Project Completion Report

To be completed by the Implementer and returned to the programme manager by **14th April 2020.** All sections should be completed. The final payment cannot be made until the Project Completion Report has been submitted to and agreed.

Project Title	Bridging the Cyber Skills Gap in Africa: A joint PGI-Meridian Project-Network initiative Working title changed at end of Year 1 to: The Cyber Experts' Fellowship: Bridging the Cyber Skills Gap in Africa: A Commonwealth Cyber Fund Network Initiative		
Countries Covered	Malawi, Zambia, Tanzania, Sierra Leone, Mauritius, Uganda, Ghana, Botswana, South Africa, Nigeria, Rwanda, Kenya – plus ECOWAS, EACO, Africa CERT and NEPAD		
Implementer	Protection Group International		
Planned Start date	April 2017	Actual start date	June 2018*
Planned End date	March 2020	Actual end date	TBC Q2 - Q3 2020**
Explain any variance in start/end dates	*Initial Release of Funds **Subject matter experts' availability and proximity to CHOGM in summer 2020.		

Project Purpose
To create a working network of African cyber security policy experts who can act as a hub for cascading best practice in key cybersecurity challenges across the continent through individual and joint projects. By the end of the project, the network should consist of 10 commonwealth countries[1] with up to 40 total Fellows as representatives and several group and country-specific projects that have been initiated in the course of the project. This purpose was adapted at the end of the first year include support for the Commonwealth Cyber Declaration.
Was the Purpose achieved? If not, give reasons. Please state your sources of information
The key agreed outcomes of the project have been achieved, together with some additional outcomes[2], thus demonstrating the success and value to the participating Commonwealth states as well as the broader international cybersecurity capacity building community. As illustrated in our project Quarterly reports, specifically on the regional and UK hosted workshops over the past three years, the network is composed of a total number of 44 Fellows, representing 12 Commonwealth countries, 2 Africa wide body (Africa CERT and NEPAD) and 2 regional organisations (ECOWAS and EACO)[3], including the new Fellows and experts that were due to join the group for the final workshop in Rwanda on 26-27th March 2020. In the interest of improving diversity and inclusion, we were particularly pleased to have increased female representation by project end. At the London workshop in October 2019, the gender split

[1] Recruitment was restricted to Commonwealth countries at the end of Year One when funding switched to the FCO Commonwealth Cyber Fund

[2] Please refer to Table 6: Projects and Project Areas with Outcomes, in the enclosed Final Impact Report

[3] Please refer to Table 3: in the enclosed Final Impact Report and Fellowship Network Map

was a healthy 50% male, 50% female for the first time and the new Fellows brought a wealth of experience and new ideas to the discussion.

The Fellowship Network itself is the key output of the project, to be referred to as the Africa Cyber Experts Network. At the London workshop it was suggested that the network be thought of as a 'Community of Practice'. The project also looked to deliver a combination of group and individual projects, good practice guides, some case studies and other analysis.

These outputs have already generated Outcomes in terms of changes in policy, legislation and practice in a significant proportion of the member states. For example, data protection in Kenya, the African contribution to the nCSIRT workshop programme, the development of the regional centre in Mauritius and the review of CIIP in a number of member states Cyber Security Strategy reviews. There is now an expert network spanning 12 Commonwealth countries and 4 African organisations, but this network is also closely linked to the CTO, GFCE and G-PEN. Significant mapping of initiatives across the member states that has been utilised by FCO, CTO, Oxford Martin School and Home Office initiatives.

The London workshop concluded with a session looking at donor mapping, engagement and resource identification, which was designed to help Fellows plan for future projects and aid sustainability of those very projects. These skills are key to ensuring the Network, Fellows and their respective national agendas (whether in-country projects or international collaborative ones) are informed by all the tools and capability they need to achieve their goals. It also enabled the network to pursue collaborative projects across the network independently outside of this project cycle.

Also, for the very last Regional Workshop we had a number of registrations for new Fellows to attend in place of the long-standing Fellows (due to their unavailability). This demonstrates that the existing Fellows and participating countries placed high in this Fellowship and the network and were keen to ensure their organisations and countries were represented at the final workshop.

Unfortunately, due to Covid-19 pandemic, we were unable to hold the final workshop in Kigali on the 26th/27th March. Plans for a virtual meeting were also postponed as many of the Fellows are government representatives who have been reassigned to other high priority roles to help deal with the crisis. At the time of writing, the date of the delayed meeting has not been agreed.

Did any external factors contribute to the achievement of the Purpose? Please describe

No, although the COVID-19 global pandemic has had a negative impact as the final workshop of the project due to take place in Kigali, Rwanda 26-27th March 2020 could not go ahead and had to be postponed to the following Quarter or until the situation improves.

Were all the Outcomes delivered as planned, with the planned results? If yes, please note the result. If not, please explain

Outcome Number[4]	**Result** *Achieved / Not achieved*	**R/A/G**
1. Pooling policy initiatives	Achieved: 26 dedicated Expert Discussions on Policy Initiatives and Best Practice[5] covering: • Overviews of Current Projects supported at Global, Commonwealth, EU, and UK levels	

[4] List all milestones as stated on the approved Project Proposal Form

[5] See Final Report and Impact Assessment, Table 4: Workshop Programme - Policy Initiative Overviews and updates and Table Workshop Programme - Specific Policy Initiative Areas

	• Cyber Security Challenge for Small and Medium Sized Enterprises • The Meridian Network and CIIP • Understanding CIIP • Global Prosecutors E-Crime Network • Safety Online • Cyber Skills Equality and Diversity Gap: Life-long learning career paths for Women Cyber Security Professionals • National Cyber Capacity Reviews • Establishing National Cyber Risk Assessment Capability within the Commonwealth • Promoting an inclusive and value-based approach to cyber policymaking • National Cyber Risk Assessment work in Africa • Oxford Cyber Maturity Modelling • The Global Forum on Cyber Expertise (GFCE) • Youth Cyber Skills Development • Girls in ICT • Women in Cyber	
2. Sharing best practice to promote legal and operational frameworks which reduce risk to the UK.	Achieved: 22 Project/Project Areas developed by Fellows and 10 Key areas of best shared as notes with member governments.[6] Key best practice outcomes included: • Members states participated in nCSIRT workshop programme • Kenyan legislation passed and model discussed across member states for data protection • Significant increase in attendance and therefore knowledge of Home Office workshops on national cyber risk assessment capability in member states • Initiatives mapped across member states for Commonwealth cyber awareness project • Member states considering membership of key networks working on child protection • Best practice shared and need agreed on, but not yet disseminated widely enough to influence policy on African Cyber Fundamentals • CIIP Models shared with member governments and some evidence of influence on strategy review, for example in Ghana • Paper shared with member states on Electoral Protection System • Models and curriculum shared with member states and links made into GPEN for law enforcement and judiciary • Network support for development of the ITC regional centre • Best practice shared and need agreed on but not yet disseminated widely enough to influence policy on SME standard setting and incident response	

[6] Final Report and Impact Assessment, Table 6: Projects and Project Areas with Outcomes

3. Training in best practice in key areas	Achieved: 3 Full training programmes delivered. Workshop programme included additional material on training programmes awareness raising and curriculum. Projects developed and areas of best practice shared include multiple training programme ideas and initiatives.	
4. Additional outcome added at Year 2 and 3 – Promote the Commonwealth Cyber Declaration	Partially achieved: All member states are Commonwealth countries, so all workshop and project outputs feed into their respective governments, specific discussion of the declaration featured at Fellowship meetings and the projected programme for the final event focused on preparation for the next CHOGM.	

Please describe any unintended outcomes that were delivered as a result of the project?

By Year 3 we achieved gender balance across the workshops, with increased female representation across the Network, thus further improving the gender diversity and equality within this group.

Were all the Outputs delivered as planned, with the planned results? If yes, please note the result. If not, please explain

Output Number[7]	**Result** *Delivered / Not delivered*	**R/A/G**
1)	**Year 3: Twenty new individuals recruited to join twenty existing Fellows** We were particularly pleased that through the fresh recruitment of Fellows during the 3rd year, gender diversity was improved. The total number of Fellows in the Network is now 44, exceeding the required 40 for the whole three-year project.[8]	

[7] List all the Outputs as stated in the Results Framework

[8] Please refer to Table 3 Results against specific numeric targets in the enclosed Final Impact Report

2)	**Years 2 and 3: Training Programme Theme Three: To be determined by Fellowship** In Year 1 the Fellowship initially covered five African nations at different maturity stages of cyber security capacity: Ghana, Mauritius, Kenya, Nigeria and South Africa. The focus for the initial programme was CIIP, with further training being identified as per the specific requirements of the programme and based on the key priorities and knowledge gaps highlighted by the Fellows[9]. As requested by the Fellows themselves, in addition to providing a training masterclass designed to help identify the component parts of a national Child Online Protection strategy, we also provided a dedicated session on Donor Mapping and Engagement, Project Proposal Writing and Budget Planning, which are all essential skills into translating best practice into national agendas. This key knowledge resource and mentored approach is often missing.[10] With the Fellowship project originally due to conclude in March 2020 (now postponed until a later date), the latter session was designed to help the Fellows sustain their project ideas into the future by providing them advice and guidance as to how they can leverage continued support (both technical and financial) for their objectives both from the network itself as well as from the international community more broadly.	
3)	**Year 3 (building on Year 1 and 2) Completion and second stage of existing project cycles, new projects supported:** After consulting with the Commonwealth Cyber Programme team, it has been agreed that for Year 3 we would focus our efforts not on the number of projects generated and/or implemented just in order to meet the above Output target, but on ensuring the Fellowship achieves a number of successful outcomes and deliverables developed through our lessons learned evaluations from Years 1 and 2. Any projects started would be on best value-for-money and based on the Fellows' countries respective needs, priorities and feasibility. Discussions at the Year 3 London workshop in October 2019 addressed the existing list of submitted proposals from Year 2 and considered a small number of new proposals in Year 3. During the roundtable summaries, a number of key issues were identified which the Fellows wish to continue to pursue: • Protection of CNI/CIIP	

[9] Please refer to Table 7: Details of the CIIP training in the enclosed Final Impact Report

[10] Please refer to Table 7: Child Safety Online and Capacity Building support in the enclosed Final Impact Report

	• Online Child Protection • Raising the cyber security awareness of senior leadership (and building business cases to present to senior leaders/'cyber champions') • Encouraging more women into cyber roles • Increasing capacity/training for law enforcement/forensic staff As per our latest Quarterly Report, a number of Fellows requested a session on Online Child Protection as it was of strong interest and a matter of concern. Peter Davies, Global Ambassador for Get Safe Online, was invited to the London workshop in October 2019 to run a masterclass on Child Online Protection. This session was very well received and as part of an ongoing dialogue, Peter and PGI will assist the Fellows in identifying the component parts of a national strategy, the resources required and identifying areas for action. Some excellent discussions were held on the subject of youth development and cyber skills in schools. Angela Matlapeng, our new Fellow from Botswana, is a strong advocate for this project having recently been honoured for her work in her school in Botswana. Angela has, since, identified a colleague within the legal department who she is working with now on cyber awareness issues, both internally and outside in schools as well putting content up on social media.	
4)	**Year 3 (building on Year 1 and 2) Completion and second stage of group projects, new group projects initiated:** Fellows from five different countries expressed their enthusiasm to explore a dedicated Women in Cyber project, primarily to encourage diversity in the cyber security industry in their respective countries. Secondly, the project would seek to encourage women into the cyber workplace. Angella Tugume from Uganda and Angela Matlapeng from Botswana have volunteered to coordinate this work once the critical issue of dealing with the global Covid-19 pandemic has eased. With regards to other projects evolving from the Fellowship, the project that was proposed on helping develop nCSIRT capability was addressed as part of another FCO and Singapore Cyber Security Agency programme. This saw the successful delivery of three regional workshops and a final plenary session in the UK which a number of our Fellows participated in. The proposed project on Child Online Protection started with a Masterclass at the London workshop in October 2019. The next stage of this is currently being considered by one of the Fellows from Rwanda pending advice and feedback from other Fellows.	

	For the Data Protection and Privacy stream, Juliet Maina, our Fellow from Kenya, provided a presentation in the same October Workshop to highlight the work she has been doing in Kenya on smart data privacy laws and what these should endeavour to achieve. She presented an industry perspective on the subject matter, and the discussions identified a number of areas where Juliet and other Fellows could potentially develop a collaborative project to further Data Protection Regimes across East Africa. Zambia, Botswana and Malawi were particularly interested in Julia's work and they are currently working to develop an implementation plan.[11]	

How did the project represent good Value for Money and how could it have been enhanced?[12]

To understand the extent to which, in terms of quality and effectiveness, this Fellowship programme has delivered, it is necessary to take an overview of the outputs produced by the Fellowship in its first three years. These are summarised in Table 1: Fellowship Outputs in Numbers from the Final Impact Report:

Table 1: Fellowship Outputs in Numbers	
44	Fellows from wider network and those attending the Fellowship meetings
16	12 Countries, 2 Africa wide organisations and 2 Regional Organisations participated
26	Expert Workshops on Policy Initiatives and Best Practice
22	Project/Project Areas developed by Fellows
10	Key areas of best shared as notes with member governments
3	Full training programmes delivered
3	International networks linked to member states
2	Externally funded projects delivered over lifetime of Fellowship
2	Fellow generated papers feed directly into work of FCO Commonwealth Cyber fund projects
1	Project being considered for piloting by Member states

Finally, the main outcome, an experts' network in a position to share and spread best practice has been created and can be sustained into the future, all at levels.

[11] Please refer to Table 1: Fellowship Outputs in Numbers in the enclosed Final Impact Report

[12] Value for Money is defined as securing the best mix of quality and effectiveness for the least outlay over the period of use of the goods or services bought. It is not about minimising up front prices.

What evidence do you have that the benefits of the project will be sustained? Please describe
The main benefit and achievement of this project has been the development of the network itself. We have brought together over 44 African cyber security experts from 12 countries and four regional organisations (AfricaCERT, NEPAD, ECOWAS and EACO). The core of this Fellowship has also been very useful in helping recruit suitable individuals for other FCO sponsored capacity building projects in Africa including the National Cyber Risk Assessment project and the nCSIRT capacity building programme. Outside of the formal correspondence to Fellows in between and in the lead up to meetings, the group have a regular and healthy exchange of news and views on the Fellowship What's App group which demonstrates their interest in maintaining the network. The introduction of a new Women in Cyber sub-group at the last London meeting was a very popular topic and two of the female Fellows have shown they are very keen and motivated to progress this as a formal project. The fact that the group members are in such regular contact about relevant cyber–related news and key achievements on the Whats App group, suggests the network we have developed will continue and grow.

What were the three main lessons identified that could be applicable to running this type of project again?
1. What's App remains the platform of choice for many African cyber experts to keep in touch with each other and the relative informality of the platform seems to make representatives from various countries more willing to engage and share than via official channels. This would not be the possible without the invaluable face to face meetings. The strong and sustained engagement on WhatsApp is only a product of the face to face interactions at the meetings.
2. Undeniable value of Face to Face interaction, both when it came to recruitment of new Fellows and in the workshops themselves as it clearly demonstrated a much more dedicated and focused level of engagement from the Fellows and assisted in developing cross-border communication and collaboration.
3. The wish and ambition of the Fellows to drive tangible outcomes from the discussions and the meetings and the network as a whole is a true testament of the value Fellows associate with networks of this kind. Not only does a network of this nature help with their individual day jobs, it can bring value to national and regional agendas as well as a network of support at international fora.

How has the project considered and addressed gender sensitivity as a result of implementation?[13]
After the second year of the project, it was clear that there was a lack of female representation in the group. This is a common issue to the cyber security industry, and in order to mitigate this under-representation, as part of the recruitment of new Fellows for the final year of the project, a conscious effort was made to identify influential female cyber security experts to join the group. As a result, the final London workshop in October 2019 was attended by as many females as there

[13] Note that all HMG funded projects should consider gender. Not doing so may do harm by reinforcing gender inequality.

were males, and we saw a number of the new female Fellows leading the group discussions and driving the creation of a new Women in Cyber sub-group.

Please describe any negative consequences that resulted, or were avoided, from project activity but that were not anticipated in the project design (Conflict Sensitivity).

There were no negative consequences that were not anticipated in the project design. Fellows who did not fully participate were encouraged to do so. Anyone who was disruptive or disrespectful in sessions was managed out conflict by the facilitators. Only one Fellow was, in the end, asked to not return to the Fellowship for subsequent meetings because of a refusal to engage collaboratively. Other changes in membership were as a result of substitutions by sponsoring institutions or ministries or because people were not available for certain specific dates.

How has the project considered human rights risk throughout the projects life and through its implementation?

There are two distinct dimensions to the relationship between human rights and this project.

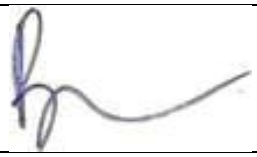
The first is in the implementation of the project itself. The second is in the subject of the discussions and the importance of being sensitive to the human rights dimensions of the topics themselves.

In terms of the former, each meeting was run by highly experienced facilitators who controlled the discussions and develop a largely self-policing ethos which ensured that there was freedom of expression but managed disagreement. The facilitation was sensitive to gender and inclusion balance in terms of discussions and group work. Each day of each meeting of the Fellowship concluded with a real time evaluation to assess the conduct of the sessions and change and adapt if this was needed to ensure better representation and voice for some participants. There was an agreement to leave political differences between states who were members of the Fellowship outside the sessions and this was the case throughout. The disagreements were mainly technical in nature, however there was a divide between some of the officials who favoured a much greater curtailment of human rights online and some others, usually non officials, who opposed this. These discussions were managed with a clear statement of UK government policy in these issues being stated as in support of both the rule of law and a free internet.

This in fact comprises the second dimension: Human Rights as a topic. The need for states to respond to cyber threats poses increasing ethical and legal challenges in terms of national security, human rights and commercial activity. The heart of this challenge is the need to manage the trade-off between public expectations of a right to privacy and the need for state surveillance in cyber space. A state actor with an extremely powerful and intrusive capability does what it needs to defend itself and its people from external threats. It has a responsibility to combat serious and organised crime, stop cyberspace being used for purposes like child exploitation, and to protect people online. The challenge is to fulfil this responsibility to protect while meeting the reasonable expectations of everyone who is using cyber space that they will be able to go about their business safely, freely and in private.

This debate was brought up in expert presentations and in group discussions at virtually all the Fellowship meetings. The state is used to dealing with issues within the confines of a border within which it is sovereign. The internet eliminates that border and the territoriality of the rule of law. States are learning how to cope with the difficulty of identifying what you have let into your country's systems when you imported them and what other states allow on their servers that you would not allow in your own jurisdiction. Different member states were at different stages of

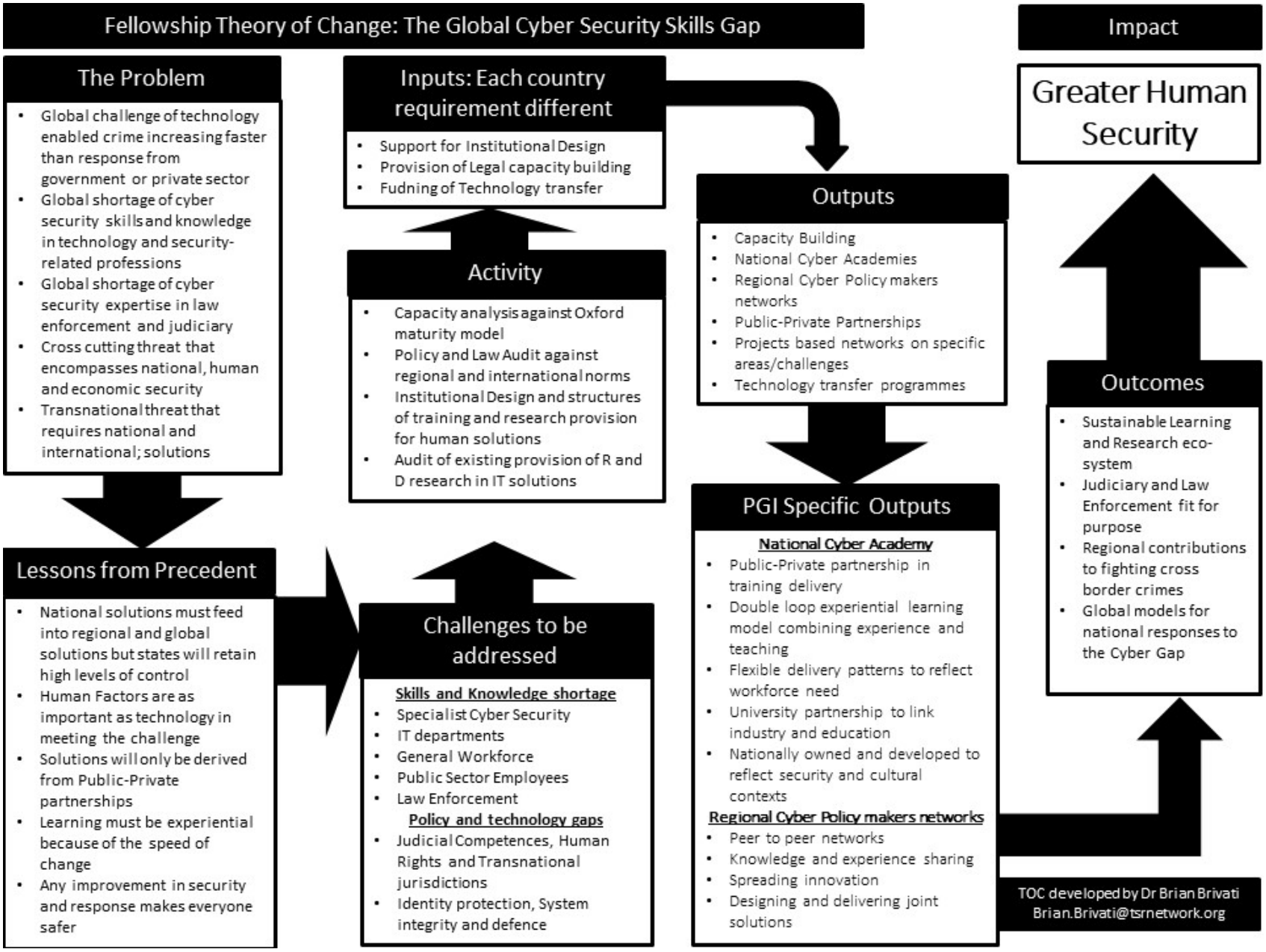
evolution on their thinking about the human rights dimensions of the issues being discussed. All these discussions were managed by the facilitators and reflected in a number of the project areas developed.

Signature	
Name	Brian Brivati
Position	Academic Director PGI Cyber (Consultant)
Date	31 March 2020

Annex 1

Final Report and Impact Assessment

Supporting information


Fellowship Theory of Change: The Global Cyber Security Skills Gap
The Problem
Global challenge of technology enabled crime increasing faster than response from government or private sector
Global shortage of cyber security skills and knowledge in technology and security-related professions
Global shortage of cyber security expertise in law enforcement and judiciary
Cross cutting threat that encompasses national, human and economic security
Transnational threat that requires national and international; solutions
Lessons from Precedent
National solutions must feed into regional and global solutions but states will retain high levels of control
Human Factors are as important as technology in meeting the challenge
Solutions will only be derived from Public-Private partnerships
Learning must be experiential because of the speed of change
Any improvement in security and response makes everyone safer
Inputs: Each country requirement different
Support for Institutional Design
Provision of Legal capacity building
Fudning of Technology transfer
Activity
Capacity analysis against Oxford maturity model
Policy and Law Audit against regional and international norms
Institutional Design and structures of training and research provision for human solutions
Audit of existing provision of R and D research in IT solutions
Challenges to be addressed
Skills and Knowledge shortage
Specialist Cyber Security
IT departments
General Workforce
Public Sector Employees
Law Enforcement
Policy and technology gaps
Judicial Competences, Human Rights and Transnational jurisdictions
Identity protection, System integrity and defence
Outputs
Capacity Building
National Cyber Academies
Regional Cyber Policy makers networks
Public-Private Partnerships
Projects based networks on specific areas/challenges
Technology transfer programmes
PGI Specific Outputs
National Cyber Academy
Public-Private partnership in training delivery
Double loop experiential learning model combining experience and teaching
Flexible delivery patterns to reflect workforce need
University partnership to link industry and education
Nationally owned and developed to reflect security and cultural contexts
Regional Cyber Policy makers networks
Peer to peer networks
Knowledge and experience sharing
Spreading innovation
Designing and delivering joint solutions
Impact
Greater Human Security
Outcomes
Sustainable Learning and Research eco-system
Judiciary and Law Enforcement fit for purpose
Regional contributions to fighting cross border crimes
Global models for national responses to the Cyber Gap
TOC developed by Dr Brian Brivati
Brian.Brivati@tsrnetwork.org

The Fellowship in Numbers

Table 1: Fellowship Outputs in Numbers	
44	Fellows from wider network and those who attended the Fellowship meetings (See Network Map)
16	12 Countries, 2 Africa wide organisation and 2 Regional Organisations participated (See Network Map)
26	Expert Workshops on Policy Initiatives and Best Practice (See Pooling policy initiatives and sharing best practice: the workshop programme – see below)
22	Project/Project Areas developed by Fellows (Pooling policy initiatives and sharing best practice: the projects – see below)
10	Key areas of best shared as notes with member governments - (Pooling policy initiatives and sharing best practice: the projects – see below)
3	Full training programmes delivered – (Training Programmes – see below)
3	International networks linked to member states – (GFCE, Child Protection and GPEN)
2	Externally funded projects delivered over lifetime of Fellowship – (Data Protection and nCSIRT)
2	Fellow generated papers feed directly into work of FCO Commonwealth Cyber fund projects (Cyber Awareness and National Cyber Risk Assessment)
1	Project being considered for piloting by Member states (Cyber Ambassadors)

Overview

In the original application for funding to the FCO Cyber Fund the following output model was proposed and accepted.

Table 2: Outputs from original funding application

Outputs: Model for creation of regional network of Cyber Security Policy Makers in Africa		
Year One: 2017-2018: **First Cycle**: Five countries **Outputs:** • Ten individuals recruited and five governments engaged • Ten individual projects supported • Up to Five Group Projects • Training Programme Theme One: CIIP	**Year Two: 2018-2019** **Second Cycle**: Five founding countries plus five new countries **Outputs:** • Ten new individuals recruited and five new governments engaged • Second stage of ten founding projects and ten new projects supported • Second stage of up to five Group Projects and five new Group projects • Training Programme Theme Two: To be determined by Fellowship	**Year Three: 2019-2020** **Third Cycle:** Five founding countries plus five new countries – fresh recruitment in each **Outputs:** • Twenty new individuals recruited to join twenty existing Fellows • Completion and second stage of existing project cycles, ten new projects supported • Completion and second stage of group projects, new group projects initiated • Training Programme Theme Three: To be determined by Fellowship

At the end of first year the funding switched to the FCO Commonwealth Cyber Fund and the country focus altered, but the overall output model remained the same. In terms of wider outcomes these were specified as:

- Pooling policy initiatives
- Sharing best practice to promote legal and operational frameworks which reduce risk to the UK
- Training in best practice in key areas

The pooling of policy initiatives was developed through a rolling agenda of specific project areas which were presented, developed and discussed, directed to donors for support, and if possible, either directly implemented or incorporated into national strategies (for example in Data Protection in Kenya). Each year of the Fellowship also featured specific training in key areas.

The output targets

The specific output delivery targets were exceeded over the lifetime of the Fellowship.

Table 3: Results against specific numeric targets				
Year	Number of countries		Number of Fellows	
	Target	Actual	Target	Actual
1	5	6*	10	11
2	10	11**	20	23
3	10	16	40	44

Changes:

*Introduction of additional country in Year One at FCO request.

**Introduction of regional groupings including ECOWAS and EACO. Also, two Africa wide organisations AfricaCERT and NEPAD

Details of the Fellows are contained in the enclosed Network Map document. This also includes additional Fellows who attended regional meetings who did not attend London meetings.

The other kind of outcomes were to share best practice and policy initiatives through the meetings programme. In all there were 26 workshops over the course of the Fellowship designed to raise awareness amongst the member states of the Fellowship, the regional organisations and the private sector Fellows. In addition, each Fellowship meeting included Fellows-led workshops at which themes were discussed or project areas developed.

There were 22 specific project areas also developed over the course of the Fellowship with outputs including concept notes, sharing of best practice papers, generation of best practice papers which were shared with other FCO Commonwealth Cyber Fund projects, and projects/policy initiatives developed and pitched to both member state governments and donors.

Pooling policy initiatives and sharing best practice: the workshop programme

In the original programme application, there were a number of different outcomes proposed. The top-level outcome was the creation of the network that would share best practice, share and develop policy initiatives and be given training in specific areas. In terms of the sharing of policy initiatives and best practice over the five physical meetings and the virtual meeting which concluded the programme the following workshops took place. These were discussions lead by a series of external experts and contributions from the Fellows themselves. They were designed to map global initiatives in capacity building, update Fellows on initiatives as they developed and ensure that governments in the network work were fully aware of the opportunities for sharing best practice.

Table 4: Workshop Programme - Policy Initiative Overviews and Updates	
1.	Overview of Current UK Projects supported by FCO Cyber Capacity Fund, Patricia Lewis, Research Director, International Security, The Royal Institute of International Affairs, Chatham House
2.	Commonwealth Cyber Security projects overview, Dr Martin Koyabe, Commonwealth Telecommunications Organisation
3.	UK Cyber Security Initiatives in Africa, Stuart Brown, Head of Cyber Alliances
4.	Global Agenda for Capacity Building for Cyber Security, Robert Collett, Head of Capacity Building, Prosperity, Cyber Crime, Cyber Policy Department
5.	EU Agenda for Capacity Building for Cyber Security in Africa, Nayia Barmpaliou, Policy Coordinator / Programme Manager for Organised Crime and Cyber, European Commission
6.	European Union Cyber Capacity Building, Andrew Dinsley, Head of Programmes, Cyber Security, National Security Directorate, FCO.
7.	Commonwealth Head of Governments Meeting, 2018 CHOGM, Anita Sohan (CTO) and Shadrach Haruna (COMSec)
8.	Digital Access Programme, Thomas Jordan, Manager FCO, FCO's Prosperity Fund
9.	Implementing the Commonwealth Cybersecurity agenda, Joyce Hakmeh, Chatham House
10.	The Commonwealth Cyber Declaration, Christine Timson, Commonwealth Secretariat
11.	Commonwealth Declaration Progress Reports and Working Session on Rwandan's Preparation for next Commonwealth Heads of Government Meeting – Calum Inverarity, Chatham House
Table 5: Workshop Programme - Specific Policy Initiative Areas	
1.	Cyber Security Challenge, Emma Philpott, The Information Assurance for Small and Medium Sized Enterprises Consortium
2.	The Meridian Network and CIIP, Peter Burnett, Meridian
3.	Understanding CIIP, Martin Huddleston, Head of Cyber, APMG International
4.	Global Prosecutors E-Crime Network, Sarah Lennard-Brown and Esther George, International Association of Prosecutors (GPEN)

5.	Safety Online, Peter Davies, Global Ambassador and Eli Peskova, Project Manager, Get Safe Online
6.	DCMS Cyber Skills Immediate Impact Fund Project: The Cyber Skills Equality and Diversity Gap: Life-long learning career paths for Women Cyber Security Professionals, Michael Keen, PGI
7.	National Cyber Capacity Review, Sandra Sargent, World Bank
8.	Establishing National Cyber Risk Assessment Capability within the Commonwealth, Jerry Ketteringham and Rebecca Seward, Home Office
9.	Promoting an inclusive and value-based approach to cyber policymaking in the Commonwealth, Global Partners Digital, Daniela Schnidrig and Matthews Shears
10.	National Cyber Risk Assessment work in Africa, Commonwealth Cyber Fund, Andrew Cameron, Home Office ICDT
11.	Cyber Maturity Modelling, Carolin Weisser-Harris, Lead International Operations at the Global Cyber Security Capacity Centre, Oxford
12.	The Global Forum on Cyber Expertise (GFCE) – working with partners to help international cyber capacity building – Robert Collett, UK FCO and Senior GFCE Liaison
13.	Youth Cyber Skills Development, Presentation on UK response including Cyber Schools Hub and the Cyber First initiatives, Cian Galvin and Measha Patel, The Department for Digital, Culture, Media & Sport
14.	Case Study: Girls in ICT – A Tanzanian Initiative (Darius Luhaga, Tanzanian Communications Regulatory Authority)
15.	Women in Cyber – A UK Case Study, Brian Brivati, PGI

Pooling policy initiatives and sharing best practice: the projects

Table 6: Projects and Project Areas with Outcomes				
Project Area	**Outputs**			**Outcomes**
	Awareness raising and sharing of best practice	Development of Concept note	Submission of concept note	
CNI Government Co-ordination and Governance Structures for Cyber Security and CIIP and incident response	UK best practice shared African best practice shared	Direct feed into related FCO Commonwealth Fund project	Yes, funded, supported and delivered	Members states participated in nCSIRT workshop programme
Data Protection and Privacy (Submission Target - World Bank Programme)	UK best practice shared African best practice shared	Developed	Yes, funded, supported and delivered	Kenyan legislation passed and model discussed across member states
CNI: Contributions to November Conference CNI Survey, Home Office	Special session arranged with the project	Direct feed into related FCO Commonwealth Fund project	N/A	Significant increase in attendance and therefore knowledge of Home Office workshops in member states
Cyber Awareness best practice report	Special session arranged with follow-up	Direct feed into related FCO Commonwealth Fund project	N/A	Initiatives mapped across member states for Commonwealth awareness project
Cyber Cadets/Ambassadors	UK best practice shared African best practice shared	Developed	Submitted to the government of Nigeria and to government of Rwanda	Pending decisions
Online Child Protection	UK best practice shared African best practice shared	N/A	Member states connected with key networks	Member states considering membership of key networks working on child protection
Lessons Learned papers	African policy initiatives and best practice	Developed	N/A	Agenda item for final meeting
Women Mapping of initiatives of inclusivity for women and	UK best practice shared African best practice shared	DCMS Model for promoting women in	N/A	Agenda item for final meeting

young people across the Fellowship countries		Cyber Security shared		
African Cyber Fundamentals - SMME	UK best practice shared African best practice shared	Developed	Not to date	Best practice shared and need identified agreed on but not yet disseminated widely enough to influence policy
Awareness across executive leadership (and building business cases to present to senior leaders/'cyber champions')	UK best practice shared African best practice shared	Models shared across governments	N/A	Learning outcome achieved within Fellowship but not more widely
CNI Dissemination of CIIP models	UK best practice shared African best practice shared	Models shared across governments	N/A	Models shared with member governments and some evidence of influence on strategy review progress for example in Ghana
Electoral Protection Processes	UK best practice shared African best practice shared	Developed	Shared with existing Commonwealth project in this area	Paper shared with member states
Law Enforcement Increasing capacity/training for law enforcement/forensic staff	UK best practice shared African best practice shared	Models for police and judicial training disseminated	N/A	Models and curriculum shared with member states and links made into GPEN
Regional Capacity Building Centre	UK best practice shared African best practice shared	N/A	Member states made aware of the centre	Network support for development of the ITC regional centre
Skills and Knowledge Disseminating models for core skills and knowledge frameworks	UK best practice shared	Models for promoting women, Neuro diverse and BAME Cyber Security	Member states have access model and curriculum	Agenda item for final meeting
SMEs - Cyber Securing African SMEs - Standard setting and incident response And ability to recover quickly from a cyber-attack.	UK best practice shared African best practice shared	Developed	Not to date	Best practice shared and need identified agreed on but not yet disseminated widely enough to influence policy

Budapest Convention and the African Convention on Cyber Security and Personal Data Protections	Policy initiatives shared	N/A	N/A	Learning outcome achieved within Fellowship but not more widely
Clearing House Fellowship to create an information clearing house online that links to existing resources	Policy initiatives shared	Not developed	N/A	Learning outcome achieved within Fellowship but not more widely
Cyber Awareness Project – central web site for Africa	UK best practice shared African best practice shared	Work started by not completed	Not to date	Learning outcome achieved within Fellowship but not more widely
DNS filtering and blocking	African best practice shared	N/A	N/A	Fellows decided not something they could influence

Training Programmes: short summaries

Table 7: Details of the CIIP training, the Child Safety online and the Capacity Building support
CIIP
Meridian and PGI carried out a specialist 1-day CIIP Training session which was delivered in Ghana covering introduction to key themes including defining your CI/CNI and CIP as well as extra dimensions of CIIP and took form of group discussions where Fellows used the time and opportunity to identify unique considerations in Africa. Further discussions followed in the second part of the day to determine criticality and dependencies within the region and country specific ones. Additional training element was focusing on how to use National Risk Profiles, involving Stakeholders and Governance.
PGI and Peter Burnett from Meridian continued to work on the CIIP training package that was put together in Year 1 of this project with the intention of sharing it more widely with the Meridian Community at their next meeting in Seoul in October 2018. The package was approved by the Meridian Steering Committee and Peter was due to share with other governments (or their contractors) who are EU or Meridian members.
Child Safety Online
One of the key issues the Fellows wanted to pursue was Child Safety Online so PGI invited a guest speaker Peter Davies - Global Ambassador for Get Safe Online - to the October 2019 Fellowship meeting in London to run a masterclass on Child Online Protection. This session was very well received and, as part of an ongoing dialogue, Peter and PGI will assist the Fellows in identifying the component parts of a national strategy, the resources required and identifying areas for action.
Capacity Building Support
This training was split over the second regional meeting and the third London meeting. At the regional meeting Lara Pace led discussion and workshop on engaging with donors and developing applications for resources. At the London meeting Lara Pace and the FCO Economist Alex Dunbar-Brookes delivered a masterclass to provide the Fellows with information on best practice for donor mapping, engagement and capacity building. With the Fellowship project due to conclude in March 2020, the latter session was designed to help the Fellows sustain their project ideas into the future by providing them advice and guidance as to how they can leverage continued support (both technical and financial) for their objectives.

Network Map

Fellowship Participants

Africa CERT

Marcus Adomey, Operations Manager at AfricaCERT

Botswana

Ronald Keikotlhaile, ICT Policy Analyst, Government of Botswana

Angela Matlapeng, Botswana Communications Regulatory Authority

Michael Kajane, Principal Communications Officer Government of the Ministry of Communication, Science and Technology, Botswana

EACO

Sarah Kabahuma, East African Communications Organisation

Eliane Mukarukundo, Administrative Assistant, East African Communications Organisation

ECOWAS

Folake Oyelola, ICT Program Officer, ECOWAS Commission

Dr Raphael Koffi, Director, Telecommunication & Regulatory Reforms

Ghana

Albert Antwi-Boasiako, National Cyber Security Advisor, Ministry of Communications

Kenneth Adu-Amonfoh, Director of Information Technology, National Communications Authority, Ghana

Philemon Hini, Consultant, e-crime Bureau Ltd, Ghana

Alex Oppong, Manager, e-Crime Bureau Ltd, Ghana

Attendees who attended the CIIP training:

Gilbert Nii Tackie Addy, Bank of Ghana

Joseph Oduro

Kenneth Ferguson-Laing

James Taylor

Marie-Louise Aikins

Joseph Quaye

Eric Allumiah

Taufre Nassiru Mohammad

Kenya

Juliet Maina, Advocacy and Regulatory Manager, GSMA, Kenya

Timothy Were, State Department of ICT and Innovation, Ministry of Information Communications and Technology, Kenya

Malawi

Thokozani Chimbe, Deputy Director Legal (Consumer Affairs) at MACRA

Mauritius

Dr Kaleem Usmani, Head of Mauritius CERT

Manish Lobin, Mauritius, CERT

Vyankoj Mulloo, Manager, Government Online Centre

Jennita Appayya, Mauritius, CERT

NEPAD

Dr Towela Nyirenda-Jere, Principal Programme Officer - NEPAD

Nigeria

Bello Hayatudeen, Managing Partner, One Alliance Nigeria Ltd

George-Maria Tyendezwa, Assistant Director & Head Cybercrime Prosecution Unit, Federal MoJ

Haru Alhassan, Director, New Media and Information Security, NCC, Nigeria

Gwa Mohammed, Assistant Director, Legal and Regulatory Services, NCC

Abubakar Jogu, Principle Manager, New Media and Information Security, NCC

Colonel Bala Fakandu, Office for National Security Adviser

Rwanda

Justin Rugondihene, Director of Emerging Communication Technologies, Department of Cybersecurity and Digital Innovation (RURA)

Roger Cyiza, Rwanda CSIRT/RISA

Ms Kevine BAJENEZA, Founder&CEO, N@tcom IT-Services Ltd.

Mahmoud Mufora*

Sierra Leone

Mariama Yormah, Ministry of Communications

Mr. Abubakarr Barrie*

South Africa

Basie von Solms, Director - Centre for Cyber Security, University of Johannesburg, South Africa and Associate Director: Global Cybersecurity Capacity Centre, University of Oxford

Dr Victor Jaquire, South African Government

Dr Kiru Pillay, WITS University, Johannesburg

Tanzania

Darius Luhaga, Senior ICT Officer, TCRA

Irene Kahwili, Principal ICT Officer, Computer Emergency Response Team, TCRA

Uganda

Arnold Mangeni, Director of Information Security, National IT Authority

Angella Tugume, National IT Authority

Peter Kahiigi, Director of e-Government Services, Uganda/Oxford Associate

Angela Ndagano, Corporate Communications Officer, NITA

Zambia

Chewe Mutale, Cyber Security Specialist, ZICTA

Project Design and Delivery

Professor Brian Brivati, Consultant Academic Director PGI and Programme Facilitator

Lara Pace, Toria Global, Subject Matter Expert/Programme Facilitation

Sebastian Madden, Chief Corporate Development Officer, PGI Cyber

Olly Jones, Senior Cyber Capacity Building Consultant, PGI Cyber

Anna Kolosenko, Project Manager, PGI Cyber

Jacqui Harrod, Training Co-ordinator, PGI Cyber

Tracey Walsh, Training Co-ordinator, PGI Cyber

Experts Speakers and Participants

Alex Dunbar-Brookes, Economist, FCO Cyber & National Security Capabilities Department

Andra Kastelic, Cyber Security Capacity Centre, Martin School, Oxford University

Andrew Cameron, Home Office ICDT

Andrew Dinsley, Head of Programmes – Cyber Security, National Security Directorate, FCO

Anita Sohan, Commonwealth Telecommunications Organisation

Brian Lord, PGI Cyber

Calum Inverarity, Chatham House

Carolin Weisser-Harris, Lead International Operations at the Global Cyber Security Capacity Centre, Oxford

Christine Timson, Commonwealth Secretariat

Cian Galvin, The Department for Digital, Culture, Media & Sport

Claire Levens, Head of Policy, Internet Matters

Daniela Schnidrig, Global Partners Digital

Dr Martin Koyabe, Commonwealth Telecommunications Organisation

Elena Tsalanidis, Commonwealth Secretariat

Eli Peskova, Project Manager, Get Safe Online

Emma Beckles, The Commonwealth Secretariat

Emma Philpott, The Information Assurance for Small and Medium Sized Enterprises Consortium

Esther George, International Association of Prosecutors (GPEN)

Ida Mboob, World Bank

Jerry Ketteringham, Home Office, Establishing National Cyber Risk Assessment Capability within the Commonwealth Project

Joyce Hakmeh, Chatham House

Kaja Ciglic, Government Cybersecurity Policy and Strategy, Microsoft

Khotpotso Mtwazi, FCO Digital Access

Lea Kaspar, Global Partners Digital

Martin Huddleston, Head of Cyber, APMG International

Matthews Shears, Global Partners Digital

Measha Patel, The Department for Digital, Culture, Media & Sport

Michael Potter, FCO Commonwealth Cyber Programme Manager a

Nayia Barmpaliou, Policy Coordinator / Programme Manager for Organised Crime and Cyber, European Commission

Patricia Lewis, Research Director, International Security, Chatham House

Peter Burnett, Meridian

Peter Davies, Global Ambassador for Get Safe Online

Pria Chetty, Endcode, Consultant to FCO Digital Access

Professor Paul Cornish, Independent Consultant and formerly Oxford Martin School

Rebecca Seward, Home Office, Establishing National Cyber Risk Assessment Capability within the Commonwealth Project

Robert Collett, Head of Capacity Building, Prosperity, Cyber Crime, Cyber Policy Department and Senior GFCE Liaison

Robert Oldham, FCO Commonwealth Cyber Programme

Sandra Sargent, World Bank, National Cyber Capacity Review

Sarah French, Marie Collins Foundation

Sarah Lennard-Brown, International Association of Prosecutors (GPEN)

Shadrach Haruna, The Commonwealth Secretariat

Stephanie Perry, Head of Information Assurance, PGI Cyber

Stuart Brown, Head of Cyber Diplomacy (Alliances), UK FCO Cyber Policy Department