SCOTTISH POLICE AUTHORITY

Agenda Item 3.3

Meeting	**SPA Policing Performance Committee**
Date	**1 September 2021**
Location	**Video Conference**
Title of Paper	**Implementing the Cyber Strategy and Plan**
Presented By	**Chief Superintendent Stephen Dolan,**
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.

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 A series of design workshops and stakeholder engagement sessions have been held which have identified a number of early deliverables to resolve current critical issues and projects. A Programme Brief has been created and approved by the Force's Programme Board on 15th July 2021 and Portfolio Management Group on 19th August 2021. This will now be progressed to Change Board (CB). The plan is to create 4 Potential Project Assessments for submission to Demand Management Group in the next two months.

2.2 **Potential Project Assessments (PPAs)**

1. Early Deliverables incorporating the following areas

- **Cybercrime Harm Prevention** - *Remodelling is required to build prevention capabilities to more effectively and proactively engage with communities / businesses / partners / service providers to reduce opportunities for victimisation.*
- **Cybercrime Investigations** - *An assessment of resources together with investment in software and equipment will improve ability and increase capacity.*
- **External Centre of Excellence** - *The creation of a Scottish Public Sector collaboration arrangement would support more effective intelligence sharing, the assessment of cyber threats and risks, testing and exercising and incident response / recovery. Work is ongoing towards the submission of a*

proposal for submission to Scottish Ministers in September 2021.

- **Internet Investigations Unit** – *Resources are required to enhance the capacity of the unit to meet existing and future demand. Process and technology improvements (likely supported by technologies proven elsewhere) would ensure that existing capabilities are able to meet demand and improve public service.*
- **Local Policing** - *The programme will consider how Local Policing delivery can be improved in terms of cybercrime related demand, starting by learning from a recently formed cyber-enabled crime team in Aberdeen.*
- **Public Protection Unit** - *Capability and capacity is under significant pressure and improving processes and technologies will bring efficiencies, improve services to victim and enhance safeguarding.*

2. Training and Capability (Training solutions to support all officers and relevant staff roles, in is envisaged there will be 3 tiers of training from basic response to specialised roles.)

3. Cyber Technologies (solutions to support investigative and preventative approaches, distinct from the ICT led Cyber Security and Assurance Programme)

4. Internal Centre of Excellence (Consolidating the Restructure) – this will propose a change to the Police Scotland operating model to support improvements in cybercrime prevention, response and investigation, working towards building a likely tiered model approach which would develop the organisation as a Centre of Excellence in dealing with cybercrime.

2.4 Professional Reference Group

Discussions are ongoing to support the creation of a group to provide the 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.

2.5 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.

2.6 Current Tasks

Following approval of the Programme Brief work is now being undertaken to finalise Potential Project Assessments (PPAs) for Training and Capability and Cyber Technologies, together with PPA for Early Deliverables for the critical issues outlined above.

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.

2.7 Next Steps

- Progress programme resourcing bids and on-board resources
- Progress Programme Brief through remaining governance
- Complete and progress PPAs
- Undertake activities to develop and deliver IBC's

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 information contained within this report.