UK Government's Global Digital Access Programme (DAP) - Project summaries

Pillar 2: Protecting the most vulnerable from cyber crime

V11 NB 18 Aug 2021

The UK Government's Global Digital Access Programme

4 Aug 2021

Protecting the most vulnerable from cyber threats

Millions of people remain excluded from the digital economy giving rise to a damaging global digital divide. Anything that prevents those excluded from getting online, such as issues around security exacerbates that divide further.

Middle-income countries are keen for their citizens and businesses to harness the potential of digital access to boost economic development. Digital access for their citizens is growing fast but improvements in cybersecurity typically lag far behind. This gap is fertile ground for cybercrime. The harm caused by cybercrime acts as a brake on development. As well as causing direct economic loss, it reduces trust in technology and the internet, particularly among the economically vulnerable.

As ever, the impact of crime is felt most keenly by those who have the least.

Governments are acting to shore up their cyber defences, making their systems and infrastructure more resilient and educating their populations on how to remain cybersecure, but this is a substantial challenge.

During a two year period from October 2020 to September 2022, the FCDO, through its Digital Access Programme (DAP), is implementing 14 projects to improve cyber capability and reduce harm in five countries – Brazil, Kenya, Nigeria, South Africa and Indonesia.

HM Government

UKaid from the British people

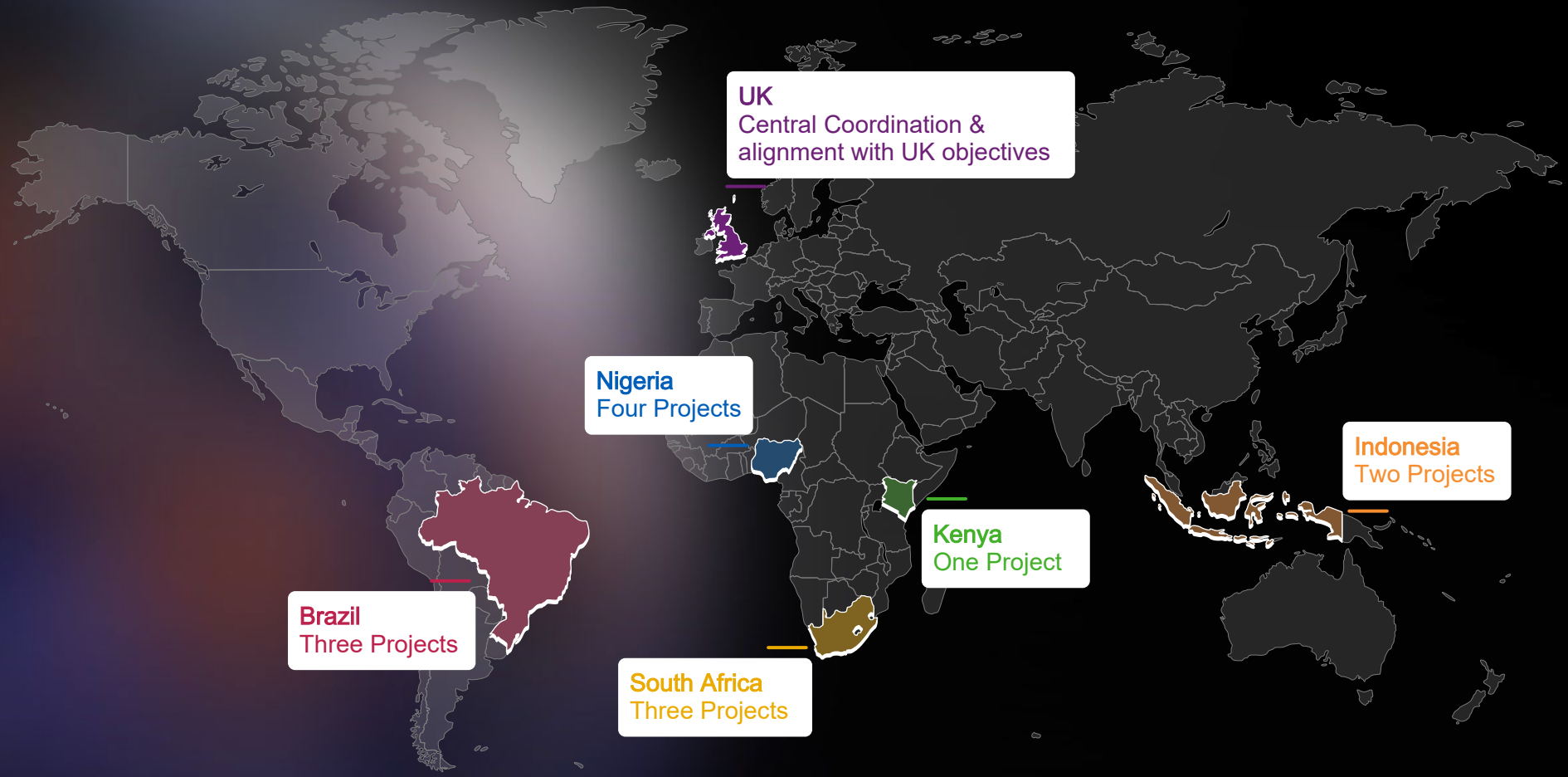
Backed by £10 million of UK aid from the Conflict, Stability and Security Fund, the DAP is the UK government's largest ever overseas cyber capacity building project. These projects will contribute to the UK & FCDO's vision of 'thriving, open digital societies powered by trusted technologies, with the UK leading efforts to uphold a free, open, peaceful and secure cyberspace'.

The 14 projects include helping the Nigerian police force to develop its digital forensic capability; enabling Kenya's government to better protect its citizens' data; assisting the delivery of Brazil's new cybersecurity school curriculum; developing Indonesia's national cybersecurity strategy with a focus on ransomware; and improving the South African police's ability to prosecute cyber criminals and combat online child exploitation.

In each instance, the ambition is to build a sustainable capability that allows national partner governments to better protect their citizens online or to defend their critical national infrastructure from cyber threats.

Ultimately, the DAP will build on the UK's cybersecurity experience to help these countries improve safe digital access, bringing excluded populations into the digital economy, reducing poverty and stimulating inclusive economic growth.

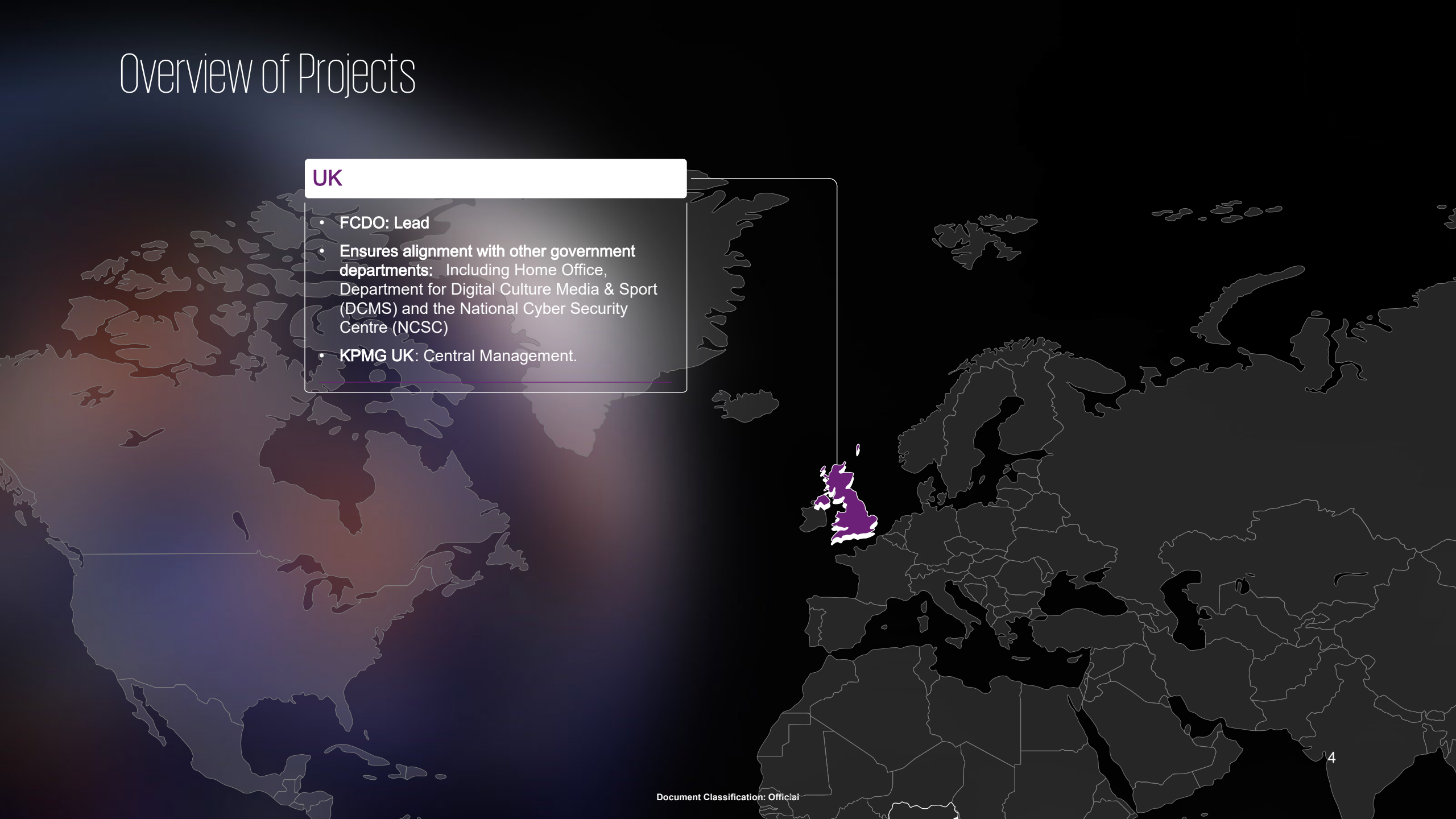
Overview of Projects (To date)



Overview of Projects

UK

- **FCDO: Lead**
- **Ensures alignment with other government departments:** Including Home Office, Department for Digital Culture Media & Sport (DCMS) and the National Cyber Security Centre (NCSC)
- **KPMG UK**: Central Management.



Overview of Projects (To date)

South Africa Projects

- **Cyber Awareness & Skills for Law Enforcement** - Tackling cybercrime and online child sexual abuse
- **Cybersecurity and Data Protection Toolkit for SMEs** - Bolstering cybercrime defences of South African small businesses
- **Training for Incident Response Teams (CSIRTs)** – Improving South Africa's response to national cyber threats

Overview of Projects (To date)

Indonesia Projects

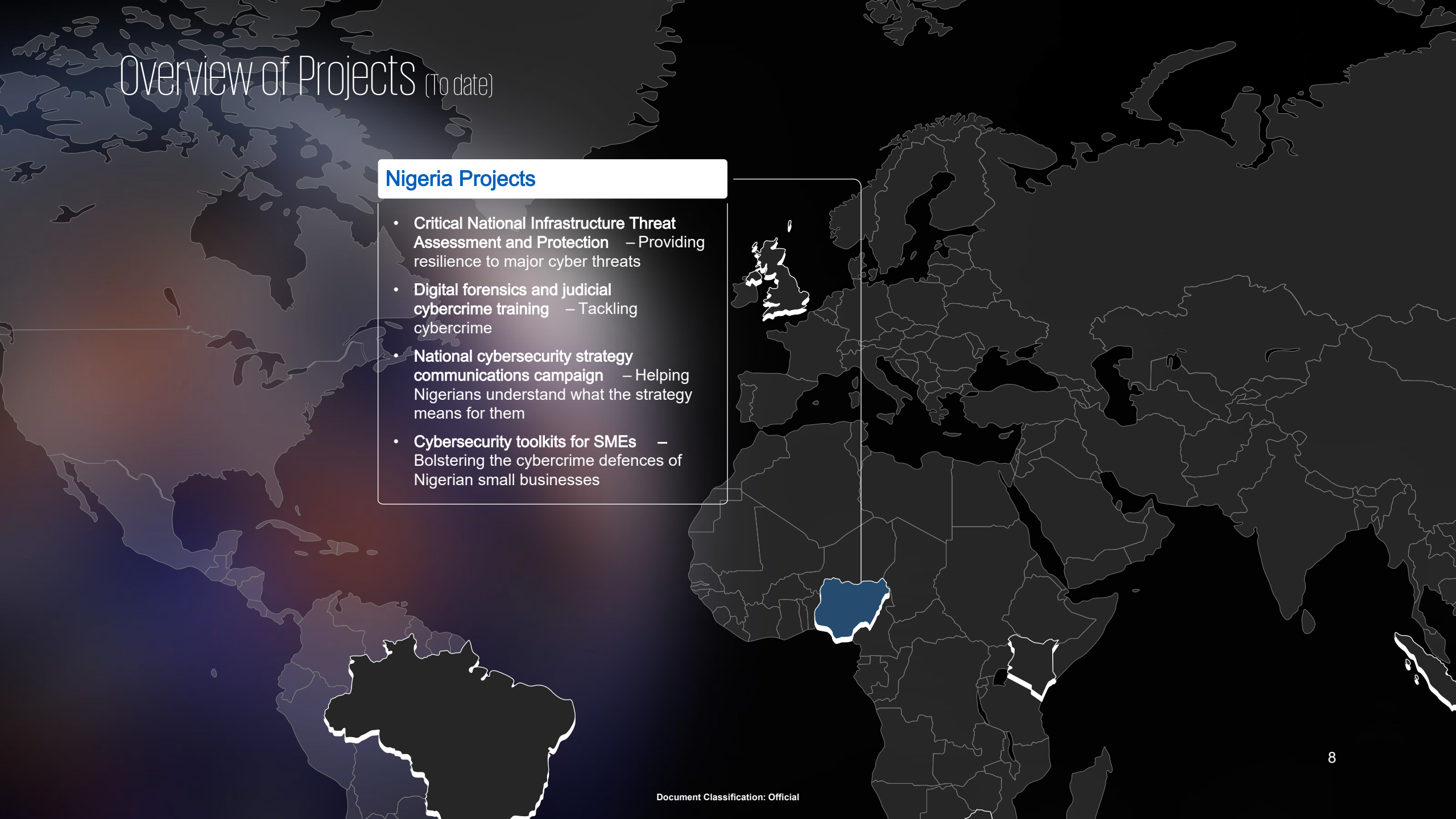
- **Strengthening Telemedicine cybersecurity** – Increasing patient's trust
- **Government Cyber Security Training** – Equipping government to tackle cyber threats

Overview of Projects (To date)

Brazil Projects

- **Securing e -Government services** – ensuring Government e-services are safe from cyber threats.
- **Building Brazil's national cybersecurity curriculum** – Increasing the resilience of teachers and school children to cyber threats
- **Raising awareness of cybersecurity across Brazil** – Increasing Brazilian's resilience

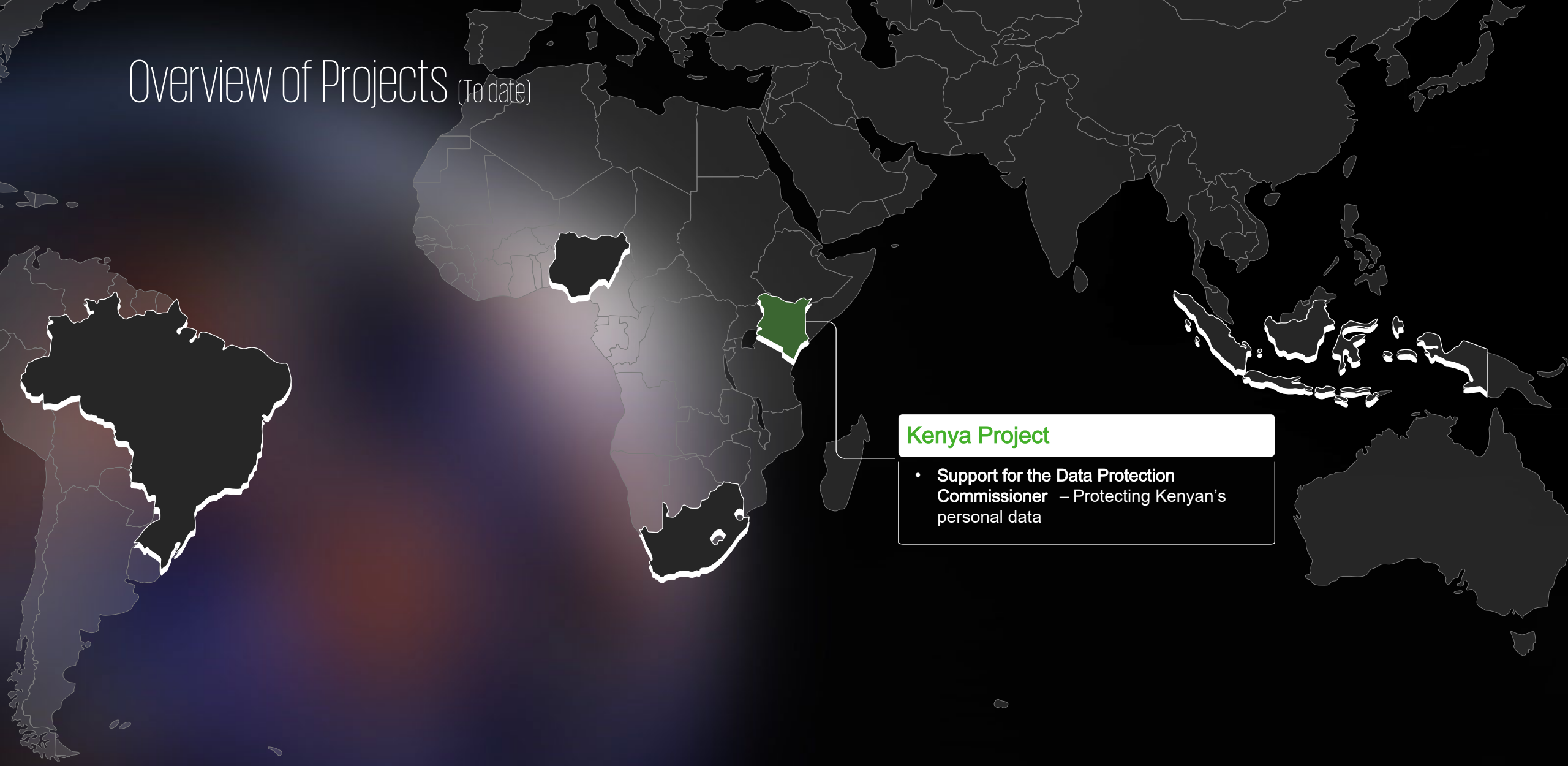
Overview of Projects (To date)



Nigeria Projects

- **Critical National Infrastructure Threat Assessment and Protection** – Providing resilience to major cyber threats
- **Digital forensics and judicial cybercrime training** – Tackling cybercrime
- **National cybersecurity strategy communications campaign** – Helping Nigerians understand what the strategy means for them
- **Cybersecurity toolkits for SMEs** – Bolstering the cybercrime defences of Nigerian small businesses

Overview of Projects (To date)



Kenya Project

- **Support for the Data Protection Commissioner** – Protecting Kenyan's personal data

South Africa

Cybercrime Awareness & Skills For Law Enforcement

Why are we delivering this work?

The South Africa Cybercrimes Bill is a priority for government. It is awaiting presidential assent. The bill is intended to act as a deterrent to cyber criminals.

The South Africa Police Service (SAPS) is empowered to act against cybercrime. However, its lack of digital forensics training and defined processes to report and manage incidents is causing short-term challenges, particularly when it comes to investigating cybercrime and bringing criminals to justice.

Greater access to online media also allows paedophiles and other online abusers to contact and exploit children and cause harm through the distribution of indecent images, fraud, and child sexual exploitation.

This is compounded by the lack of requisite infrastructure, training, and funding for SAPS to receive and process referrals from the National Centre for Missing and Exploited Children to create effective investigations into cases of online child sexual abuse and exploitation, and help to protect these vulnerable children.

At the same time, the number of case referrals from overseas intelligence and law enforcement agencies is growing. Many do not get investigated, leaving vulnerable groups at heightened risk, and criminals in the clear.

SA1

Tackling cybercrime and online child sexual abuse

Who are we working with?

- Police, including its Directorate for Priority Crime Investigation (DPCI) and Serial and Electronic Crimes Unit (SECI)
- The National Prosecution Authority (NPA) and other key agencies which are tasked with implementing the Cybercrimes Act
- Key delivery partner is CYSIAM, a UK supplier specialised in digital forensics training.

What is being delivered?

- Two-day workshop jointly led by local think tank, to explore the scope of South Africa's Cybercrimes Act and the implementation challenges
- Digital Evidence Training Policy, Digital Evidence Training Framework and Standard Operating Procedures (SOPs)
- Specialist and baseline digital forensics training to enable detection, prevention and investigation of cybercrimes
- A pilot awareness campaign aimed at a segmented audience, i.e. women and children, to help protect against cybercrime.
- Training and equipment provided to the SECI unit to process NCMEC referrals.

Cybersecurity and Data Protection Toolkits for SMEs

Why are we delivering this work?

Small and medium sized businesses play a crucial role in the South African economy. They account for 98% of South African businesses, employ 50 - 60% of the total workforce and contribute 39% of GDP.

Many use cyberspace to promote their business and conduct business transactions. This has increased rapidly as a result of the pandemic. Lack of training and cyber security awareness makes these businesses easy targets for phishing and ransomware attacks which often result in economic losses, unemployment, and possible supply chain risks. Almost 40% of small and medium sized businesses are owned by women, many of whom have also experienced abuse, harassment and hate crimes as a result of moving their businesses online.

At the same time, the recently introduced Protection of Personal Information (PPI) Act requires all businesses to comply with new information handling regulations, with violations that could cost businesses up to R10 million.

Given this, the **South African government** wants to provide much -needed cyber security and data privacy guidance to support the small and medium sized business community, especially in rural and excluded populations, to increase their resilience to cyber harms.

SA4

Bolstering cybercrime defences of South African small businesses

Who are we working with?

- The Cybersecurity Hub and National Computer Security Incident Response Team (CSIRT) from the Department of Telecommunications and Postal Services
- Information Regulator SA – Department of Justice
- WomHub , a boutique pan-African incubator for female founders in STEM. They will support local delivery.

What is being delivered?

- Cybersecurity and data protection toolkits and basic cyber hygiene training for small and medium sized businesses in South Africa, aligned to the UK Cyber Essentials scheme and international good practices, underpinned by regulation and incentives
- A series of workshops to disseminate toolkits through a Train -the-Trainer approach and supported by a communications strategy.

Training for Incident Response Teams (CSIRTs)

Why are we delivering this work?

South Africa is in the process of bolstering its national cyber incident response capacity. It has two government **CSIRTs**, approximately six industry sector equivalents, and a series of draft protocols that shape its response to major cyber incidents. However, these protocols are not yet live.

Allianz Global Corporate & Speciality, a global corporate insurer, has published its Business Risk Barometer 2021. For South African companies, business interruption, pandemic outbreak and cyber incidents are the top three business risks for 2021 – all strongly interlinked.

Without well understood and well -rehearsed incident response plans, cyber incidents can cause substantial impact carrying longer lasting harms. Typically, vulnerable groups are worst affected and have few or no alternative solutions while the incident plays out.

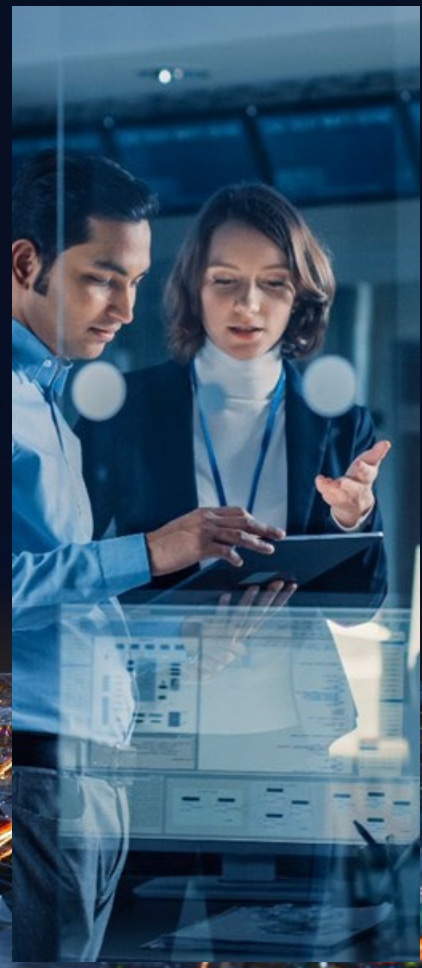
This project will help address this by providing skills and resources to efficiently resolve major cyber incidents in a coordinated fashion across **South Africa's CSIRT groups** .

The CSIRTs will be offered incident response playbooks alongside enhanced incident response training and exercising.

This will strengthen the relationships between the two CSIRT groups and result in more effective exchange of information, data and insights, and ultimately a more coordinated response to any incident or emerging threat – for the benefit of **South African citizens and businesses** alike.

SA10

Improving South Africa's response to national cyber threats



Who are we working with?

- The Cybersecurity Hub and National CSIRT from the Department of Telecommunications and Postal Services
- Volunteer Sector CSIRTs including SABRIC and ISPA
- CYSIAM, a UK CREST registered and accredited Critical Security Incident Response Company

What is being delivered?

- Improved incident response playbooks, protocols and crisis communication channels
- Cyber incident response training to South African CSIRTs
- Three customised incident response playbooks covering prevalent threats and TTPs (Tactics, techniques and procedures)
- Scenario-based incident response exercising for each government CSIRTs, including post-exercise reports and a recommendations roadmap

UKaid
from the British people

Indonesia

Strengthening Telemedicine cybersecurity

Why are we delivering this work?

Indonesia has the world's fourth largest population (over 270 million), nearly half dispersed across some 17,000 islands, making physical access to healthcare challenging. It has therefore been interested in telemedicine for some time.

Given the challenge for these rural and vulnerable communities in particular, the Indonesian government has been encouraging the use of telemedicine for online consultations and treatments. Over the last year, the use of telemedicine apps doubled.

COVID-19 accelerated this growth as the Indonesian health system came under pressure. But as demand for telemedicine services grew, now serving millions of patients, so did the urgency for making telemedicine platforms secure.

Without effective cybersecurity, huge amounts of confidential patient data could be compromised, and remotely operated medical devices exploited.

Our work aims to improve the cyber defences of telemedicine platforms and so reassure Indonesians that their data is secure. This should help increase healthcare coverage in rural areas and lessen the strain on existing healthcare facilities.

IN5

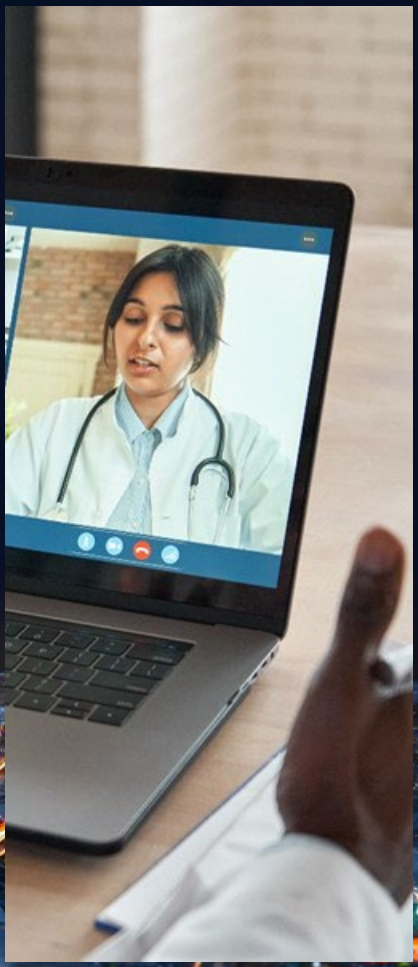
Increasing patients' trust

Who are we working with?

Multiple Indonesian government stakeholders including the Ministry of Health, the National Cyber and Cryptography Agency, the Ministry of Communication and Information Technology and the Health Social Security Agency.

What is being delivered?

- A security framework for telemedicine platforms and services taking into account key legislative arrangements
- A Privacy Impact Assessment (PIA) methodology for electronic medical records and telemedicine patient data
- A multi-agency and ministry incident response exercise programme to raise awareness across agencies, and to develop governance and procedures for cyber incident response across telemedicine providers



Government Cyber security training

Why are we delivering this work?

In 2019, Indonesia had the largest and fastest growing online population of all ASEAN nations, with almost 170 million citizens accessing the internet through their mobile device. By 2025, an additional 80 million Indonesians are expected to be online for the first time.

With such a huge online population, the fall-out from a significant data breach at a major national institution such as telemedicine could be substantial. Added to this, progress on the development of effective cybersecurity policies and frameworks for Critical National Infrastructure (CNI) operators has not kept pace, in part because of the number of ministries involved in their development. The **National Cyber and Cryptography Agency** are now taking the lead and are setting up the **National Critical Infrastructure (CI) Group** .

This National CI Group will consolidate government efforts to protect Indonesian CNI. This project will deliver cybersecurity training and skills to the ministries and government officials that will form this Group.

This will lead to more effective cybersecurity practices among CNI operators, increased resilience of their services, and sensitive data managed more securely.

IN9

Equipping government to tackle cyber threats

Who are we working with?

- 200 people from nine Critical National Infrastructure (CNI) Ministries ((BSSN State Cyber and Code Agency, Ministry of Energy and Mineral Resources, Ministry of Transportation, Bank of Indonesia and Financial Services Authority, Ministry of Industry, Ministry of Communication and Information, Ministry of Defence, Ministry of Health, Ministry of Agriculture)
- The National Cyber and Cryptography Agency (BSSN)

What is being delivered?

Information Security Training

- Three day Cyber Practitioner Course delivered by Chatham House to 200 participants from nine CNI Ministries
- One day ISO training course covering the international information security standard ISO27001
- ISO27001:2013 training and certification for 24 BSSN government officials

Government Security Skills Framework

- A framework that identifies cyber security roles (and role families) and associated levels of competencies e.g. foundation, awareness, practical and expert. The framework will describe each role, with a definition of expected skills and proficiency levels.

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Brazil

Raising awareness of cybersecurity across Brazil

Why are we delivering this work?

Across the country, online sexual exploitation, discrimination, cyber bullying and abuses of personal data are rising rapidly. Many cyber harms particularly affect vulnerable members of society, including women, young people, under-represented minority groups and the elderly.

When Brazil launched its first ever national cybersecurity strategy E-Cyber, it recognised Brazilians are not as aware as they need to be of cyber threats and how they can avoid them. To help address this, an important objective of the strategy is " *to carry out actions to raise public awareness*"

The Brazilian government is now preparing to run a host of national campaigns, designed to improve awareness of the importance of being cybersecure, and to provide citizens with basic cyber hygiene guidance.

This project aims to improve the government's in-house capability for designing and executing such campaigns. Once suitably equipped, the Brazilian government agency responsible for E-Cyber, GSI-PR, will have the capability to run future national campaigns, as government looks to steadily improve Brazil's cyber maturity.

BR1

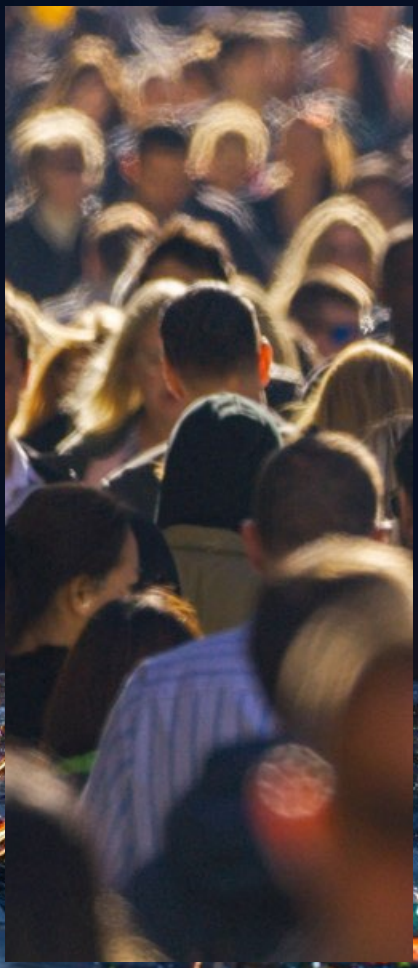
Increasing Brazilians' resilience to online threats

Who are we working with?

- Institutional Security Cabinet of the President of the Republic (GSI-PR)
- GSI-PR Social Communication Office GSI-ASSESSORIA DE COMUNICAÇÃO
- Tonica - Local Brazilian communications agency
- KPMG Brazil

What is being delivered?

- Review of existing models, methodologies and materials for awareness campaign execution, including knowledge sharing activities and review of lessons learned
- A framework and a strategic action plan for executing awareness campaigns using existing models and tailoring these to the requirements and needs of GSI-PR
- Materials for awareness campaigns
- Engagement with potential co-funders and interested parties to establish a forum of organisations with an interest in increasing cyber security awareness in Brazil



Securing e-Government services

Why are we delivering this work?

Brazil is digitising its government services to reduce bureaucracy and provide its citizens with more efficient access to public services. It is a huge undertaking, involving more than 250 government departments and thousands of apps, webpages and online processes.

Government e-services must be secure. The country has already been exposed to damaging and high profile data breaches. E-Government services must also be aligned with Brazil's new data protection act, the LGPD.

Such a wholescale shift to online services provides a risk that citizens will be exposed to more cyber harms, unless security and privacy concerns are comprehensively addressed during the design of these services.

Everything from access controls and encryption through to governance and privacy regulation must be addressed at the outset. This is referred to as Secure by Design. Not only will this heightened focus on security and privacy help to reassure citizens about their personal data, it will also safeguard the integrity and availability of these services. Secure, efficient and trusted services provide particular value to the many Brazilians living in remote, rural communities that have limited physical access to public services.

BR3

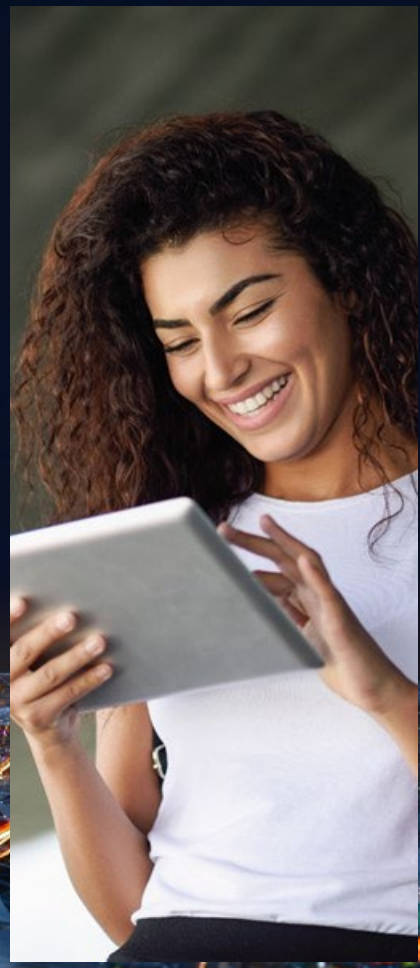
Ensuring Government e -services are safer from cyber threats

Who are we working with?

- Brazil's Ministry of Economy – Special Secretariat of De-bureaucratisation, Management, and Digital Government (SGD)
- KPMG Brazil who will be the main implementer

What is being delivered?

- An assessment of the maturity of the Ministry of Economy's current approach to Security by Design and identification of where improvements may be required
- Security by Design framework for Ministry of Economy to use in its digitisation programme and more widely where desired
- E-Government services created with Security by Design procedures



Building Brazil's national cybersecurity curriculum

Why are we delivering this work?

As in every country, young children in Brazil are exposed to a number of cyber harms, from phishing to online grooming and sexual exploitation. By improving their cyber awareness while at school, the Brazilian government is empowering children to securely navigate cyberspace by teaching them how to recognise the risks, and learn how to avoid them.

There is no shortage of content available in this area. However, there is a need to bring greater consistency to the way digital skills are taught in Brazilian schools. The challenge is to curate a high quality toolkit, drawing on existing materials from across the public, private and third sectors; and help teachers to deliver the curriculum across the country.

The federal government, through the Ministry of Education, is fully behind this project. This will mean the good work already achieved at state level can be built upon by encouraging many more organisations to become involved.

With federal and state governments working hand-in-hand, cyber security education will be delivered across Brazilian schools in a more effective, consistent and sustainable manner.

BR7/9

Increasing teacher's and school children's resilience to cyber threats

Who are we working with?

- Brazil's Ministry of Education and partner State Secretariats for Education
- Brazilian NGO SaferNet, which focus on the struggle against crimes and violations of human rights on the internet and KPMG Brazil

What is being delivered?

- Research to identify existing materials for teacher training. This will be compared against the Basic National Curriculum requirements. It will also be tested against the set of needs and harms identified in the initial research phase. Together this will inform the digital toolkit design
- Report providing teacher and pupil experiences and insights into online harms
- Knowledge sharing workshops to collate relevant toolkit and training materials
- Beta version of toolkits; gathering and applying feedback from a selection of schools
- Long term implementation plan

Nigeria

Critical National Infrastructure Threat Assessment and Protection

Why are we delivering this work?

When critical national infrastructure (CNI) fails, the impact of losing services such as electricity or clean water, no matter how temporarily, can be devastating – particularly for vulnerable groups.

Previously, Nigeria lacked a central regulator, so had no single consistent approach to regulating its CNI. There was incomplete knowledge of what constituted CNI, plus incomplete knowledge of the cyber threats posed and how to mitigate them.

To tackle this, as part of its new cybersecurity and policy strategy, Nigeria's Office of the National Security Adviser (ONSA) is developing a framework for identifying its CNI, assessing the key threats posed to it, and establishing measures that can be taken to provide protection from cyberattacks.

Secure CNI is a critical part of a cyber resilient society. A reduction in the likelihood of a significant cyber incident disrupting critical services will particularly protect vulnerable groups from harm. Improved national resilience will also lead to enhanced prospects for international trade, overseas investment and improved economic development.

NG1

Providing resilience to major cyber threats

Who are we working with?

- Nigeria's Office of the National Security Advisor (ONSA)
- KPMG Nigeria
- Nigerian CNI providers
- Nigerian SMEs
- Home Office
- Chatham House and Cysiam

What is being delivered?

- Assessment of current Nigerian CNI regulation, providing a review of how CNI is regulated
- International Good Practice Report on CNI regulation, taking account of different approaches and geographies such as UK, Europe, US, and Asia
- Threat Analysis Report – analysing the sector specific threats on Nigeria
- A cyber resilience exercise involving key CNI stakeholders
- An operating model, strategy, and implementation plan for regulation of CNI in Nigeria

Cybersecurity toolkits for SMEs

Why are we delivering this work?

Small and medium sized business in Nigeria often do not have sufficient cybersecurity measures in place to protect them against growing cybercrime. They represent vulnerable targets to the attacks of cybercriminals which can cause them significant financial hardship and or even force them to stop trading.

With these businesses responsible for the majority of Nigerian employment, the fallout from successful cyberattacks can be substantial. Furthermore, female-owned small and medium sized businesses are more likely to be significantly impacted by a cyberattack than their male-owned counterparts – partly because they appear to have less access to valuable resources, support or advice.

The current lack of understanding among these businesses about the scale of cyber threats is a critical consideration within this project. Nigerian small and medium sized businesses will be provided with cybersecurity toolkits that take into account the local business environment and cyber threat landscape, using relatable real-life examples.

These will be accompanied by a vulnerability assessment tool, helping these businesses understand better their cyber maturity and posture, and will include e-learning modules on cybersecurity and cyber hygiene. The measures will raise awareness of the scale of the threat facing these organisations, encouraging and incentivising them to invest the time needed to make best use of the available tools, improve their overall cybersecurity posture, and protect their livelihoods.

NG4

Bolstering Nigerian small businesses' cybercrime defences

Who are we working with?

- Federal Ministry of Communications and Digital Economy
- Office for ICT Innovation and Entrepreneurship (OIIE)
- Nigerian Small and Medium Enterprises (SMEs)
- Development Agency of Nigeria (SMEDAN)
- National Information Technology Development Office (NITDA)
- Office of the National Security Advisor (ONSA)
- local NGO CyberSafe Foundation which specialises in working with Nigerian SMEs to help deliver the services in addition to other local specialist organisations

What is being delivered?

- Selection and tailoring of a toolkit through consultation with key stakeholders (including government departments and local NGOs)
- A communications strategy and implementation plan for the dissemination of toolkits to NGOs
- Pilot launch of toolkit including cyber e-learning for 25 to 50 female owned businesses
- Workshops and conferences for NGOs, Tech Hubs developed as part of this Digital Access Programme – Pillar 3, and target small and medium sized businesses to disseminate toolkits through a Train-the-Trainer approach

Digital forensics and judicial cybercrime training

why are we delivering this work?

Nigerian cybercrime causes significant financial losses for unsuspecting Nigerian citizens and businesses, particularly the most vulnerable. Over the next five years 100m additional Nigerians are expected to be online for the first time. The prevalence of cybercrime, and its impact abroad, also damages Nigeria's global reputation, which could affect its ability to attract inward investment.

The Nigerian government aims to improve its record of combating cybercrime, building on its 2015 Cybercrimes Act. Its recent National Cybersecurity Policy and Strategy identified several capacity gaps, including a lack of digital forensics skills and processes for reporting and managing cybercrime. In addition, judges and prosecutors often lack sufficient cybercrime knowledge, reducing the likelihood that perpetrators are successfully prosecuted.

This project will address this issue by providing training to the Nigerian Police Force's (NPF's) specialist cybercrime unit, helping them to conduct effective and professional investigations. Training will also be provided to the National Judicial Institute on how to best prosecute cybercrime.

Together, these efforts will disrupt the source of cybercrime activity that targets Nigeria's domestic population and countries worldwide. It will improve the public's faith in the NPF and its ability to prosecute cybercrime domestically, helping to increase the level of cybercrime reporting in general and specifically from vulnerable groups. It will also improve the country's international reputation in cybersecurity, and its prospects for inward investment and economic development.

NG7

Tackling cybercrime

Who are we working with?

- The Nigerian Police Force (NPF)
- The National Judicial Institute (NJI)
- Office of the National Security Advisor (ONSA)
- KPMG Nigeria
- Cysiam, Chatham House and Social Development Direct (SDD)

What is being delivered?

- Cybercrime diagnostic assessment to understand the gaps in the way cybercrime is tackled in the Nigerian criminal justice sector
- Professional Training Policy and Framework for law enforcement, judges, and prosecutors
- Training courses, modules and workshops for Nigeria's specialist cybercrime unit and Judges and prosecutors, covering topics such as digital data sources and exploitation, data integrity, chain of custody and attribution
- A strategic communications campaign aimed at the general public to raise awareness of cybercrime

National cybersecurity strategy communications campaign

Why are we delivering this work?

Nigeria is launching a refresh of its National Cybersecurity Policy and Strategy (NCPS), led by the **Office of the National Security Adviser (ONSA)**. The strategy focuses on eight areas, ranging from strengthening cybersecurity governance and protecting critical national infrastructure through to strengthening the legal and regulatory framework and promoting a thriving digital economy.

As part of the refresh, ONSA wants to deploy a substantial communications campaign to raise awareness of the strategy and provoke discussions on its implementation. This campaign will highlight what has changed as a result of the review, why this matters and what people might be expected to do differently as a result.

The campaign will engage a broad mix of different audiences, from other government agencies and critical industry sectors through to the general population.

Senior government officials need to understand how changes to the NCPS may affect their departments and what policy -related actions might be expected of them. Critical industries, including defence, energy and telecommunications, need to understand what NCPS means for them. And the general population need to understand what they need to do to protect themselves and to help build a more cyber-aware and cybersecure Nigeria.

NG18

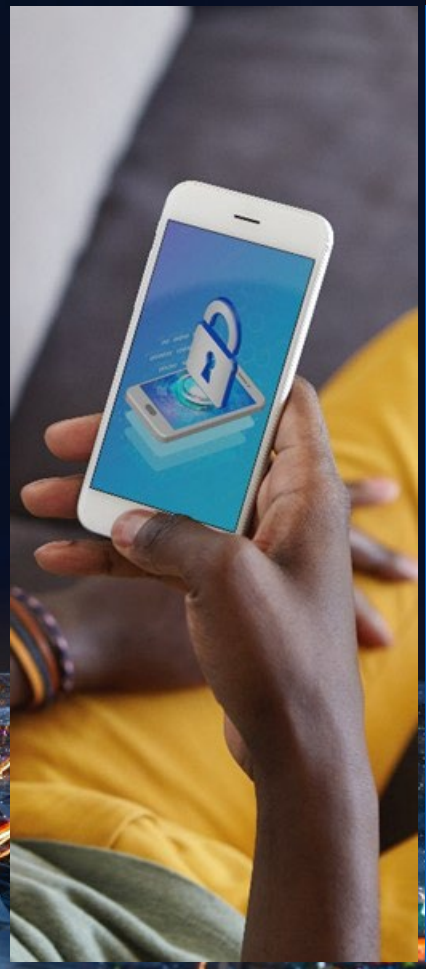
Helping Nigerians understand what the strategy means for them

Who are we working with?

- Office of the National Security Advisor (ONSA)
- KPMG Nigeria
- Social Development Direct (SDD). UK organisation ensuring social inclusion, equality and human rights are central to UK Aid programmes
- UK based Torchlight Group– Support national security and resilience and strategic communications

What is being delivered?

- A multi-channel communications campaign that will drive awareness and uptake of the Nigerian Cyber-Security Strategy
- Capacity to deliver future strategic communications campaigns
- Sector specific guidance for key stakeholders from six sectors to enable them to understand their responsibilities as outlined in the Cybersecurity Strategy and Policy



Kenya

Supporting the Data Protection Commissioner

Why are we delivering this work?

Kenya has previously suffered from significant data breaches and its citizens have experienced frequent cases of fraud, identity theft, stalking and even kidnap stemming from the abuse of personal data. Vulnerable groups have been at particular risk from these threats – unaware how their data has been used, let alone protected.

Keen to better protect the personal data of its citizens, the Kenyan government has established the Office of the Data Protection Commissioner (ODPC), but it is still developing its capacity towards becoming fully operational.

This three-stage project will help to accelerate the ODPC's effectiveness, first by helping it develop its initial three -year strategy. This will be followed by a capacity building phase to ensure employees are suitably equipped and trained, and then supported to implement the strategy.

Overall, establishing the regulatory environment will ensure Kenyans' personal data is better protected. Since this is becoming a pre-requisite for international trade and governmental collaboration, this will lead to wider benefits for Kenya.

KE1

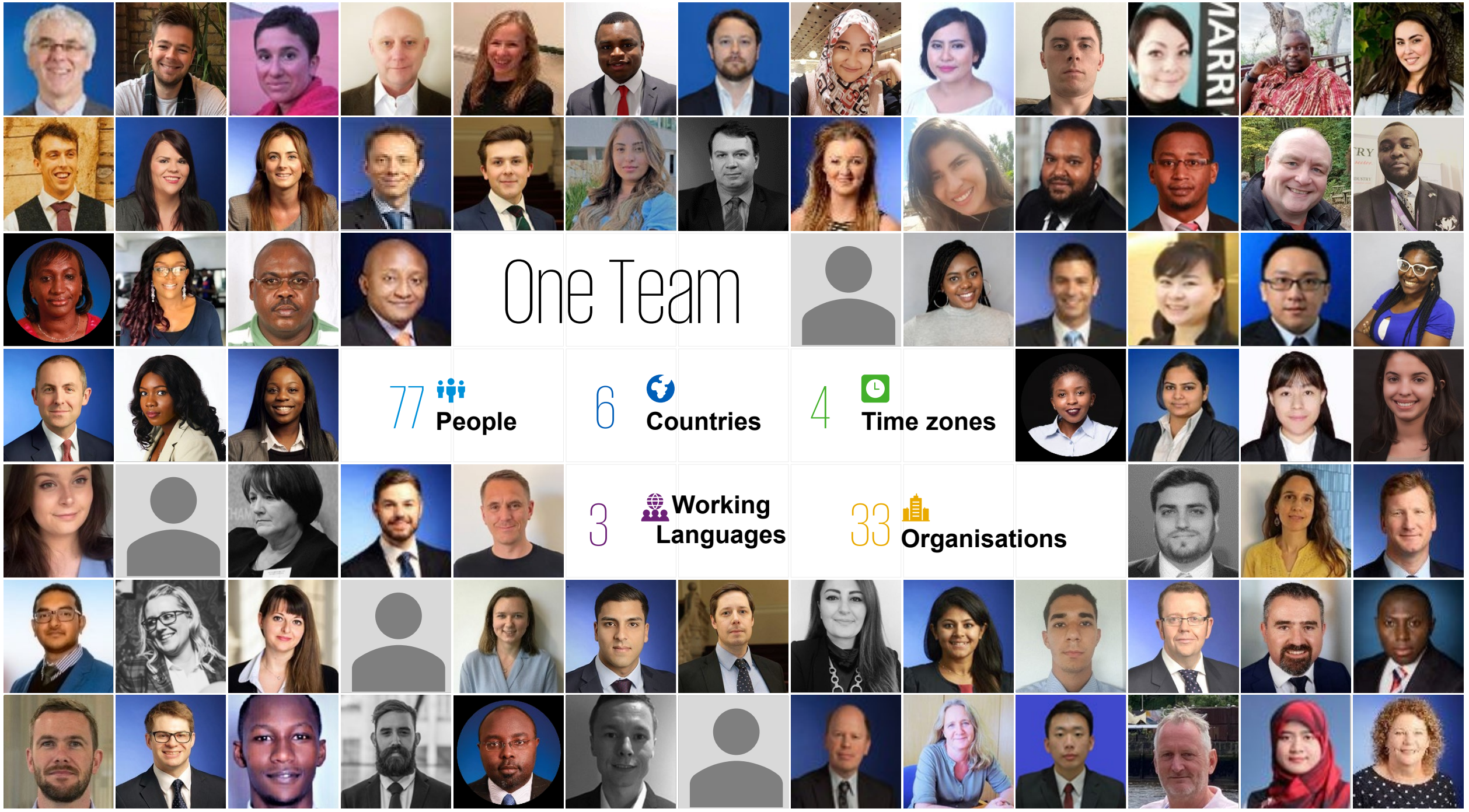
Protecting Kenyan's personal data

Who are we working with?

- Office of the Data Protection Officer Kenya (ODPC)
- Communications Authority Kenya
- Civil Society organisations within Kenya
- KPMG Kenya
- Social Development Direct (SDD)
- Strathmore University

What is being delivered?

- Support to ODPC to enable it to accelerate including prioritising its operational goals
- A multi-year data protection strategy
- Knowledge transfer to equip ODPC staff and build the Office's capacity to deliver priority elements of data strategy
- Framework for building capacity through a relevant group such as the Common Thread Network


One Team
77 People
6 Countries
4 Time zones
3 Working Languages
33 Organisations