SCOTTISH POLICE AUTHORITY

Agenda Item 3.4

Meeting	**SPA Policing Performance Committee**
Date	**9 December 2021**
Location	**Video Conference**
Title of Paper	**Implementing the Cyber Strategy and Plan**
Presented By	**DCC Malcolm Graham, Crime and Operational Support**
Recommendation to Members	**For Discussion**
Appendix Attached	**No**

PURPOSE

The purpose of this paper is to provide members with an update on progress and direction of travel of the Cyber Strategy Implementation Programme.

This paper will specifically provide a progress report in relation to:

- Agenda item – Cyber Strategy Implementation Plan

Members are invited to discuss the contents of this paper.

1. BACKGROUND

1.1 Police Scotland's Cyber Strategy 2020 '*Keeping People Safe in a Digital World'* was approved by the Scottish Police Authority (SPA) on 30 September 2020.

1.2 An Implementation Plan was subsequently presented to Strategic Leadership Board and SPA in February 2021, following which a small programme team has been established.

1.3 The Cyber Strategy Implementation Programme has been established to enhance the organisations delivery of initiatives aimed at transforming and enhancing Police Scotland's position in relation to the threats presented by cybercrime. It will support the force priorities of tackling priority crime types and organisational objectives contained within other enabling strategies, including the Digital, Data and ICT Strategy (DDICT). It is proposed that it will embed a 4P's approach to dealing with cyber related threats (Pursue, Protect, Prepare and Prevent), in line with the NPCC led 'Team Cyber UK' methodology.

1.4 The programme will enable Police Scotland to;

- Focus on an improved victim experience
- Deliver an effective investigative response
- Target local cybercrime prevention messaging
- Work to identify and divert people vulnerable to embarking on cybercrime
- Engage with businesses and organisations to help them develop effective measures to mitigate threats and risks associated with cybercrime and, where appropriate, engage in testing and exercising
- Develop Centres of Excellence and provide guidance to the wider force, helping mainstream cyber skills and knowledge into most areas of policing.

1.5 Cyber enabled and cyber dependent crime has been increasing for a considerable period of time and this has escalated further during the COVID-19 pandemic. This is an area of increasing risk and Police Scotland must ensure that our policing model can respond effectively.

1.6 Police Scotland has made good progress in this space, including the roll out of digital triage capabilities. We have established partnerships across the cyber ecosystem, including being a key

partner in Cyber Scotland Partnership, with a focus on reaching public/private/3rd sector/learning and skills development, promoting cyber security and online safety.

1.7 Police Scotland's critical role during the COVID-19 pandemic has been recognised, most recently in the Programme for Government 2020-21. This sets out a Scottish Government priority to ensure Scotland is safely and securely able to develop smart digital solutions to meet the needs of the immediate and long term economic future. The Scottish Government published its 'A Changing Nation, How Scotland will Thrive in a Digital World' strategy in March 2021 and Police Scotland is a key partner, supporting delivery to the related 'Scottish Public Sector Cyber Resilience Framework'.

2. FURTHER DETAIL ON THE REPORT TOPIC

PROGRESS TO DATE/PROGRAMME BRIEF/BUSINESS CASES

2.1 The Programme Brief was approved by Change Board on 31 August. Two Potential Project Assessments were approved by Demand Management Board (DMB) on 9 September and 14 October, for the 'Training and Capability Project' and 'Critical Issues Project' respectively. This formally stood up the projects and allows progression towards Initial Business Case/Business Justification Case.

2.2 Approved Projects

Critical Issues

Through engagement with a range of business areas a number of critical issues have been identified which require to be resolved prior to the implementation of wider strategic change. Predominately relating to SCD and PPCW capabilities and capacity to deliver effective cyber related prevention and investigations, the project seeks to implement improvements to technology, training, equipment and resources to deliver improvements in the short term, addressing critical issues identified in early engagement whilst strategic solutions are developed. A PPA for this work stream was supported at DMB on 14 October 2021 and work is ongoing to deliver a BJC.

Training and Capability

The project will implement a range of Cyber training from basic to specialist levels, improving the capability and capacity of our

workforce. The project aims to develop and deliver innovative, agile and flexible training to provide officers and staff with the best training available to support improvements in service delivery. Engagement is currently ongoing with National Police Chiefs Council (NPCC) leads to understand their journey so far and to gain knowledge from their lessons learned. A 'Request for Information' (RFI) is also currently being finalised to allow engagement with the market to deepen understanding of available products and assist in formulating the Initial Business Case (IBC).

2.3 Projects and Workstreams

Cyber Technologies

A range of technology to improve capability and capacity in the medium to long term. Providing tools to improve efficiency and capability from the first point of contact to investigation. The introduction of new technology will reduce the need for officers to spend long periods of time accessing disturbing images, importantly improving officer wellbeing and will enable Police Scotland to deal more effectively with the threats presented by cyber dependent and enabled crimes, including those relating to child protection and financial crime.

A PPA for this work stream is finalised and discussions are ongoing in relation to how delivery of Cyber related technologies can be introduced to the organisation as part of proposed changes to the delivery of technology related change.

Cybercrime Harm Prevention

A subgroup has been established, co-chaired by the Cyber Strategy Implementation Programme and PPCW leads, to develop a Cybercrime Harm Prevention Plan in support of the overall strategy. This will involve a Public Health approach to reducing cybercrime and will ensure that partners from a range of sectors can positively influence and support our objectives. A Police Scotland Prevent Strategy has been drafted and will finalised through a series of peer reviews.

Consolidating and Restructure (Building a new model)

This is the final piece of the jigsaw and will include the design and implementation of a future working model to allow Police Scotland to improve our response to preventing and dealing with cybercrime. It will produce proposals for change in terms future workforce

requirements, including staff/officer structures, recruitment routes and means to both improve and future-proof our prevention and response capabilities, alongside improvements in our strategic partnerships and processes.

External Centre of Excellence

A proposal to develop and deliver a Scottish Cyber Co-ordination Centre (SCCC) has been devised in conjunction with Scottish Government and senior representatives from across the public sector within Scotland.

A collaborative approach which would support more effective intelligence sharing, assessment of national cyber threats and risk, testing and exercising and incident response/recovery, significant progress has been made, with support from sectoral leads. A proposal is being presented to the Deputy First Minister in November and it is currently understood that Scottish Government are likely to provide funding and establish a project to support delivery.

It is envisaged that the SCCC would be a Scottish Government led entity and would deliver improvements across the Scottish Public Sector, ensuring that the threats to the provision of services through complex and/or simultaneous cyber-attacks would be minimised. Police Scotland would likely contribute limited resources to support the SCCC and it is envisaged that the entity would complement, rather than replace the functions of the UK-wide National Cyber Security Centre (representatives of which are supportive of the current proposal).

Whilst an initial public sector focus exists, it is recognised that extending the reach of the SCCC into other sectors would realise benefits and may be incorporated into any future model on an incremental basis.

2.4 Professional Services Business Justification Case (BJC)

Substantial progress has been made with the programme team which have been in post since May 2021. However due to the complexities and size of the programme further progress at pace has been limited for a number of reasons including approval and recruitment of sufficient resources to deliver a programme of this size.

Following a number of Executive level discussions considering options to accelerate the Cyber Strategy Programme, it has been agreed to procure the services of a Professional Services organisation with effect from January 2021 to help support and drive change in this strategically important area of policing. A BJC is being finalised in this regard and will be presented through Police Scotland governance by 15th December 2021.

Service Requirement

The successful supplier will be required to;

- Conduct a review of the Strategy (light touch "critical friend" validation of the vision/outcomes/ambition/approach and expand as required)
- Produce a strategic outline business case.
- Finalise the "as is" operational and supporting structures and lead the development of a new target operating model.
- Produce a 5 year Strategic Roadmap with short, medium and long term deliverables and a supporting Implementation Plan with a multi-year costed delivery resource model.
- Support the development of business cases aligned to Police Scotland's Investment Governance Framework e.g. Cyber digital and technology business case.
- Supplement the existing Police Scotland Programme team with Programme/Project management support for the initial development of the OBC, Strategic Roadmap / Implementation Plan and new TOM

2.5 Professional Reference Group

The Strategic Leadership Board (SLB) recently endorsed the establishment of the Professional Reference Group. The group will provide Police Scotland Executive with strategic advice, support and expertise. This group will be chaired by DCC Malcolm Graham and comprise of experts from academia, industry and the UK cyber security and resilience community. The SPA will be represented on the group. It is intended that the inaugural meeting will be in early 2022.

2.6 Resourcing Cyber Strategy and Plan Implementation

The Programme Brief outlines the resource requirements to develop Business Cases and deliver the associated transformational change. Relevant resource bids are being progressed in this regard. A bid will be presented to the ODDG on 26th November.
Under the auspices of the Cyber Capabilities Programme, approval has now been secured to recruit 3 Police Staff members to perform Quality Assurance roles in relation to ISO 17025 accreditation. A further bid for 2 police officer roles is being presented to ODDG on the above date. Recruitment of these resources will allow ISO accreditation related work to progress beyond the initial planning phase.

2.7 Current Tasks

Following approval of Potential Project Assessments work is being progressed developing business cases for Training and Capability and Critical Issues projects. Discovery work continues for the remaining workstreams. In particular design work, through a series of workshops is underway for Cybercrime Harm Prevention.

Work is continuing to develop a Communications Strategy / Plan in support of internal and external communications and engagement. This will incorporate activities to support public messaging to raise awareness of developing capabilities and improve public trust and confidence in Police Scotland's' ability to deal effectively with cybercrime, alongside internal messaging to inform staff and change behaviours regarding organisational security and resilience. This will also be developed in support of the Strategic Engagement Plan which will provide insights into public expectations of policing in a digital age.

Work is also ongoing to develop and enhance a range of partnerships across policing and other sectors, nationally and internationally, in order to ensure that Strategy delivery takes account of learning elsewhere and that policing in Scotland can influence the development of approaches to mitigating cyber threats across the wider landscape.

2.8 Next Steps

- Continue progressing programme resourcing bids
- Develop, and progress through governance remaining PPAs
- Undertake activities to develop and deliver IBC's
- Engage with successful supplier for Professional Services
- Manage Professional Services contract and monitor progress

2.9 Cyber Scotland Partnership

The Cyber Scotland Partnership is a collaboration of key strategic stakeholders, derived from a range of sectors across Scotland. The aim of the partnership is to improve cyber resilience across Scotland through a collective focus on harm prevention and reduction, enhancing incident responses and improving access to cyber skills and opportunities. It operates in support of the Scottish Government '*Strategic Framework for a Cyber Resilient Scotland*', with agencies interacting and delivering associated activities through established strategic and tactical level arrangements.

The partnership is active in promoting methods of improved cyber resilience and harm reduction, including through the monthly publication of awareness raising bulletins, including those of a technical nature. In addition to also publishing a range of online learning and other resources, the partnership also delivers regular skills enhancement sessions and co-ordinates prevention activities as part of the annual CyberScotland Week (next taking place 28 February – 6 March 2022). Police Scotland is an active member of the partnership and is represented by senior leaders from Preventions, Partnership and Community Wellbeing (PPCW) Division.

3. FINANCIAL IMPLICATIONS

3.1 The full financial implications will be researched and understood as part of the business case process.

4. PERSONNEL IMPLICATIONS

4.1 Additional Programme resources are required to deliver next stages. Longer term, organisational change will be proposed in relation to structures required to enhance capabilities to prevent and deal more effectively with cyber dependant and enabled crimes.

5. LEGAL IMPLICATIONS

5.1 There are no legal implications with the report.

6. REPUTATIONAL IMPLICATIONS

6.1 There are reputational implications for Police Scotland if the improved capabilities and capacity are not delivered.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications with the report.

8. COMMUNITY IMPACT

8.1 There are no community impact issues with the report.

9. EQUALITIES IMPLICATIONS

9.1 All relevant documents will be completed in line with the formal investment governance process e.g. at Business Case stage. This will include a full consideration of Rights-based issues within relevant EQHRIA and DPIAs.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications with the report.

RECOMMENDATIONS

Members are invited to discuss the contents of this paper.