deployment schedules. This phase will continue to provide a menu driven option for common activities and will also introduce a free text field where users can interact in the way that they do today with the chat service. The chatbot will respond where content is available. Using natural language recognition and continuing to learn over time, the chatbot will respond with preventative and educational information as well as prompting users to report as appropriate. To preserve the principle of accessibility, there will continue to be an ongoing availability of a live advisor option throughout the experience.

10. The benefits of chatbot will be a victim focussed service which further supports access for victims into the Action Fraud service. It will enhance the service we currently deliver and will create a greater capacity onto the Action Fraud full service.

11. For policing, this is a pioneering use of technology to support victims of crime. The project will be monitored and evaluated over the next year to ensure the technology is effectively supporting the user experience.

12. Other planned improvements to be delivered this year include a homepage broadcast for scam reporting linking to the phishing section of the website, an information banner to provide improved understanding of the role of Action Fraud and regularly updated news and articles on prevailing fraud types. The redevelopment of the web reporting element of the Next Generation Service has also been brought forward to 2021/22 which will deliver significant improvements to the user experience.

<u>Outcome 2: People and organisations are prevented from being victims of fraud, and victims are supported</u>

13. COLP is responsible for providing first contact support for victims who report to Action Fraud. It is also responsible for developing and disseminating national protect messaging for policing based upon latest crime reporting trends. COLP

is constantly looking for new channels to strengthen the reach and impact of fraud prevention advice to the public.

Juniors Scheme

14. Following a successful pilot in the City of London and Kent, COLP's Cyber Detectives programme will now be available to children across the UK to teach them all about fraud and cyber crime. The new nationwide programme aims to raise awareness of online fraud and its associated risks. It is a partnership between the City of London Police, Lloyds Banking Group who funded and co-developed the programme, and the Personal, Social, Health and Economic Education Association (PSHE) who will distribute the lessons to schools through a website link. The lessons will support pupils to:

    a. Explain what online fraud is and identify and analyse some examples of scams

    b. Describe the importance of protecting personal information and data online

    c. Explain why age restrictions for online games can help to keep people safe and prevent fraud

    d. Recognise ways to stay as safe as possible online and how to report concerns about online fraud

<u>Outcome 3: Police resources are coordinated and deployed efficiently and effectively</u>

15. City of London Police is responsible for developing and disseminating crime reports for intelligence, protect and pursue action to policing and other law enforcement through the National Fraud Intelligence Bureau. It is also responsible for leading and coordinating the police response to fraud. Its current focus includes increasing judicial outcomes and the effectiveness of operational activity undertaken by policing through leadership and coordination of activity against high harm crimes.

Project Otello

16. COLP continues to lead and coordinate the police response to Project Otello (a series of national campaigns to address high harm fraud types: courier fraud, romance fraud, investment fraud, covid-19 fraud and payment diversion fraud), extending the work beyond short term intensifications to sustainable police action.

17. Through coordinated operations and intelligence, there have now been over **150 arrests** for courier fraud since January 2020. In January 2021, COLP hosted a courier fraud surgery for forces to provide advice and share good practice nationally. During 2021, COLP's Lead Force Operations Room will lead on coordination of resources across NLF, local forces and regions on activity to proactively target of suspects and identify of victims for intervention / safeguarding.

18. The romance fraud campaign now has a social media reach of **11.3 million with 34.4 million impressions**. A recent appearance on BBC's For Love or Money resulted in an individual self-identifying as a victim of romance fraud and able to access support from Action Fraud. During 2021 NFIB will continue to work with forces to develop opportunities for disruption and pursue activity linked to romance fraud and extend its engagement with international partners .

Outcome 4: Fraudsters operating nationally are identified and their offending is being disrupted

19. City of London Police investigates nationally significant, serious and complex fraud on behalf of policing. It received referrals from a range of stakeholders including police forces, ROCUs, National Fraud Intelligence Bureau and the National Economic Crime Centre, as well as stakeholders linked to its funded units.

Dedicated Card and Payment Crime Unit (DCPCU)

20. DCPCU targets the organised criminal gangs responsible for fraud and is made up of officers from the City of London Police and Metropolitan Police Service and support staff from UK Finance. In 2020, DCPCU prevented almost £20 million of fraud and arrested 122 suspected criminals, including several involved in scams exploiting the COVID-19 pandemic. 54 criminals were convicted, with a total of 50 years in prison handed out to defendants. The convictions include a criminal involved in a large-scale campaign sending out fake text messages claiming to offer tax refunds from the UK government due to the pandemic, and the jailing of a courier scam fraudster who spent £5,000 in a two-day period on cards stolen from three elderly victims.

21. Close collaboration with social media and telecommunications partners enabled DCPCU to take down 731 social media accounts linked to fraudulent activity, of which 258 were involved in recruiting money mules. DCPCU seized £2.59 million of assets from criminal gangs, and recovered 18,175 compromised card numbers from active criminal gangs. The unit remains on the frontline in protecting the public against fraud and is currently investigating over 150 live cases, including several Covid-related scams.

22. COLP is engaging with UK Finance on opportunities to grow this unit.

Outcome 5: Policing has the capability and capacity to detect, disrupt and deter economic crime

23. City of London Police is a centre of expertise for fraud and is responsible for identifying , developing and disseminating good practice. It provides economic crime investigation training to policing, government and the private sector through its Economic Crime Academy. It is working with policing to build fraud capabilities and reform the fraud operating model.

Police Uplift Programme (PUP) / Proactive Economic Crime Network

24. City of London Police has received a PUP allocation of 30 FTE which are to be used to build national fraud capabilities.

25. The National Fraud Policing Strategy published in 2019 set out an ambition to develop a more dynamic and proactive response to fraud. It aimed to secure additional investment in regional pursue capabilities to "build a nationally networked and coordinated capability focussed on disruption of high harm threats". City of London Police intends to use its allocation of 30 FTE to pilot this in four ROCUs: North West, West Midlands, Yorkshire & Humber and Eastern.

26. The vision is to establish a new proactive economic crime capability targeting fraud, and money laundering associated with fraud. Across the four regions, the teams will operate as a national network led by COLP. The teams will work to NFIB control strategy high harm fraud priorities and nationally led pursue campaigns. The network will identify and investigate offenders, disrupt and dismantle OCGs, and seize and recover criminal proceeds.

27. An implementation board has been established with members from all participating ROCUs. A team profile has been developed and has been submitted to NPCC leads for economic crime and SOC for agreement. A performance framework and processes for tasking and coordination are in development. Tasking and coordination processes will align with the new model for tasking and coordination that is being developed in partnership with the NECC.

North West Police Intellectual Property Crime Unit (PIPCU)

28. The North West branch of the Police Intellectual Property Crime Unit was launched in March. It has already seized £1.7m worth of fake goods, including clothes, electricals and fireworks. North West PIPCU was created following a successful bid to the Intellectual Property Office by City of London Police to develop economic crime capabilities outside of the City. It is a partnership between City, the North West ROCU and Intellectual Property Office. The unit will combat intellectual property crime in the north west of England and support existing partners to disrupt and prosecute existing and new organised crime groups.

CONCLUSION

This report provides an overview of the NLF outcomes and highlights a selection of ongoing activities. This report will form a standing agenda at future committees and will be developed to include timelines and key millstones.

Committee(s): Economic Crime & Cyber Committee	**Dated:** 05/05/2021
Subject: Innovation & Growth – Overview of Cyber & Economic Crime related activities	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1, 6, 7
Does this proposal require extra revenue and/or capital spending?	**No**
What is the source of Funding?	**NA**
Report of: Executive Director, Innovation & Growth	**For information**
Report author: Mary Kyle - Head of FPS Technology	

Summary

The core objective of Innovation & Growth (IG) is to strengthen the UK's competitiveness as the world's leading global hub for financial and professional services (FPS). This includes promoting the strengths of the UK's offer and enhancing the UK's position as a leader in FPS technology and innovation.

Economic crime and cyber represent a hot topic for firms across the FPS sector. In 2020 the UK payments industry alone suffered total fraud losses of £1.26bn. IG's activities include promoting the UK's strengths, including in relation to both cyber and economic crime. They also support the development of the UK business environment and technology to equip FPS to respond to evolving threats.

This report summarises the relevant activity taking place across IG. It also highlights opportunities for IG to promote work being undertaken by the City of London Police.

Links to the Corporate Plan

1. IG's activities relating to economic crime and cyber help deliver against the Corporate Plan aim to support a thriving economy. This includes outcome 6c - to lead nationally and advise internationally on the fight against economic and cybercrime. It also supports outcome 7, positioning the UK as a global hub for innovation in financial and professional services.

Recommendations

Members are asked to note the report.

Main Report

Background

2. IG delivers a range of activity to support its overarching objective of strengthening the UK's competitiveness as the world's leading global FPS hub. There are many important aspects to competitiveness. These include ensuring that the surrounding eco-system is supportive, both from a regulatory aspect and in terms of nurturing

innovation. The activities set out below aim to enhance the UK's competitiveness and are relevant to the broader work being undertaken by the City Corporation and City of London Police on economic crime and cyber.

Recent Innovation & Growth Activity

Digital Sandbox

3. For UK FPS to thrive and remain competitive it needs to have access to innovative products and services that it needs. In 2020 the Financial Conduct Authority and City Corporation partnered to develop and deliver a Digital Sandbox pilot. The Digital Sandbox provides a virtual eco-system where technology companies can develop and test products responding to specific challenges faced by UK FPS. Out of 28 participating teams, 12 focused on products to prevent fraud and scams.

4. The technology being developed included solutions to detect and intervene in unusual behaviour by customers likely to be in response to payment fraud. There were also technologies used to identify suspicious behaviours and anomalous transactions amongst payment transactions and the development of networks to enable better information sharing between financial institutions.

5. Over 1000 users registered for the Digital Sandbox pilot including FPS firms, regulators, investors and other technology providers. Positive feedback on the pilot was received from participants and the broader FPS sector. The Chancellor also gave his support for developing a second phase of the Digital Sandbox during a recent speech at UK Fintech Week.

6. The City Corporation and FCA are in the process of developing a second iteration of the Digital Sandbox. This will focus on technology solutions to help FPS firms tackle sustainability and climate change-related activities. However, there are also plans to open up the platform for organisations that may wish to access the data and/or testing environment for other products. This includes discussions around technologies relating to cyber and economic crime.

Cyber Insurance Report

7. To remain globally competitive it is vital that UK FPS provides thought leadership in areas of emerging interest. In December 2020 the City Corporation launched the report 'The Future of Cyber Insurance: Next Steps for the London Market', in association with Accenture. The report stressed the importance of cyber insurance as a key growth area for the London market. It highlighted the opportunity for London, as the world's premier insurance centre and Europe's most concentrated cyber security centre. It also addressed some challenges. These include a persisting trust gap and the limited adoption of cyber standards. It was agreed that there needs to be collaboration across sectors, and that the City Corporation could play a key convening role.

8. On 28th January, the Chair of Policy opened the Global Cyber Insurance Summit 2021, which the City Corporation co-hosted with GIC Re and the Data Security Council of India. Discussions focussed on how London's cyber security ecosystem and the London Market can provide solutions and cyber insurance products that will benefit both India and the UK insurance industry.

Benchmarking Report

9. To track the UK's competitiveness, it is important to benchmark its position internationally. In January the City Corporation released benchmarking research entitled "Our global offer to business: London and the UK's competitive strengths in a changing world." The report considered competitiveness across 91 different metrics and highlighted London's competitive strengths as the leading city for FPS.

10. In particular, the report showed London as leading in terms of offering both an innovative ecosystem and a resilient business infrastructure. The work cited "the country's strong cyber security framework and digital security measures [which] offers firms a business environment they can operate in with trust." It also referred to the UK's top ranking in the ITU Global Cybersecurity Index and the Cyber Griffin programme.

RegTech Report

11. For UK FPS to evolve and improve its service offering it needs a supportive regulatory environment. On 16th April the City Corporation launched a report with RegTech Associates entitled '2021: A critical year for RegTech.' The report identified the key challenges and opportunities for UK RegTech as well as international best practice for driving growth. Information for the report was collated from 161 global RegTech firms along with both domestic and international regulators and financial institutions.

12. The report highlighted that almost one-third of global RegTech products relate to Financial Crime and around 16% to Cyber, Identity and Privacy. Adoption of RegTech is on the rise in these critical areas, but significant barriers to adoption remain. The recommendations for overcoming these barriers include increasing the awareness of the benefits of RegTech. There was also a call to the regulator to adopt a 'tech embracing' stance and issue clearer guidance on technology risk.

City of London Police

13. IG provided support to the City of London Police during the two-year pilot of the Cyber Griffin programme. This included promoting Cyber Griffin across stakeholder networks and raising its profile at both a domestic and international level. This was achieved by incorporating information about the programme into briefings, on the Global City website and in various reports and articles.

14. IG is keen to continue promoting Cyber Griffin and the broader work of the City of London Police. A broader dialogue has recently been developed between IG and City of London Police. This will continue to inform activity of mutual interest and identify areas where promotional or other support may assist either team.

Conclusion

15. A positive response to cyber and economic crime is an important component of the UK's competitiveness as a global FPS hub. Innovation & Growth is keen to share information about its activities relating to this topic. It is also well positioned to promote the broader work of the City Corporation and City of London Police.

Mary Kyle
Head of FPS Technology
Innovation & Growth
T: +44 (0) 7834 808 240
E: mary.kyle@cityoflondon.gov.uk

Committee(s): Economic and Cyber Crime Committee	**Dated:** 5 May 2021
Subject: Cyber Griffin – Overview	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1, 6, 7, 9, 10 and 12
Does this proposal require extra revenue and/or capital spending?	**Under discussion**
What is the source of Funding?	**Not determined**
Report of: Assistant Commissioner Angela McLaren	**For Information**
Report author: Sgt Charlie Morrison, Helen Thurtle	

Summary

The City of London's financial and professional services (FPS) industry faces a unique cyber threat which continues to grow in its severity. As a sector designated as Critical National Infrastructure, there is a need to offer enhanced protection from future cyber attacks. Work began on this in June 2018 when the City of London Police (CoLP) launched Cyber Griffin with the support of the Innovation and Growth Directorate.

At the close of its pilot period on the 1st April 2021, Cyber Griffin will have successfully met the objectives set by the Policy and Resources Committee (see Appendix 1). Moreover, an external review conducted by KPMG has confirmed the programme's impact on security as well as its value for money (Appendix 6). The same report has outlined out a number of local, regional and international opportunities for future development.

Over the same period the COVID-19 pandemic has dramatically changed the position of global business hubs and the services they must provide in order to remain world leading. The most valuable security programmes will be those which can meet the needs of a remote working culture. Increasingly, protecting the Square Mile and remaining a globally desirable place to do business, will mean giving the organisations present within it, protection which extends beyond the Mile itself.

Cyber Griffin responded to the pandemic by developing digital versions of its services which have exponentially increased the programme's capacity and deployment potential. Cyber Griffin is now in a position to deliver beyond the Square Mile. Such an offering supports policing objectives and compliments the Corporation's aim to remain a centre of investment and innovation in a rapidly changing global market.

As the newly appointed National Police Chiefs' Council (NPCC) lead for cyber, CoLP now seeks to build on the success of Cyber Griffin and wishes to investigate the opportunities set out in the KPMG report. In summary these include: Cyber Griffin taking on a national role within policing, the programme exploring overseas markets for revenue generation and Cyber Griffin developing its services further in line with KPMG's recommendations.

For these reasons CoLP are considering the following:

- To continue the work conducted and services offered by Cyber Griffin to support businesses and individuals in the Square Mile.

- How these developmental opportunities can be fully investigated and piloted.

- Additional officers to manage the increased workload these opportunities would create.

- The scope of Cyber Griffin being expanded in order to conduct work nationally and internationally in line with the developmental opportunities listed.

Links to the Corporate Plan

This overview primarily maps to Outcome 1 of the Corporate Plan – People are safe and feel safe. In particular, under this outcome the 'City Corporation commits to tackling fraud and cyber crime. This sits alongside the commitment under supporting a thriving economy to "lead nationally and advise internationally on the fight against economic and cyber crime (Outcome 6(c))."

The Cyber Griffin programme also supports the CoLP Corporate Policing Plan 2018 - 2023 – developing a world class digital policing environment, supporting safety by design and leading the delivery of a safe place to live, work and visit.

Recommendations:

Members are asked to note the report.

Main Report

Background

1. It is now a largely settled point that cyber criminality represents a substantial threat to global centres of business like the City of London and that in the coming decade this threat is set to steadily increase (see Appendix 2).

2. The COVID-19 pandemic has now triggered an even greater reliance on technology. Global business centres must now consider how they will evolve to meet this new environment and remain world leading within it. Alongside this, the pandemic has been a cyber event itself. From the start of outbreak, ransomware and phishing campaigns began to focus on the human and network security weaknesses the pandemic instigated (see Appendix 2).

3. Given the severity and borderless nature of cyber criminality, it is clear that for the City of London, effective policing and continued global business leadership requires the same innovation. Namely, to provide security to businesses within the Square Mile that can also extend beyond its borders. Future world leading security

services will be those which can protect an organisation as a whole, not just the offices in a given area.

Current Position

4. In response to these trends business centres around the world have begun to develop area-based programmes of digital protection such as Estonia's Cyber Security Vision 2019-2022 and Singapore's Cyber Security Unity Strategy (see Appendix 2). Here in the City of London we have the Corporation's Cyber Strategy of which Cyber Griffin is a part. Critically, Cyber Griffin is now ideally positioned to act as a world leading security brand for the Corporation. With its digital delivery platform and accredited officers, Cyber Griffin can protect organisations both in and outside of the Square Mile, and in so doing become an area-based security programme with an international reach.

5. The City of London's programme, Cyber Griffin was formally established in June 2018. Like its predecessor, Project Griffin (see Appendix 3), Cyber Griffin is driven by the principle that our best opportunities to tackle cyber criminality lie in improving our collective defences against it. Cyber Griffin (see Appendix 4) provides four core services which can be delivered digitally or in person. Each service is delivered by a specialist team of officers and designed to protect individuals and businesses in the Square Mile from cyber attack. These services are as follows:

   - **Baseline Briefings:** Non-technical briefings designed to take audiences through today's most prolific digital threats with the aim of teaching the simplest and most functional defences to each. This service is National Cyber Security Centre (NCSC) accredited.

   - **Table Top Exercise:** An interactive exercise used to explore simulated cyber security choices which mimic progressively complex cyber attacks with the aim of teaching strategy, managing security and decision making. This service is NCSC accredited.

   - **Incident Response Training:** A practical service in which officers teach police command structures and decision making models in the context of cyber incident response. This helps to develop improved cyber incident responses using tried and tested techniques developed in policing. This service is NCSC accredited.

   - **Cyber Capability Assessment:** A detailed assessment of an organisation's cyber security maturity level which includes a vulnerability assessment, a comparison of the organisation's maturity gauged against best practice standards and a road map for improvement.

Options

6. Now at the end of its pilot period, Cyber Griffin has met the targets set at the programme's creation. A report conducted in 2021 by KPMG confirms this, *'Cyber Griffin has delivered a consistently positive impact on cyber security in the Square*

Mile and established a trusted brand based on the quality of the services.' [1] Cyber Griffin has won multiple awards, engaged with over 460 companies and trained over 11,000 people. Additionally, KPMG recognised that, *'Cyber Griffin is the only cyber unit nationally that has achieved NCSC accreditation for three out of four core services. This differentiates Cyber Griffin from a significant number of private sector organisations.'* [2]

7. These accolades combined with the successes of the new digital delivery platform that Cyber Griffin has pioneered, have now presented the programme with a number of promising developmental opportunities. KPMG's report details these as follows:

   - Cyber Griffin to support the delivery of a national Cyber UK Strategy.[3]

   - Cyber Griffin to create a revenue raising capacity targeting overseas markets.[4]

   - Cyber Griffin to develop its existing services in the following ways[5] :

     - Incorporate the police initiative Cyber Alarm into the Cyber Griffin offering.
     - To begin development of Digital Security Coordinators (DSecCo's) – officers who assess the digital risk of police run events.
     - To develop an intelligence led mechanism into Cyber Griffin's delivery in order to better target vulnerable organisations and subsequently offer support.
     - Create a new cyber Incident Response Exercise which incorporates the research conducted by Bristol University with the existing training principles used by Cyber Griffin in its Incident Response Exercise.

For further details of each of the developmental services mentioned above please see Appendix 5. For details of KPMG's recommendations in regard to these services, please refer to the KPMG report (Appendix 6).

8. Overall Cyber Griffin has proved a trusted, impactive and cost-effective security programme which now presents excellent prospects for further development including the potential for revenue generation. The subject of this overview is to update members of the Police Authority Board (PAB) on the Cyber Griffin programme and to explain how it currently functions. Additionally, this overview sets out the opportunities for further development which could be considered in the future.

[1] KPMG, 'Cyber Griffin Evaluation for the City of London Corporation'.:5
[2] KPMG (n 1).:8
[3] KPMG (n 1).:22
[4] KPMG (n 1).:23
[5] KPMG (n 1).:22-24

Funding

9. The Cyber Griffin programme is currently supported by one Police Sergeant (a CoLP funded post), five PC/DC's and one D Grade Office Manager (funded by the Corporation's grant for Cyber Griffin in 2018). One PC/DC post is currently vacant.

10. Corporation of London funding for Cyber Griffin concluded at the end of this pilot programme on the 31st March 2021. Discussions are now being had as to how the programme should be funded in the future and which of the opportunities above should be investigated.

Performance Targets (April 2021 to April 2022)

Cyber Griffin will report on the following performance metrics:

11. The number of end users trained, businesses engaged with and services conducted. Over this period the programme aims to reach 7,000 individuals, 100 businesses and to deliver 150 services.

12. The satisfaction rate of attendees and businesses that Cyber Griffin engages with to ensure the services remain of the highest quality. In line with national reporting standards, the programme aims to achieve an above 75% satisfaction rate and accompanying positive qualitative feedback through survey responses.

13. The percentage of victims referred to Cyber Griffin from Action Fraud and other channels who are engaged with by Cyber Griffin officers. In accordance with national reporting standards, the programme aims to engage with 100% of all victims identified in the Square Mile.

The Cyber Griffin Reporting Lines:

14. A quarterly report to Team Cyber UK detailing the performance metrics listed above and a summary update of the programme's progress. The structure of this report is nationally standardised.

Corporate and Strategic Implications

15. In addressing the emerging cyber threats facing the City of London, Cyber Griffin directly contributes to the achievement of a number of outcomes from the Corporation's Corporate Plan. By building resilience within the City to, 'fraud and cybercrime' the proposal primarily maps to Outcome 12 – Our spaces are secure, resilient and well-maintained, under the theme of 'build resilience to natural and man-made threats by strengthening, protecting and adapting our infrastructure, directly and by influencing others.'

16. Cyber Griffin also enables the Corporation to assert national leadership and advise internationally on the fight against cyber crime, helping to promote the City's world

class legal and regulatory framework. This maps to Outcome 6 – We have the world's best legal and regulatory framework and access to global markets.

17. It also ensures the City remains a global hub for FPS innovation by supporting businesses in preparing for technological transformations of the economy and because partnership with Cyber Griffin could be a competitive advantage for organisations in the City (Outcome 7 – We are a global hub for innovation in financial and professional services, commerce and culture). Research indicates some firms are already considering how their cyber investment could be a value-add for their customers, either as a market differentiator or the basis for enhanced security-based products and services.[6]

18. More broadly, Cyber Griffin helps to maintain the competitiveness of the City's FPS offering, when faced with the innovative cyber protection programmes being launched by its competitors. This maps to Outcome 9 – We are digitally and physically well-connected and responsive, Outcome 10 – We inspire enterprise, excellence, creativity and collaboration and Outcome 1 – People are safe and feel safe.

Conclusion

19. At the conclusion of its pilot, Cyber Griffin has created a brand that is well regarded and reputable. The programme has also built a team of technically trained and NCSC accredited officers' capable of delivering its four core services (three of which are also NCSC accredited) to very high standards. Furthermore, Cyber Griffin won a number of awards and developed a digital platform of delivery significantly increasing its reach.

20. CoLP seeks to continue combatting cyber threats currently facing the City of London's FPS sector through the work conducted and services offered by Cyber Griffin.

21. With the opportunities now available to Cyber Griffin, CoLP is now considering how to investigate, and where possible to pilot, how the programme can be expanded on. These opportunities include: Cyber Griffin taking on a national role within policing, the programme exploring overseas markets for revenue generation and Cyber Griffin developing its core services further, in line with KPMG's recommendations.

22. Cyber Griffin is ideally positioned to act as a world leading cyber security brand for the Corporation. With continued support, Cyber Griffin can protect organisations both in and outside of the Square Mile, and in so doing become an area-based security programme with an international reach.

[6] TheCityUk, 'Governing Cyber Security Risk' <https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/governing-cyber-security-risk.html>.

Appendices

- Appendix 1 - Original Cyber Griffin Objectives and Outcomes
- Appendix 2 - Cyber Security Landscape
- Appendix 3 - Project Griffin - The Predecessor to Cyber Griffin
- Appendix 4 - Cyber Griffin
- Appendix 5 - Cyber Griffin Developmental Projects
- Appendix 6 - 2021 KPMG Report, 'Cyber Griffin Evaluation for the City of London Corporation' (non-public)

Background Papers

- Cyber Strategy and Cyber Griffin Proposal 2018

Charlie Morrison
Police Sergeant, Cyber Crime Unit
City of London Police
T: +44 (0) 7803 305 436
E: charlie.morrison@cityoflondon.police.uk

Helen Thurtle
Analyst, Cyber Crime Unit
City of London Police
T: +44 (0) 7849 208 638
E: helen.thurtle@cityoflondon.police.uk

This page is intentionally left blank

Appendix 1: Original Cyber Griffin Objectives and Outcomes

Objective - Cyber Griffin will offer the following key services for free to businesses in the Square Mile:

- Baseline Briefing: monthly open attendance briefings designed to build defender skills in key areas.
- Base Line Incident Response: including table-top exercises developed by Bristol, in which cyber security decision making is evaluated and red flag exercises which examine readiness in real time response conditions and teach key police decision making skills.
- Cyber Advisory Group: an assembly of senior professionals in cyber security, which meets regularly to advise third parties on best practice and appraise of new approaches to cyber-threats.

Outcome – From its inception, Cyber Griffin has delivered 232 Baseline Briefings. The original objective was to conduct one public briefing a month; Cyber Griffin now conducts, at minimum, biweekly public briefings. Additionally, this service is also NCSC accredited as are the officers delivering it. This exceeds the initial objective.

Outcome - Cyber Griffin has delivered 63 of the Bristol developed Table Top exercises to date. In addition, Cyber Griffin further developed this exercise into a CoLP variant and won a SANS award for innovation in 2019 for this work. This exercise has also received NCSC accreditation. These results exceed the initial objective.

Outcome - The programme investigated creating a Cyber Advisory Group. It was established over the period of the pilot that this group was not able to offer the value anticipated in the programme's initial objectives. In consultation with the Cyber Security Steering Group, the programme later evolved this service into what is now called the Cyber Capability Assessment. This assessment offers a detailed assessment of an organisation's cyber security maturity level which includes a vulnerability assessment, a comparison of the organisation's maturity gauged against best practice standards as well as a road map for improvement. The initial objective was therefore not met, however, following changes agreed with the Cyber Security Steering Group, this objective was modified and the overall purpose has been met.

Outcome – Beyond the three deliverables detailed in Cyber Griffin's original objectives the programme also developed an Incident Response Training exercise. This is a practical service in which officers teach police command structures and decision making in the context of cyber incident response. This helps to develop improved incident response skills using tried and tested techniques developed in policing. This exceeds the objective set.

Objective - The success of the cyber strategy, for the duration of the pilot program, will be measured by the number of businesses that successfully complete the Cyber Griffin programme. Running at full capacity, for year 1, we could service up to 100

businesses with the Cyber Griffin programme, not including those who simply receive the briefing.

Outcome – From its beginning, Cyber Griffin has engaged with over 460 companies and delivered its core services to over 11,000 people. It was identified upon delivery of the programme that companies preferred to select specific services that reflected their current requirements. Whilst some organisations completed all four services within the Cyber Griffin programme, more commonly organisations chose to focus on training large groups of employees via one service delivered repeatedly. The most commonly chosen services were the Baseline Briefing and the Table Top exercise. This objective was partially met.

Objective - We also want to ensure that we deliver a product of the highest quality, so we will survey those businesses, at the time of completion of the Cyber Griffin programme, and six months after, to measure what difference it has made to their confidence in cyber security. This survey has already been designed and tested.

Outcome – An external review conducted by KPMG assessed all the services offered by Cyber Griffin. Included in this review were interviews with a randomly selected group of clients who were able to independently confirm long lasting security improvements facilitated by the work conducted by Cyber Griffin. In addition to the objective above, this report also evaluated and confirmed Cyber Griffin's value for money and listed further developmental opportunities. The change of measure to an external assessment was a choice made by the Cyber Security Steering Group who decided a different range of metrics should be analysed. For these reasons this objective is deemed to have been met.

Outcome – Further positive developments achieved by Cyber Griffin beyond the objectives set include the following: NCSC accreditation of all officers and three out of four services, a digital delivery platform for all services, customer relationship management platforms headed by a Cyber Griffin website, a national webinar series and a home working video series.

Appendix 2: Cyber Security Landscape

1. It is now a largely agreed point that cyber criminality represents a substantial threat to global centres of business such as the City of London. In 2018, the banking industry incurred the highest cyber crime losses of $18.3 million.[1] Moreover, in the coming decade this threat is set to steadily increase.[2] Commonly sighted reasons include:
   - Cyber criminality is hard to attribute and to prosecute.
   - The bar for criminals entering this field is lowering each year as 'off the shelf' hacking tools become increasingly available.
   - This criminality's lucrative nature has driven criminal groups to refine their exploitation of this vein.
   - Cryptocurrency has facilitated the movement of currency on a global scale, in a manner which is challenging to track, and therefore made it possible for any individual with internet access to engage in cyber criminality.

2. There has been significant growth in cyber criminality in the past year; 80.7% of organisations have been affected by a cyber security attack and for the first year 35.7% of organisations experienced 6 or more successful attacks.[3] Analysis have also calculated that collectively security breaches have increased by 67% since 2014.[4]

3. In tandem with this escalation, developed economies are becoming increasingly reliant on technology. The COVID-19 pandemic in March 2020 also triggered an even greater move to digital dependence. This elicited a clear increase of ransomware and phishing campaigns that focused on the human and network security weaknesses in an organisation.

4. In 2020, 62% of organisations were targeted with high-profile ransomware and phishing campaigns, an increase from 56% and 55% in 2018 and 2017 respectively.[5] Phishing campaigns accounted for 22% of all breaches featuring hacking,[6] which corresponded to 1 phishing email for every 4,200 emails sent.[7]

5. Across the landscape, it is well accepted that attack vectors such as ransomware are, 'a big problem that is getting bigger, and *[there is]* a lack of protection from this type of malware in organizations.'[8]

[1] Accenture Security, 'The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study' [2019]
[2] NCSC and NCA, 'The Cyber Threat to UK Business' [2017]
[3] North America and Europe Asia, '2020 Cyberthreat Defense Report' 58
[4] Accenture Security, 'The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study' [2019]
[5] North America and Europe Asia, '2020 Cyberthreat Defense Report' 58
[6] Andrew J Nathan and Andrew Scobell, '2020 Data Breach Investigations Report' [2020] Verizon
[7] Symantec, 'Threat Landscape Trends – Q1 2020'
[8] Andrew J Nathan and Andrew Scobell, '2020 Data Breach Investigations Report' [2020] Verizon

6. In response to the rise of cyber criminality, business centres have begun to develop area-based programmes of digital protection. Estonia's Cyber Security Vision 2019-2022[9] sets out ambitious plans to develop a 'digitally secure' and 'cyber literate' society following attacks on its capital Tallinn in 2007. Similarly, Singapore Cyber Security Unity Strategy[10] details a series of monitoring and public engagement programmes designed to achieve the same result.

[9] ETH Zürich Center for Security Studies (CSS), 'Estonia's National Cybersecurity and Cyberdefense Posture - Policy and Organizations'
[10] William Martin, 'Singapore Cyber Security Strategy'.

Appendix 3: Project Griffin - The Predecessor to Cyber Griffin

1. In 2004, the City of London Police (CoLP) faced sustained terror threats. The City was a high value target and at that time a terrorist incident would have likely overwhelmed police resources. The situation forced a change in police approach and resulted in the launch of 'Project Griffin' in April 2004. The programme was designed to help the financial sector better self-protect against terror threats.

2. Project Griffin sought to recruit the community to combat the terror threat. CoLP's highly trained Counter Terrorism Security Advisers (CTSAs) educated City workers on counter terrorism measures, trained security staff working in the City to support CoLP critical incident responses and established lines of communication to make the community, CoLP's 'eyes and ears.'

3. Project Griffin's success at developing a community-based protection network resulted in the model being adopted nationally as well as overseas.

4. The National Counter Terrorism Security Office (NaCTSO) also developed a complementary programme, 'Project Argus', which was a multimedia simulation posing questions and dilemmas for participants working in syndicates. Project Argus aimed to raise an organisation's awareness to a terrorist threat and provide practical advice on preventing, handling and recovering from an attack. The programme highlighted the importance of being prepared and having necessary plans in place to help safeguard staff, visitors and assets.

5. The successful implementation of Projects Griffin and Argus relied on the expertise of CTSAs, who are specially trained and tasked by NaCTSO. CTSAs' high level of technical knowledge, enabled them to deliver effective counter terrorism briefings, advice and presentations to participants and to develop innovative new counter terrorism techniques, such as behaviour detection. CTSAs remain the backbone of CoLP's successful counter terrorism projects.

6. CoLP's experience with Project Griffin suggested that a community-based approach would be more effective at promoting cyber resilience within the Square Mile than the current efforts which focused on media campaigns and non-technical briefings to audiences on invitation.

Appendix 4: Cyber Griffin

1. Cyber Griffin is a public facing, vendor-neutral police led programme designed to protect the City of London's community from cyber attack. Like its predecessor (Project Griffin) the central idea behind Cyber Griffin is that our best opportunity to tackle cyber criminality lies in our collective defences to it.

2. The programme comprises a small group of technically trained and National Cyber Security Centre (NCSC) accredited officers' who work with the community and offer four core services (figure 1). These core services are outlined on Cyber Griffin's website[11] and also summarised below:

   - **Baseline Briefings:** Non-technical briefings designed to take audiences through today's most prolific digital threats with the aim of teaching the simplest and most functional defences to each. This service is NCSC accredited.

   - **Table Top Exercise:** An interactive exercise used to explore simulated cyber security choices which mimic progressively complex cyber-attacks with the aim of teaching strategy, managing security and decision making. This service is NCSC accredited.

   - **Incident Response Training:** A practical service in which officers teach police command structures and decision making models in the context of cyber incident response. This helps to develop improved cyber incident responses using tried and tested techniques developed in policing. This service is NCSC accredited.

   - **Cyber Capability Assessment:** A detailed assessment of an organisation's cyber security maturity level which includes a vulnerability assessment, a comparison of the organisation's maturity gauged against best practice standards and a road map for improvement.

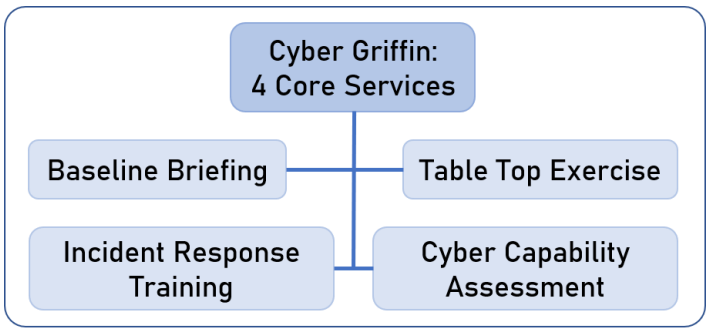

Figure 1: Cyber Griffin's 4 core services

[11] Cyber Griffin, 'Cyber Griffin Website'.

3. In addition to these core deliverables Cyber Griffin have produced a number of other 'peripheral services.' These are bespoke releases in response to a specific development. Two examples include the YouTube home working video series[12] created at the start of the pandemic and the National Police webinar series delivered to support other forces over the same period. The National Police webinar series was also shared *via* YouTube. [13]

4. The programme's current unit comprises one Police Sergeant, five Police/Detective Constable's and one Office Manager. At the time of writing one Police/Detective Constable space is vacant. Figure 2 illustrates the team's current structure (red outline indicating the current vacant position).

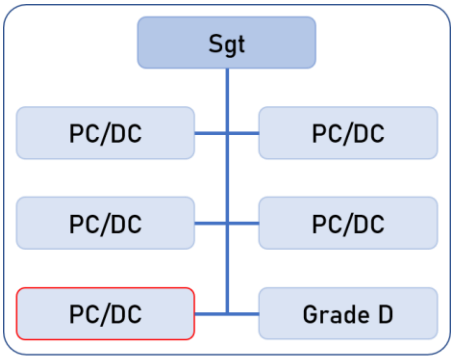

Figure 2: Cyber Griffin structure (as of Feb 2021)

5. Furthermore, as part of its force remit, Cyber Griffin responds to all victim contacts referred to the programme by Action Fraud and through other channels. In this capacity, Cyber Griffin also supports its partner group within the CoLP Cyber Crime Unit, 'the pursue team,' who act as the CoLP's cyber crime investigators. The technical skill sets of the Cyber Griffin officers make them a natural fit for this support role.

[12] Cyber Griffin, 'Cyber Griffin Guides: Home Working' (2020).
[13] Cyber Griffin, 'National Policing Cyber Security Webinars' (2020).

Appendix 5: Cyber Griffin Developmental Projects

A further explanation of the developmental options sighted in point 7 of the proposal:

Cyber Alarm

This is a police led initiative being pioneered as part of Team Cyber UK and designed to keep businesses safe from network level attacks. Cyber Alarm is a software businesses can enable which extracts non-sensitive information from the organisation's firewall and assesses this for digital threats. As more organisations join, Cyber Alarm will grow its ability to detect security risks and inform client organisations. Cyber Alarm has already been successfully piloted in other regions of the country and is continually adding to its core security service to deliver more security benefits. Regional level data storage is now being implemented which allows participating forces to invite and manage organsiations on platforms which the force can manage locally.

Digital Security Coordinators

This is a previously unexplored idea which stems from the current work done by police Security Coordinators (SecCo's). Police SecCo's are trained to assess the security needs and policing requirements of police controlled events. The SecCo's plan informs what police resources will be deployed to the event and the manner in which it will be policed, so as to best maintain safety and security. Should the idea be developed, Digital Security Coordinators (DSecCo's) will support SecCo's by reviewing the digital security of policed events.

Intelligence led Cyber Griffin Services

Currently Cyber Griffin prioritises victims of crime. Beyond this, the programme is made available to the wider public in the Square Mile. Each service is updated based on the latest intelligence however the services themselves are not targeted to groups specifically identified as being at greater risk. Over the next period, Cyber Griffin officers could investigate building this function into the delivery for the programme's core services. The aim would be to maximise impact by delivering services where they are most needed. It should be noted that greater officer resilience would be required to achieve this approach.

Bristol Response Exercise

Throughout the pilot programme, Cyber Griffin have been working with Bristol University to create a new, research based, Incident Response Exercise aimed to directly support cyber incident responders in the financial sector. This exercise is due to be completed in 2021 and will be incorporated into the key services that Cyber Griffin offers. It is of note, that responder skills are one of the strongest aspects policing can deliver to the private sector, it is therefore important that policing develops their offerings within this field as here specifically lies CoLP's opportunity to be world leading.

Committee: Economic and Cyber Crime Committee – For information	**Dated:** 05/05/2021
Subject: Economic Crime Academy Update	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1,10, 12
Does this proposal require extra revenue and/or capital spending?	**N**
If so, how much?	**NA**
What is the source of Funding?	**NA**
Has this Funding Source been agreed with the Chamberlain's Department?	**NA**
Report of: T/Commander Clinton Blackburn	**For Information**
Report author: Christopher Felton	

SUMMARY

Despite the impact of Covid-19 the Academy has continued to deliver training maximising the use of online platforms. Course numbers and delegates have now returned to pre-covid levels.

The Academy is actively developing new courses covering cyber crime and fraud prevention.

The Academy revenue was £863,715 representing a loss of £106,743. These surplus costs were met by last year's underspend. The Academy has a balance of £65,257 for 21/22 and an order book of over £600k.

RECOMMENDATIONS

Members are recommended to note the contents of this report.

MAIN REPORT

INTRODUCTION

1. This report provides an update on the Economic Crime Academy.

CURRENT POSITION

Training

2. Numbers of course and delegates trained have now returned to pre COVID levels.

3. Classroom based course are all being delivered virtually. There is no set date for the return to classroom. This has included international training for Ukraine and Iraq.

4. The Illicit Finance budget has provided £200,000 to continue rolling out volume fraud investigation training. 132 police officers will be trained this year. It will also fund a 36 delegate pilot of the new fraud prevention training course developed jointly with Cifas. This will be targeted at local protect officers.

5. Two new online courses will be launched in May: Demystifying Cybercrime and Fraud Risk Assessment in partnership with the Cabinet Office. The Demystifying Cybercrime course will be offered to all COLP officers and staff at no cost.

6. A Crypto Currency course is being developed and Cyber Fraud and replacement training for reporting on Action Fraud are in a scoping phase.

Financial Position

7. Accounts for this financial year 2020/21

Total revenue (after adjustments) of £863,715 comprising:

i. Courses & Seminars (£469,903)
ii. Commission & Royalties (£1,932)
iii. Illicit Finance funded training (£391,880)

Total costs for the year were £970,458

Total loss for the year £106,743
(172k surplus from last year to offset this loss)

Total balance of £65,257

8. For 2021/22, the Academy already has an order book of £607,227.

Future strategy

9. The future strategy for the Academy is being developed as part of the Transform project.

CONCLUSION

10. Despite the impact of Covid-19 the Academy has continued to deliver training maximising the use of online platforms. Course numbers and delegates have now returned to pre-covid levels.

11. The Academy is actively developing new courses covering cyber crime and fraud prevention and has an active order book for the coming financial year.

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