National Cyber Security and Data Protection Strategy 2017 – 2022

(DRAFT)

NATIONAL CYBER SECURITY AND DATA PROTECTION STRATEGY 2017-2022

Table of Contents

1.0 EXECUTIVE SUMMARY

The future of our security and prosperity rests on a robust and secure digital environment. Our generation's greatest test lies in a flourishing digital environment that is resilient to computer threats, armed with the understanding and requirements to maximize opportunities and mitigate risk. Our dependence on the internet breeds a lot of insecurity as its very invention was based on robustness and adaptability instead of its security. These loopholes have given birth to criminals of different intent trying to exploit vulnerabilities by launching cyber-attacks. Due to the evolving nature of the cyber landscape, these threats cannot be eradicated but Sierra Leone is committed to ensure the risks are minimized to enhance the safety, security and prosperity of the state.

1.1 INTRODUCTION

The biggest revolution ever seen by the human race is that of Information and communication technologies, and keeps evolving and is now integrated into virtually every aspect of our lives. The world is digitalized and Sierra Leone is not an exception. The integrity of cyberspace is enormous as loss of trust in that integrity would jeopardize the benefits of this technological revolution.

Most of the hardware and software originally created to facilitate this interconnected digital environment has prioritized efficiency, cost and the convenience of the user, but has not always had security designed in from the start. Malicious actors – hostile states, criminal or terrorist organizations and individuals – can exploit the gap between convenience and security. Narrowing that gap is a national priority.

The introduction of internet of things (IOTs) is expanding the Internet beyond computers and mobile phones into other cyber-physical or 'smart' systems which are extending the threats of remote exploitation to a whole host of new technologies. Systems and technologies that underpin our daily lives are therefore potentially compromised. The government of Sierra Leone has now seen cyber threats as part of its routine concerns and pose a greater risk to the state of Sierra Leone.

1.2 THE SCOPE OF THE STRATEGY

This strategy is intended to shape the Government's policy on cyber security, while also offering a rational and compelling vision to share with the public and private sector, civil society, academia and the wider population. The strategy blankets the whole of the state.

The strategy sets out proposed or recommended actions aimed at all sectors of the economy and society, from ministries, departments and agencies, to leaders across industry and the individual citizen. The strategy aims to increase cyber security at all levels for our collective benefit - good internet governance.

In this strategy, 'cyber security' refers to a set of activities and measures, both technical and non-technical, intended to protect the bioelectric environment from all possible threats.

Consistent with our assessment of the challenge we face, this document sets out:

- assessment of the strategic context, including present and evolving threats;
- a preview of vulnerabilities and how these can be developed over the next five years;
- objectives to achieve our goal, including guiding principles, roles and responsibilities;
- Intentions to put our policy into practice.

1.3 MISSION STATEMENT:

This 2017 National Cyber Security Strategy plan, underpinned by the Government's commitment to boaster our state security, has the potential to deliver substantial improvements to Sierra Leone's cyber security. It hopes to achieve important outcomes by looking to the market to drive secure cyber ethics. But this approach will not achieve all the scale and pace of change required to stay ahead of the fast-moving threats; we need to go further as time passes by as technology is an evolving subject matter.

The 2017 National Cyber Security Strategy Plan, driven by government's commitment to enhance state security shall deliver substantial improvements to Sierra Leone's cyber security; regardless of the scale and pace of the change required to stay ahead of the fast-moving threats, this strategy hopes to achieve positive outcomes by looking to the market to drive best practice cyber ethics.

1.4 VISION STATEMENT

Our vision for 2023 is to ensure that Sierra Leone is safe, secure, resilient and trusted to provide opportunities for its populace, protect national interest and resources, enhance peaceful environment and proactive engagement to deter and defend cyber threats and be prosperous and confident in the digital world.

Our vision is to protect our national interests and resources to enhance a safe and secure environment with proactive engagement to deter and defend against cyber threats in our digital domain.

The following thresholds shall be met in other to actualize this vision:

- DEFEND - We shall provide the means require to defend the state against evolving cyber threats, to respond effectively to incidents, to ensure our networks, data and systems are protected and resilient. The citizens, private and public sectors have the understanding and resources to defend themselves.
- DETER - The state shall be a hard nut to crack for all brands of hostility in cyberspace. We shall diagnose, investigate and disrupt unfriendly action taken against the state while, pursuing and prosecuting culprits. The state shall resort to alternatives to take invasive measures in cyberspace, should the need arise.
- DEVELOP - The state shall build and develop its cyber security industry, supported by international trends and best practices by harnessing the untapped talent and resources of its citizens to provide the skills required to meet our national needs across the public and private sectors. Our hunger and determination shall enable us to meet and overcome future threats and challenges.

Reinforcing the above targets, we shall pursue and deepen existing links with our closest international partners, recognizing that this enhances our collective security.

To achieve these outcomes over the next five years, the Government of Sierra Leone shall intervene more actively and provide more investment to support market forces to raise cyber security standards across the state. The Cyber Incident and Response Team of Sierra Leone (CIRT-SL) will work with the private and public sectors to ensure that individuals, businesses and organizations adopt the behaviors required and the appropriate measures to stay safe on the

Internet. We shall drive improvements that are in the national interest, particularly in relation to the cyber security of our critical national infrastructure.

The Government will draw on its capabilities and those of industry to develop and apply active cyber defense measures to significantly enhance the levels of cyber security across networks. These measures include minimizing the most common forms of phishing attacks, filtering known bad IP addresses, and actively blocking malicious online activity. Improvements in basic cyber security will raise our resilience to the most commonly deployed cyber threats.

We have created CIRT-SL to be the leading authority on Sierra Leone's cyber security environment, sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues. We shall have the means to respond to cyber-attacks in the same way as we respond to any other attack, using whichever capability is most appropriate, including an offensive cyber capability.

2.0 STRATEGIC CONTEXT

The scale of global technological change and its impact is already apparent. The trends and opportunities described before have since accelerated. New technologies and applications have come to the fore, and greater uptake of internet-based technologies worldwide, in particular in developing countries like Sierra Leone, has offered increasing opportunities for economic and social development. These developments have brought, and will continue to bring significant advantages to connected societies such as ours. But as our reliance on networks grows, so do the opportunities for those who would seek to compromise our systems. Equally, the geopolitical landscape has changed. Malicious cyber activity knows no international boundaries. State actors are experimenting with offensive cyber capabilities. Cyber criminals are broadening their efforts and expanding their modus operandi to achieve higher value pay-outs. Terrorists, and their sympathizers, are conducting low-level attacks and aspire to carry out more significant acts. This chapter sets out our assessment of the nature of these threats, our vulnerabilities and how these continue to evolve.

2.1.1 THREATS

2.1.1.1 Cyber criminals

This strategy deals with cybercrime in the context of two interrelated forms of criminal activity:

- cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. Infectious and Malicious codes for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and
- Cyber-enabled crimes – old-fashioned crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

These criminals are primarily responsible for developing and deploying the increasingly advanced malware that infects our computers and networks across all sectors. The impact is dispersed throughout, but the cumulative effect is significant. These attacks are becoming increasingly aggressive and confrontational, as illustrated by the increasing use of ransomware, phishing, and threats of distributed denial of service (DDoS) for extortion.

Whilst criminals may pose a significant threat to our collective prosperity and security, equally of concern is the continuing threat from acts of less sophisticated but widespread cyber-crimes carried out against individuals or smaller organizations. Financial and personal data, industrial blueprints and government secrets are not safe except countermeasures are installed to manage such.

2.1.1.2 States and state-sponsored threats

We are conversant with regular attempts by states and state-sponsored groups to penetrate sovereign networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defense, finance and other critical national infrastructures.

The capacity and impact of these state cyber programmes varies. The most advanced nations continue to improve their capabilities at pace, integrating encryption services into their tools in order to remain covert. While they have the technical capability to deploy sophisticated attacks,

they can often achieve their aims using basic tools and techniques against vulnerable targets because the defenses of their victims are poor.

2.1.1.2 Terrorists

Terrorist groups continue to aspire to conduct damaging cyber activities against nations and their interests. The current technical capability of terrorists is judged to be low. Nonetheless, the impact of even low-capability activities against the state to date has been unpredictable: the sniffing of Al Shabab, Boku Haram and possible ISIS as we are seen as allies of western states is a case in point.

The use of online radicalization and spreading fear through social networks would have serious consequences on our national security if not countered. Terrorists will likely use any cyber capability to achieve the maximum effect possible. Thus, even a moderate increase in terrorist capability may constitute a significant threat to the Sierra Leone and its interests.

2.1.1.3 **Hacktivists**

Hacktivists (hackers and activists) groups are decentralized and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of Hacktivists cyber activities are disruptive in nature (website defacement or DDoS), well trained Hacktivists have been able to inflict greater and lasting damage on their victims.

Insider threats remain a cyber-risk to organizations in Sierra Leone. Malicious insiders, who are trusted employees of an organization and have access to critical systems and data, pose the greatest threat. They can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their privileged knowledge, or access, to facilitate, or launch, an attack to disrupt or degrade critical services on the network of their organizations, or wipe data from the network.

2.2 VULNERABILITIES

2.2.1 Internet of things (IOTs)

Most people conceive of cyber security through the prism of protecting devices such as their desktop computer or laptop. However, the internet has become increasingly integrated into our daily lives in ways we are largely oblivious of. The IOTs creates new opportunities for

exploitation and increases the potential impact of attacks which have the potential to cause physical damage, injury to persons and, in a worst case scenario, death.

The rapid implementation of connectivity in industrial control processes in critical systems, across a wide range of industries such as energy, mining, agriculture and aviation, has created the Industrial Internet of Things. This is simultaneously opens up the possibility of devices and processes, which were never vulnerable to such interference in the past, being hacked and tampered with, with potentially disastrous consequences.

2.2.2 Poor cyber hygiene and compliance

Awareness of technical vulnerabilities in software and networks, and the need for cyber hygiene, has undoubtedly been ignored due to lack of awareness and initiatives to promote cyber safety, Cyber-attacks are not necessarily sophisticated or inevitable and are often the result of exploited – but easily rectifiable and, often, preventable – vulnerabilities. In most cases, it continues to be the vulnerability of the victim, rather than the ingenuity of the attacker, that is the deciding factor in the success of a cyber-attack. Businesses and organizations decide on where and how to invest in cyber security based on a cost-benefit assessment, but they are ultimately liable for the security of their data and systems. Only by balancing the risk to their critical systems and sensitive data from cyber-attacks, with sufficient investment in people, technology and governance, will businesses reduce their exposure to potential cyber harm.

2.2.3 Insufficient training and skills

The lack of skills and knowledge to meet our cyber security needs across both the public and private sector is a cause for concern. In businesses, many staff members are not cyber security aware and do not understand their responsibilities in this regard, partially due to a lack of formal training. The public is also insufficiently cyber aware.

We also need to develop the specialist skills and capabilities that will allow us to keep pace with rapidly evolving technology and manage the associated cyber risks. This skills gap represents a national vulnerability that must be resolved.

2.2.4 Legacy and unpatched systems

Many networks continue to use vulnerable legacy systems until their next IT upgrades. Software on these systems will often rely on older, unpatched versions. These older versions often suffer

from vulnerabilities that attackers look for and have the tools to exploit. An additional issue is the use by some organizations of unsupported software, for which patching regimes do not exist. According to CISCO's 2016 annual security report, 106,000 devices out of 115,000 analyzed, had vulnerabilities in the software they are running on.

2.2.5 **Access to hacking resources**

The readily available hacking information and user-friendly hacking tools on the Internet is enabling those who want to develop a hacking capability to do so. The information hackers need in order to compromise victims successfully is often openly accessible and can be reaped quickly. Everyone needs to be aware of the extent of exposure of their personal details and systems on the Internet, and the degree to which that could leave them vulnerable to malicious cyber exploitation.

2.3 CONCLUSIONS

We have adopted a national cyber security and data protection policy and established institution(s) that will enhanced our resilience and mitigate some of the threats we face in cyberspace. However, we are not yet ahead of the threats. The types of malicious cyber actors we must contend with, and their motivations, have largely endured, even as the volume of malware and the numbers of such malicious actors has grown rapidly. Our collective challenge is to ensure our defenses are evolved, reinforced and responsive enough to counter such threats, to reduce the ability of malicious actors to attack us and to address the root causes of the vulnerabilities outlined above.

3.0 NATIONAL RESPONSE

To mitigate the multiple threats we face and safeguard our interests in cyberspace, we need a strategic approach that underpins all our collective and individual actions in the digital domain over the next five years. This section sets our strategic approach.

3.1 PRINCIPLES

In working towards these objectives, the Government will apply the following principles:

- our policies shall be driven by the need to both protect our people and enhance our prosperity;

- we shall treat all forms of cyber-attack serious and we will defend ourselves at all cost;
- we shall act in accordance with national and international laws;
- We shall protect and promote our core values. These include democracy; the rule of law; human rights;
- we shall preserve and protect citizens' privacy;
- We shall work in partnership with all sectors. Government shall meet its responsibilities and lead the national response;
- responsibility for the security of organizations across the public sector, including cyber security and the protection of online data and services, lies with respective MDAs;
- we shall not accept significant risk being posed as a result of businesses and organizations failing to take the steps needed to manage cyber threats; and
- We shall ensure Government interventions have substantive impact on overall national cyber security initiatives.

3.2 DUTIES

Securing the national cyberspace will require a collective effort. Each and every one of us has an important part to play.

3.2.1 Persons

As citizens and noncitizens, we should take practical steps to secure the assets we value in the virtual world just as we do in the physical world. That means fulfilling our personal responsibility to take all reasonable steps to safeguard not only our hardware – our smart phones and other devices – but also the data, software and systems that affords us freedom, flexibility and convenience in our private and professional lives.

3.2.2 Private sectors and organizations

Businesses, public and private sector organizations and other institutions hold personal data, provide services, and operate systems in the electronic domain. The connectivity of this information has revolutionized their operations. However, with this technological transformation comes the responsibility to safeguard the assets which they hold, maintain the services they provide, and incorporate the appropriate level of security into the products they sell. Society shall look to businesses and organizations to take all reasonable steps to protect their personal data,

and build resilience. Businesses and organizations must also understand that, if they are the victim of a cyber-attack, they are liable for the consequences.

3.2.3 Government

The primary duty of the Government is to defend the country from attacks by other states, to protect citizens and the economy from harm, and to set the domestic and international framework to protect our interests, safeguard fundamental rights, and bring criminals to justice.

As the holder of significant data and a provider of services, the Government takes stringent measures to provide safeguards for its information assets. The Government also has an important responsibility to advise and inform citizens and organizations what they need to do to protect themselves online, and where necessary, set the standards we expect key companies and organizations to meet.

3.2.4 Driving change

This Strategy seeks to derive outcomes and increase capacity in both the public and private sector by looking to the market to drive the right behaviors. It is expected that commercial pressures and government- incentives will drive adequate business investment to enhance appropriate cyber security standards that will stimulate a flow of investment into our industry, and to encourage an adequate pull of skills to the sector.

The Government is committed to bring about significant improvements in our national cyber security over the next five years. This ambitious and transformational programme will focus on the following three broad areas:

1. Expanded intelligence and law enforcement focus on the threats. The intelligence agencies, the ONS, CISU, Ministry of Defense, the police and other National Crime Agencies, in coordination with international partner agencies, will expand their efforts to identify, anticipate and disrupt hostile cyber activities by foreign actors, cyber criminals and terrorists. This will improve their intelligence collection and exploitation, with the aim of obtaining pre-emptive intelligence on the intent and capabilities of our adversaries.
2. Development and deployment of technology in partnership with industry, including Active Cyber Defense measures, to deepen our understanding of the threats, to strengthen the security of the public and private sector systems and networks in the face of these threats, and to disrupt malicious activity.

3. Cyber Incidence Response - The Government has established the Cyber Incident Response Team (CIRT-SL) as the, central body for cyber security at the national level. This body will manage national cyber incidents, provide an authoritative voice and center of expertise on cyber security, and deliver tailored support and advice to departments, regulators and businesses. This body will coordinate efforts to detect, analyze, respond to and recover from cyber threats, and will also provide its cyber security expertise to support the Government's efforts to support a promising cyber secured environment, and stimulate the development of cyber security skills.

The CIRT-SL provides:

- a unified source of advice for the Government's cyber security threat intelligence and information assurance;
- the strong public face of the Government's action against cyber threats – working hand in hand with industry, academia and international partners to keep the state protected against cyber-attack.
- A frontline organization that draws on necessary secret intelligence and technical expertise.

4.0 IMPLEMENTATION PLAN

Our goals for the country's cyber security over the next five years are rightly ambitious. To achieve them will require us to act with consequence and determination across the digital landscape. Activities to deliver the Government's vision will advance the three primary objectives of the strategy: to DEFEND our cyberspace, to DETER our adversaries and to DEVELOP our capabilities.

4.1 DEFEND

4.1.1 ACTIVE CYBER DEFENCE

Active Cyber Defense (ACD) is the principle of implementing security measures to strengthen a network or system to make it more robust against attack. In a commercial context, Active Cyber Defense normally refers to cyber security analysts developing an understanding of the threats to their networks, and then devising and implementing measures to proactively combat, or defend, against those threats. The 'network' we are attempting to defend is the entire national

cyberspace. The activities proposed represent a defensive action plan, drawing on the expertise of CIRT-SL as the Authority to respond to cyber threats.

In undertaking ACD, the Government aims to:

- make the state much harder target for state sponsored actors and cyber criminals by increasing the resilience of our networks;
- defeat the vast majority of high-volume/low-sophistication malware activity on networks by blocking malware communications;
- evolve and increase the scope and scale of Government's capabilities to disrupt serious state sponsored and cybercriminal threats;
- secure our internet and telecommunications gateways, from hijacking;
- harden the Sierra Leone's critical information infrastructure and services against cyber threats; and
- Disrupt the business model of attackers of every type.

In pursuit of these aims, the Government shall:

- Work with industry, especially telecoms, to make it significantly harder to attack internet services and users, and greatly reduce the prospect of attacks having a sustained impact on Sierra Leone;
- increase the scale and development of all cyber constituents to disrupt the most serious cyber threats to Serra Leone; and
- better protect government systems and networks, to help industry build greater security into the CNI supply chain.

Where possible, these initiatives will be delivered with or through partnerships with industry. For many, industry will be designing and leading implementation, with the Government's critical contribution being expert support, advice and thought-leadership.

The Government will also undertake specific actions to implement these measures, which will include:

- Working with internet service providers (ISPs) to block malware attacks. We will do this by restricting access to specific domains or web sites that are known sources of malware.
- preventing phishing activity that relies on domain 'spoofing' (where an email appears to be from a specific sender, such as a bank or government department, but is actually

fraudulent) by deploying an email verification system on government networks as standard and encouraging industry to do likewise;

- promoting security best practice through multi-stakeholder internet governance organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and UN Internet Governance Forum (IGF);
- working with law enforcement channels to protect citizens from being targeted in cyber-attacks from unprotected infrastructure overseas;
- working towards the implementation of controls to secure the routing of internet traffic for MDAs to ensure that it cannot be illegitimately re-routed by malicious actors.

We will develop these technical interventions as threats evolve to ensure that citizens and businesses are protected by default from the majority of large-scale commodity cyber-attacks.

The Government will measure its success in establishing effective ACD by assessing progress towards the following outcomes:

- Sierra Leone is harder to 'phish', because we would have better defenses against the use of malicious domains and deter social engineering attacks;
- a far larger proportion of malware communications and technical artifacts associated with cyber-attacks and exploitation are being blocked;
- Sierra Leone's internet and telecommunications traffic is significantly less vulnerable to rerouting by malicious actors;
- ONS/CISU, the Armed Forces' and other units to respond to serious state - sponsored and criminal threats have significantly increased.

4.1.2 BUILDING A MORE SECURE INTERNET

Changing technology provides us with the opportunity to significantly reduce the ability of our adversaries to conduct cybercrime in Sierra Leone by ensuring that future online products and services coming into use are 'secure by default'. That means ensuring that the security controls built into the software and hardware we use are activated as a default setting by the manufacturer so that the user experiences the maximum security offered to them, unless they actively choose to turn it off. The challenge is to effect transformative change in a way that supports the end user and offers a commercially viable, but secure, product or service – all within the context of maintaining the free and open nature of the Internet.

The majority of online products and services coming into use become 'secure by default' by 2022. Consumers will be empowered to choose products and services that have built-in security as a default setting. Individuals can switch off these settings if they choose to do so but those consumers who wish to engage in cyberspace in the most secure way will be automatically protected.

We will pursue the following actions:

- the Government shall lead by example by running secure services on the Internet that do not rely on the Internet itself being secure;
- the Government shall explore options for collaboration with industry to develop cutting-edge ways to make hardware and software more 'secure by default'; and
- We shall adopt challenging new cyber security technologies in government, encouraging administrations to do likewise, in order to reduce perceived risks of adoption. This will provide proof of concept and demonstrate the security benefits of new technologies and approaches.

It will also put security at the heart of new product development, eliminate opportunities for criminal exploitation and thereby protect the end user.

To do this we shall:

- Continue to encourage procuring bodies to purchase hardware and software products with security settings activated as default, requiring the user to actively disable these settings to make them insecure. Some vendors are already doing this, but some are not yet taking these necessary steps;
- continue to develop an Internet Protocol (IP) reputation service to protect government digital services (this would allow online services to get information about an IP address connecting to them, helping the service make more informed risk management decisions in real time);
- seek to install products on government networks that will provide assurance that software is running correctly, and not being maliciously interfered with;
- look to expand beyond the CIRT. GOV.SL domain into other digital services measures that notify users who are running out-of-date browsers; and

- Invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast Identity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate.

The Government shall also explore how to encourage the market by providing security ratings for new products, so that consumers have clear information on which products and services offer them the greatest security. The Government shall also explore how to link these product ratings to new and existing regulators, and ways to warn consumers when they are about to take an action online that might compromise their security.

The Government shall measure its success in building a secure Internet by assessing progress towards the following outcomes:

- the majority of commodity products and services available in Sierra Leone in 2022 are making Sierra Leone more secure because they have their default security settings enabled by default or have security integrated into their design; and
- all government services provided at national, local and Devolved Administration level are trusted by the Sierra Leone public because they have been implemented as securely as possible, and fraud levels are within acceptable risk parameters.

4.1.3 PROTECTING GOVERNMENT

The Government, Devolved Administrations and the wider public sector hold large quantities of sensitive data. They deliver essential services to the public and operate networks that are critical to national security and resilience. The Government's systems underpin the functioning of our society. The modernization of public sector services will continue to be the cornerstone of the Digital Strategy. To retain the trust of citizens in online public sector services and systems, data held by government must be protected and all branches of government must implement appropriate levels of cyber security in the face of continuous attempts by hostile actors to gain access to government and public sector networks and data.

We want to achieve the following outcomes:

- citizens use government online services with confidence: and trust that their sensitive information is safe and, in turn, understand their responsibility to submit their sensitive information online in a secure manner;
- the Government shall set and adhere to the most appropriate cyber security standards, to ensure that all branches of government understand and meet their obligations to secure their networks, data and services; and
- The Government's critical assets, including those at the highest classification, are protected from cyber-attacks.

The Government shall continue to move more of its services online so that the state can become truly 'digital by default'. The Government's ministry of information stakeholders and CIRT-SL shall ensure that all new digital services built or procured by government are also 'secure by default'. The Government's networks are highly complex and in many cases still incorporate legacy systems, as well as some commercially available software which is no longer supported by the vendor. We will ensure that there are no unmanaged risks from legacy systems and unsupported software.

We will improve government and wider public sector resilience to cyber-attack. This means ensuring an accurate and up to date knowledge of all systems, data, and those who have access to them. The likelihood and impact of a cyber-incident will be minimized by implementing best practice as set out by the CIRT-SL. The Government will also ensure that it is able to respond effectively to cyber incidents through a programme of incident exercises and regular testing of government networks. We will invite Entrusted Administrations and local authorities to participate in these exercises, as appropriate

Cyber security is not just about technology. Almost all successful cyber-attacks have a contributing human factor. We will therefore continue to invest in our people, to ensure that everyone who works in government has a sound awareness of cyber risk. We will develop specific cyber expertise in areas where the risks are heightened and ensure that we have the right processes in place to manage these risks effectively.

The CIRT-SL will develop/assemble world- leading cyber security guidance which will keep pace with the threat and development of new technologies. We will take steps to make sure

government organizations have easy access to threat information to inform their understanding of their own cyber risks and take appropriate action.

We will continue to improve our highest classification networks to safeguard the Government's most sensitive communications.

CIRT-SL will work closely with the MOD to confront its cyber challenges and contribute to the wider national cyber security. The Government shall measure its success in protecting government networks, systems and data by assessing progress towards the following outcomes:

- an in-depth understanding of the level of cyber security risk across the whole of government and the wider public sector;
- individual government departments and other bodies protect themselves in proportion to their level of risk and to an agreed government minimum standard;
- government departments and the wider public sector are resilient and can respond effectively to cyber incidents, maintaining functions and recovering quickly;
- new technologies and digital services deployed by government will be cyber secure by default;
- we are aware of, and actively mitigating, all known internet-facing vulnerabilities in government systems and services; and
- all suppliers to the Government meet appropriate cyber security standards.

4.1.4 PROTECTING OUR CRITICAL NATIONAL INFASTRUCTURE(CNI) AND OTHER PRIORITY SECTORS

The cyber security of certain organizations is of particular importance because a successful cyber-attack on them would have the severest impact on the country's national security. This impact could have a bearing on the lives of citizens, the stability and strength of the economy. This premium group of companies and organizations within the public and private sector includes the critical national infrastructure (CNI), which provides essential services to the nation. Ensuring the CNI is secure and resilient against cyber-attack shall be a priority for the Government. This premium group also includes other companies and organizations, beyond the CNI, that require a greater level of support. They include:

- the jewels in our economic crown – the most successful companies and also those that hold our future economic strength in the value of their research and intellectual property;

data holders – not just organizations that hold large amounts of personal data, but also those that hold data on vulnerable citizens here and abroad, such as charities;

- high-threat targets – such as media organizations, where an attack could harm our reputation, damage public confidence in the Government, or endanger freedom of expression;
- the touchstones of our digital economy – digital service providers that enable e-commerce and our digital economy, and who depend on consumer trust in their services; and
- those organizations that, through market forces and authority, can exert influence on the whole economy to improve their cyber security, such as insurers, investors, regulators and professional advisors.

. Our CNI – in both the private and public sector – continues to be a target for attack hence the need to protect these vital parts of our economy and support the organizations that heavily influence others. Across these and many other priority sectors cyber risk is still not properly understood or managed, even as the threat continues to diversify and increase.

The Government shall, therefore, understand the level of cyber security across our CNI and have measures in place to intervene where necessary to drive improvements that are in the national interest.

The Government shall:

- share threat information with industry that only the Government can obtain so they know what they must protect themselves against;
- produce advice and guidance on how to manage cyber risk and, working collaboratively with industry and academia, define what good cyber security looks like;
- stimulate the introduction of the high- end security needed to protect the CNI, such as training facilities, testing labs, security standards and consultancy services; and
- conduct exercises with CNI companies to assist them in managing their cyber risks and vulnerabilities.

The CIRT-SL will provide these services for the most important companies and organizations, including the CNI. It will do so in partnership with departments and regulators, who will assure

whether cyber risk is being managed in their sectors to the level demanded by the national interest.

The Government shall also ensure that the right regulatory framework for cyber security is in place, one that:

- ensure industry acts to protect itself from the threat;
- is outcome focused and sufficiently flexible so that it will not fall behind the threat, or lead to compliance rather than sound risk management;
- is agile enough to foster growth and innovation, rather than lead it;
- is harmonized with regimes in other jurisdictions so that companies do not suffer from a fragmented and burdensome approach; and
- delivers, when combined with effective support from the Government, a competitive advantage for CIRT-SL.

Many of our industry sectors are already regulated for cyber security. Nonetheless, we must ensure the right steps are taken across the whole economy, including the CNI, to manage cyber security risks.

The Government will measure its success in protecting our CNI and other priority sectors by assessing progress towards the following outcomes:

- we understand the level of cyber security across the CNI, and have measures in place to intervene, where necessary, to drive improvements in the national interest; and
- our most important companies and organizations understand the level of threat and implement proportionate cyber security practices.

4.1.5 CHANGING PUBLIC AND BUSINESS BEHAVIOURS

A successful digital economy relies upon the confidence of businesses and the public in online services. The Government is working with industry and other parts of the public sector to increase awareness and understanding of the threat. The Government is also providing the public and business with access to some of the tools that they need to protect themselves. While there are many organizations that are doing an excellent job of protecting themselves, and in providing services to others online, the majority of businesses and individuals are still not properly managing cyber risk.

Our objective is to ensure that individuals and organizations, regardless of size or sector, are taking appropriate steps to protect themselves, and their customers, from the harm caused by cyber-attacks.

The Government shall provide the advice that the economy needs to protect itself. We will improve how this advice is delivered to maximize its effect. For the public, the Government shall harness 'trusted voices' to increase the reach, credibility and relevance of our message. We will provide advice that is easy to act upon and relevant to individuals, at the point they are accessing services and exposing themselves to risk. We will involve the Devolved Administrations and other authorities as appropriate.

For businesses, we will work through organizations such as insurers, regulators and investors which can exert influence over companies to ensure they manage cyber risk. In doing so, we will highlight the clear business benefits and the pricing of cyber risk by market influencers. We will seek to understand better why many organizations still fail to protect themselves adequately and then work in partnership with organizations such as professional standards bodies, to move beyond raising awareness to persuade companies to take action. We will also make sure we have the right regulatory framework in place to manage those cyber risks the market fails to address. As part of this, we will seek to use levers, such as the GDPR, to drive up standards of cyber security and protect citizens.

Individuals and organizations in Sierra Leone will have access to the information, education, and tools they need to protect themselves. To ensure we deliver a step-change in public behavior, we will maintain a coherent and consistent set of messages on cyber security guidance from both the Government and our partners. The CIRT-CIRT-SL will provide technical advice to underpin this guidance. It will reflect business and public priorities and practices, and be clear, easily accessible and consistent, while keeping pace with the threat. Law enforcement will work closely with industry and the CIRT-CIRT-SL to share the latest criminal threat intelligence, to support industry to defend itself against threats, and to mitigate the impact of attacks on victims.

4.1.6 CYBER AWARENESS

A Cyber Awareness campaign, will give the public the advice they need to protect themselves from cyber criminals. Targeted messaging delivered through social media and advertising and in partnership with businesses to promote:

- using three random words to create a strong password; and

- always downloading the latest software updates.

Experts agree adopting these behaviors will provide small businesses and individuals with protection against cybercrime. Cyber Awareness should be supported by all partners, including the police and businesses in the retail, leisure, travel and professional services sectors.

4.1.7 CYBER ESSENTIALS

The Cyber Essentials scheme was developed to show organizations how to protect themselves against low-level "commodity threat". It lists five technical controls (access control; boundary firewalls and Internet gateways; malware protection; patch management and secure configuration) that organizations should have in place. The vast majority of cyber-attacks use relatively simple methods which exploit basic vulnerabilities in software and computer systems. There are tools and techniques openly available on the Internet which enables even low-skill actors to exploit these vulnerabilities. Properly implementing the Cyber Essentials scheme will protect against the vast majority of common internet threats.

4.1.8 MANAGING INCIDENTS AND UNDERSTANDING THE THREAT

The number and severity of cyber incidents affecting organizations across the public and private sector are likely to increase. We therefore need to define how both the private sector and the public engage with the Government during a cyber-incident. We will ensure that Government's level of support for each sector – taking into account its cyber maturity – is clearly defined and understood. The Government's collection and dissemination of information about the threat must be delivered in a manner and at a speed suitable for all types of organization. The private sector, government and the public can currently access multiple sources of information, guidance and assistance on cyber security. This must be simplified.

We must ensure that the Government offering, both in responses to incidents, and in the provision of guidance, does not exist in isolation, but in partnership with the private sector. Our incident management processes should reflect a holistic approach to incidents, whereby we learn from partners and share mitigation techniques. We will also continue to use our relationships with other CIRTs allies as an integrated part of our incident management function.

Current incident management remains somewhat fragmented across government departments and this strategy will create a unified approach. The CIRT-SL will deliver a streamlined and

effective government-led incident response function. Government continues to stress the importance of industry, society and the public acting to safeguard their basic cyber security.

Our objectives are as follows:

- The Government shall provide a single, joined-up approach to incident management, based on an improved understanding and awareness of the threat and actions being taken against us. The CIRT-SL will be a key enabler, as will partnership with the private sector, law enforcement and other government departments, authorities and agencies;
- the CIRT-SL defines clear processes for reporting incidents, tailored to the profile of the victim; and
- we will prevent the most common cyber incidents, and we will have effective information-sharing structures in place to inform 'pre-incident' planning.

It is the responsibility of organization and company management, in both the public and private sector, to ensure their networks are secure and to exercise incident response plans. In the event of a significant incident, the Government incident management process will reflect the three distinct elements of a cyber-incident: the precursor causes, the incident itself and the post-incident response.

To deliver incident management that is effective for both government and the private sector, we will work closely to review and define the scope of the Government response to ensure it reinforces cooperation. We will build on our national cyber exercise plan, using our improved understanding and awareness of the threat, to improve our offer of support to public and private sector partners.

We will create a trusted and credible government identity for incident advice, assistance and assurance. This will increase the cyber security awareness across the digital community and will enable us the better to identify trends, take pro-active measures and, ultimately, prevent incidents.

In moving towards automated information sharing (i.e. cyber security systems automatically alerting each other to incidents or attacks), we will deliver a more effective service. This will allow organizations to act swiftly on relevant threat information.

The Government shall measure its success in managing incidents by assessing progress towards the following outcomes:

- a higher proportion of incidents are reported to the authorities, leading to a better understanding of the size and scale of the threat;
- cyber incidents are managed more effectively, efficiently and comprehensively, as a result of the creation of the CIRT-SL as a centralized incident reporting and response mechanism; and
- we will address the root causes of attacks at a national level, reducing the occurrence of repeated exploitation across multiple victims and sectors.

4.2 DETER

The National Security Strategy states that defense and protection start with deterrence. This is as true in cyberspace as any other sphere. To realize our vision of a nation that is secure and resilient to cyber threats, and prosperous and confident in the digital world, we have to dissuade and deter those who would intend to harm us and our interests. To achieve this, we all need to continue to raise levels of cyber security so that attacking us in cyberspace – whether to steal from us or harm us – is neither cheap nor easy. Our adversaries must know that they cannot act with impunity: that we can and will identify them, and that we can act against them, using the most appropriate response from amongst all the tools at our disposal. We will continue to build global alliances and promote the application of international law in cyberspace. We will also more actively disrupt the activity of all those who threaten us in cyberspace and the infrastructure on which they rely. Delivering this ambition requires world-class sovereign capabilities.

4.2.1 CYBER'S ROLE IN DETERRENCE

Cyberspace is only one sphere in which we must defend our interests and sovereignty. Just as our actions in the physical sphere are relevant to our cyber security and deterrence, so our actions and posture in cyberspace must contribute to our wider national security.

The principles of deterrence are as applicable in cyberspace as they are in the physical sphere. CIRT-SL makes clear that the full spectrum of our capabilities will be used to deter adversaries and to deny them opportunities to attack us. However, we recognize that cyber security and resilience are in themselves a means of deterring attacks that rely on the exploitation of vulnerabilities.

4.2.2 REDUCING CYBER CRIME

We need to raise the cost, raise the risk, and reduce the reward of cyber criminals' activity. While we must harden Sierra Leone against cyber-attacks and reduce vulnerabilities, we must also focus relentlessly on pursuing criminals who continue to target CIRT-SL.

Law enforcement agencies will focus their efforts on pursuing the criminals who persist in attacking SL's citizens and businesses. We will work with domestic and international partners to target criminals wherever they are located, and to dismantle their infrastructure and facilitation networks. Law enforcement agencies will also continue to help raise awareness and standards of cyber security, in collaboration with the CIRT-SL.

We will reduce the impact of cybercrime on Sierra Leone and its interests by deterring cyber criminals from targeting Sierra Leone and relentlessly pursuing those who persist in attacking us.

To reduce the impact of cybercrime, we will:

- enhance the law enforcement capabilities and skills at national, regional and local level to identify, pursue, prosecute and deter cyber criminals within Sierra Leone and overseas;
- build a better understanding of the cybercrime business model, so we know where to target interventions in order to have the most disruptive effect on criminal activity;
- deter individuals from being attracted to, or becoming involved in, cybercrime by building on our early intervention measures;
- enhance collaborations with industry to provide them with proactive intelligence on the threat, and to provide us with the upstream intelligence that they possess, in order to assist with our upstream disruption efforts;
- develop a 24/7 reporting and triage capability in Action Fraud, linked to the CIRT-SL, the crime agencies and the wider law enforcement community, to improve support to victims of cybercrime, to provide a faster response to reported crimes and enhanced protective security advice.;
- work with the CIRT-SL and the private sector to reduce vulnerabilities in Sierra Leone infrastructure that could be exploited at scale by cyber criminals; and
- Work with the finance sector to make Sierra Leone a more hostile environment for those seeking to monetize stolen credentials, including by disrupting their networks.

The Government shall measure its success in reducing cybercrime by assessing progress towards the following outcomes:

- we have a greater disruptive effect on cyber criminals attacking the Sierra Leone, with higher numbers of arrests and convictions, and larger numbers of criminal networks dismantled as a result of law enforcement intervention;
- there is improved law enforcement capability, including greater capacity and skills of dedicated specialists and mainstream officers and enhanced law enforcement capability amongst overseas partners;
- there is improved effectiveness and increased scale of early intervention measures dissuades and reforms offenders; and
- There are fewer low-level cyber offences as a result of cybercriminal services being harder to access and less effective.

4.2.3 COUNTERING HOSTILE FOREIGN ACTORS

We need to coordinate the full range of government capabilities to counter the threat posed by hostile foreign actors that increasingly threaten our political, economic and military security. Working with international partners will be crucial to our success, and greater emphasis will be placed on engaging them and working with them to counter the threat. Much of this action will not be in the public domain. Our investment in sovereign capabilities and partnerships with industry and the private sector will continue to underpin our ability to detect, observe and identify this constantly evolving activity against us.

To reduce the cyber threat from hostile foreign actors, we will:

- reinforce the application of international law in cyberspace in addition to promoting the agreement of voluntary, non-binding norms of responsible state behavior and the development and implementation of confidence building measures;
- work with international partners, particularly through collective defense, cooperative security, and enhanced deterrence that our membership of ECOWAS affords;
- identify both the unique and generic aspects of our adversaries' cyber activity;
- Generate and explore all available options for deterring and countering this threat, drawing on the full range of government capabilities. We will take full account of other

related factors, including country-specific strategies, international cyber priorities, and cybercrime and prosperity objectives;

- use existing networks and relationships with our key international partners to share information about current and nascent threats, adding value to existing thought and expertise; and
- Attribute specific cyber identities publicly when we judge it in the national interest to do so.

The Government shall measure its success in countering the actions of hostile foreign actors by assessing progress towards the following outcomes:

- the stronger information-sharing networks that we have established with our international partners, and wider multilateral agreements in support of lawful and responsible behavior by states, are substantially contributing to our ability to understand and respond to the threat, resulting in a better defended Sierra Leone; and
- Our defense and deterrence measures, alongside our country-specific strategies, are making CIRT-SL a harder target for hostile foreign actors to act against.

4.2.4 PREVENTING TERRORISM

The technical capability of terrorists currently remains limited but they continue to aspire to conduct damaging computer network operations against Sierra Leone, with publicity and disruption as the primary objective of their cyber activity. The Government shall identify and disrupt any terrorists use and intending to use cyber for this purpose. In doing so, we will minimize their impact and prevent an uplift in terrorist cyber capability that would further threaten SL networks and national security.

To ensure the threat posed by cyber terrorism remains low, we will:

- detect cyber terrorism threats, identifying actors who are seeking to conduct damaging network operations against Sierra Leone and our allies;
- investigate and disrupt these cyber terrorism actors to prevent them from using cyber capability against Sierra Leone; and
- Work closely with international partners to enable us to better tackle the threat from cyber terrorism.

The Government shall measure its success in preventing terrorism by assessing progress towards the following outcomes:

- a full understanding of risk posed by cyber terrorism, through identification and investigation of cyber terrorism threats to Sierra Leone; and
- Close monitoring, and disruption of terrorist cyber capability at the earliest opportunity, with the aim of preventing an increase in such terrorist capability in the long term.

4.3 CAPACITY DEVELOPMENT

The DEVELOPMENT strand of the strategy sets out how we will acquire and strengthen the tools and capabilities that the Sierra Leone needs to protect itself from cyber threat.

CIRT-SL requires more talented and qualified cyber security professionals. The Government shall act now to plug the growing gap between demand and supply for key cyber security roles, and inject renewed vigor into this area of education and training. This is a long-term, transformative objective, and this strategy wills kick-start this important work, which will necessarily continue beyond 2022. A skilled workforce is the lifeblood of a vital cyber security commercial ecosystem. This ecosystem will ensure cyber start-ups prosper and receive the investment and support they need.

4.3.1 STRENGTHENING CYBER SECURITY SKILLS

The need for Sierra Leone to tackle the systemic issues at the heart of the cyber skills shortage: the lack of young people entering the profession; the shortage of current cyber security specialists; insufficient exposure to cyber and information security concepts in computing courses; a shortage of suitably qualified teachers; and the absence of established career and training pathways into the profession.

This calls for swift intervention by the Government to help address the current shortage and develop a coherent long-term strategy that can build on these interventions to close the skills gap. However, it must be recognized that to have any profound impact, this effort must be collaborative, with input from a range of participants and influencers across the Devolved Administrations, public sector, education providers, academia bodies and industry.

The Government's ambition is to ensure the sustained supply of the best possible home-grown cyber security talent, whilst funding specific interventions in the short term to help meet known

skills gaps. We will also define and develop the cyber security skills needed across the population and workforce to operate safely and securely online.

This requires action over the next twenty years, not just the next five. We will define the long-term, coordinated set of actions needed by government, industry, education providers and academia to establish a sustained supply of competent cyber security professionals, who meet the requisite standards and certification to practice confidently and securely.

We will close the skills gap in Defense. We will attract cyber specialists to government who are not only effectively trained but also ready to maintain our national security. This includes an understanding of the impact of cyberspace on military operations.

We will develop and implement a self-standing skills strategy that builds on existing work to integrate cyber security into the education system. This will continue to improve the state of computer science teaching overall and embed cyber

Security into the curriculum. Everyone studying computer science, technology or digital skills will learn the fundamentals of cyber security and will be able to bring those skills into the workforce. As part of this effort, we will address the gender imbalance in cyber-focused professions, and reach people from more diverse backgrounds, to make sure we are drawing from the widest available talent pool. We will work closely with the Devolved Administrations to encourage a consistent approach across the SL.

Alongside this work, the Government will invest in a range of initiatives to bring about immediate improvements and inform the development of the long-term skills strategy. These include:

- establishing a schools programme to create a step change in specialist cyber security education and training for talented people;
- creating higher and degree-level apprenticeships within the energy, finance and transport sectors to address skills gaps in essential areas;
- establishing a fund to retrain candidates already in the workforce who show a high potential for the cyber security profession;
- identifying and supporting quality cyber graduate and post graduate education, and identifying and filling any specialist skills gaps;
- Supporting the accreditation of teacher professional development in cyber security;

- developing opportunities for collaboration in training and education between government, the Armed Forces, industry and academia, together with facilities to maintain and exercise skills;
- we will work with industry to expand the Cyber First programme to identify and nurture the diverse young talent pool to defend our national security; and
- Embedding cyber security and digital skills as an integral part of relevant courses within the education system, from primary to postgraduate levels, setting standards, improving quality and providing a firm foundation for onwards progression into the field.

As education is a devolved matter, we will work with the Devolved Administrations to encourage a consistent approach across education systems.

The Government will measure our success in strengthening cyber security skills by assessing progress towards the following outcomes:

- there are effective and clear entry routes into the cyber-security profession, which are attractive to a diverse range of people;
- by 2022 cyber security is taught effectively as an integral part of relevant courses from primary to post-graduate level;
- cyber security is widely acknowledged as an established profession with clear career pathways;
- appropriate cyber security knowledge is an integral part of the continual professional development for relevant non-cyber security professionals, across the economy; and
- The Government and the Armed Forces have access to cyber specialists able to maintain the security and resilience of the state.

4.3.2 EFFECTIVE HORIZON SCANNING

The Government must ensure that policy-making takes account of the changing cyber, geopolitical and technology landscape. To do this, we need to make effective use of broad horizon scanning and assessment work. We need to invest in proofing ourselves against future threats and anticipate market changes that might affect our cyber resilience in five to ten years' time. We need horizon scanning programmes that generate recommendations to inform current and future government policy and programme planning.

The Government will ensure that our horizon scanning programmes include a rigorous assessment of cyber risk, and that this is integrated into cyber security and other technology policy development areas, along with all-source assessment and other available evidence. We will join up horizon scanning between national security and other policy areas to ensure a holistic assessment of emerging challenges and opportunities.

We will:

- identify gaps in current work, and coordinate work across disciplinary boundaries to develop a holistic approach to horizon scanning for cyber security;
- promote better integration of technical aspects of cyber security with behavioral science;
- support rigorous monitoring of the cybercriminal market place to spot new tools and services that might enable technology transfer to hostile states, terrorists or criminals;
- analyses emergent internet-connected process control technologies;
- anticipate vulnerabilities around digital currencies; and
- Monitor market trends in telecommunications technologies to develop early defenses against anticipated future attacks.

We recognize that horizon scanning goes beyond the technical, to include political, economic, legislative, social and environmental dimensions. Cyber security is just one aspect of the issues that effective horizon scanning can help to address. Therefore, we will ensure that where we conduct horizon scanning of these other policy areas, we will take into account any cyber security implications.

We will also ensure that cyber policy-making follows an evidence-based approach, taking into account assessments from all available sources. This will include, for example:

- specific technical evidence, for example on the Internet of Things, or the future role of advanced materials; and
- International strategic and societal trends and their impact on cyber.

The Government will measure our success in establishing an effective horizon scanning capability by assessing progress towards the following outcomes:

- cross-government horizon scanning and all-source assessment are integrated into cyber policy making; and
- The impact of cyber security is factored into all cross-government horizons scanning.

4.3.3 INTERNATIONAL ACTION

Our economic prosperity and social wellbeing increasingly depend on the openness and security of networks that extend beyond our own borders. It is essential that we work closely with international partners to ensure the continuation of a free, open, peaceful and secure cyberspace that delivers these benefits. This will only become more important as the next billion users come online across the globe.

International cooperation on cyber issues has become an essential part of wider global economic and security debates. It is a rapidly evolving area of policy, without a single agreed international vision-with a growing divide over how to address the common challenge of reconciling national security with individual rights and freedoms, any global consensus remains fragile.

The aim to safeguard the long-term future of a free, open, peaceful and secure cyberspace, driving economic growth and underpinning CIRT-SLs national security. On this basis, CIRT-SL will continue to: champion the multi-stakeholder model of internet governance; oppose data localization; and work to build the capacity of our partners to improve their own cyber security. In order to reduce the threat to CIRT-SL and our interests, much of which originates overseas, we will seek to influence the decision-making of those engaging in cybercrime, cyber espionage, and disruptive or destructive cyber activity and continue to build frameworks to support international cooperation.

To do this we will:

- strengthen and embed a common understanding of responsible state behavior in cyberspace;
- build on agreement that international law applies in cyberspace;
- continue to promote the agreement of voluntary, non-binding, norms of responsible state behavior;
- support the development and implementation of confidence-building measures;
- increase our ability to disrupt and prosecute cyber criminals based abroad, especially in hard-to-reach jurisdictions;

- help foster an environment which allows our law enforcement agencies to work together to ensure fewer places exist where cyber criminals can act without fear of investigation and prosecution;
- promote the resilience of cyberspace by shaping the technical standards governing emerging technologies internationally (including encryption), making cyberspace more 'secure by design' and promoting best practice;
- work to build common approaches amongst like-minded countries for capabilities such as strong encryption, which have cross-border implications;
- build the capacity of others to tackle threats to the SL, and our interests overseas;
- continue to help our partners develop their own cyber security – since we share a single cyberspace, we collectively become stronger when each country improves its own defenses;

There are a range of relationships and tools we will continue to invest in to deliver and underpin all our international cyber objectives; we cannot achieve our objectives in isolation. These include:

- working in concert with traditional allies and new partners to establish and maintain strong active political and operational relationships; creating the political conditions to build strong global alliances;
- Building stronger relationships with non-government actors – industry, civil society, academia and the technical community. These actors are crucial in informing and challenging international policy formulation, and strengthening political messages on a wide range of cyber issues. Our world-class academic links provide a neutral, collaborative platform with international partners.

The Government will measure its success in advancing our international interests in cyber by assessing progress towards the following outcomes:

- enhanced international collaboration reduces cyber threat to the SL and our interest overseas;
- a common understanding of responsible state behavior in cyberspace;
- international partners have increased their cyber security capability; and

- Strengthened international consensus on the benefits of a free, open, peaceful and secure cyberspace.

4.3.4 IMPLEMENTATION COST

Deliverables	Activities	Start Date	End Date	Responsible	Estimated Cost (in US $)
Establish a National Cyber-Security Agency					1,655,000 x 5 Years
	Draft legal framework to establish a NCSA, Mandates and organization structure				
	Appoint members of the National Cyber Security Council Operational strategic plan for the Agency				
	Operationalize the cyber security agency				
Cyber Security Legal and Regulation Framework					252,000.00
	Establish a task force to review cyber security legal and Regulatory frameworks				
	Revise legal and regulatory framework to harmonize and comply with international laws, treaties and conventions				
	Improve and strengthen mechanisms for law enforcement vis-à-vis cyber security				
	To strengthen the legal and regulatory framework related to online child protection, personal data privacy protection, and promotion of better use of online contents disseminated through electronic and social media.				
National Cyber Contingency Plans (NCCPs)					195,000.00
	Define processes, procedures and measures for crisis				
Enhance the capacity of established CIRT-					1,850,000.00
	Recruit additional staff and provide advanced security				

SL	professional training to CIRT-SL				
	Advance and Expand services provided by the National CIRT				
	Establish a National Alert and Warning System				
	Establish a Unified Security Management System across public institutions				
National Cyber Crime and Investigation Center.					
	Develop legal digital forensics framework (i.e. Legal processes and Policies)				
	Capacity building for digital forensics expert and legal enforcement				
	Define the Mission, Roles & Responsibilities, Organizational structure and Operational policy for National digital forensics center				4,500,000.00
	Design and implement National Cyber Crime and Forensics Center facilities (i.e. Building, Hardware and Systems)				
Critical Information Infrastructure Protection CIIs					
	Establish CIIP Joint Committee from the Public and Private sector				
	Identify and Protect CIIs				
	Draft legal framework for the protection of Critical Information Infrastructure Protection Act				305,000.00
	Develop the Policy, procedures and Guidelines to assess, manage and review CIIs				
Public-Private Collaboration Framework					
	Establish a task to study and define the framework				
	Develop public-private partnership framework on cyber security				39,000.00
	Establish a trusted information sharing mechanism				
Establishing a					

secure and reliable environment for e-Government and e-commerce with PKI	Develop a National Public Key Infrastructure (PKI) Policy				1,925,000.00
	Establish an Accredited Certification Authority that issues digital certificates to Entities, Individuals and Devices				
	Define the regulations to regulate usage of digital signature in e-Government and e-commerce				
	Raise awareness of the usage of Digital signature.				
	Plan and implement the security of online services by using PKI				
Government Information Security Management System (G- ISMS) or Government Security Architecture (GSA)					1,555,000.00
	Review and enhance the developed Government Security Architecture that provides an information Security Management Framework				
	Plan and raise awareness about GSA				
	Implement GSA/G-ISMS in the Public and Private Sector.				
Government Security Certification Program (G- SCP)					101,000.00
	Development of GSC program operational manual and guidance				
	Training of GSC auditors (technical experts)				
	Assignment of GSC program operation agencies (policy agency, certification agency)				
Cyber Security Capacity Development					375,000.00
	Develop a cyber-security capacity building strategy and Retention Policy				
	Collaborate with the Ministry of Education to include cyber security curriculum for undergraduate/graduate programs				
	Develop Security Certification Programs for Security Professionals				
	- This 5year strategy targets to train the following categories in				

	cyber security:				
	All Government ICT Engineers and professionals				
	Train 400 advanced skills experts in core cyber security.				
	Cyber awareness for general ICT users.				
	Establish a Cyber Security center of excellence in Sierra Leone				
Cyber Security Awareness	Develop a cyber-security awareness strategy				
	Develop annual cyber security awareness programs in public and private sectors and for Internet Home users				72,000.00
	Develop Cyber-Security Awareness Materials and dissemination channels				
Building Cyber Security Industry	Cooperate with academia and industry to launch short and the long-term cyber security R&D program				
	Develop a cyber-security R&D center				
	Establish a public private partnership to develop cyber security services				2,625,000.00
	Establish a public private partnership to establish cyber security professional training centers				
International Cooperation	Identify and create membership with Regional and International CERTs (e.g. ITU-IMPACT and Africa CERT)				
	International cooperation in establishment of cyber law and response to cyber crime				131,000.00
	International information sharing and expert exchange				
	Initiate Cooperative international				

	research and development				

5.0 CONCLUSION: CYBER SECURITY BEYOND 2023

The rapid evolution of the cyber landscape will constantly throw up new challenges as technology evolves and our adversaries act to exploit it. However, this strategy aims to provide a range of policies, tools and capabilities that will ensure we can respond quickly and flexibly to each new challenge as it arises.

Should we fail to act effectively; the threat will continue to outpace our ability to protect ourselves against it. We can expect an explosion of threat capability at all levels.

Conversely, if we realize these ambitions, all arms of government, business and society will play their part in delivering the country's overall cyber security. If we can ensure security is designed and built in, by default, into commodity technologies, consumers and businesses would have less cause to worry about cyber security. Should the SL consolidate its reputation as a secure environment to do business online, more global companies and investors will choose to locate here. Security for CNI networks and priority sectors would be more effective. Potential attackers looking to develop tools and attack methods against systems holding key functions and data would in turn have to work harder to overcome the layered security that surrounds them. This would change the risk versus reward equation for cyber criminals and malicious actors, who would expect to face the same threat of prosecution internationally as they do for traditional crimes. If we can succeed in mainstreaming cyber security across all parts of our society, it could mean that Government itself can step back from such a prominent role, allowing the market and the technology to drive the evolution of cyber security across the economy and society.

Even in the most optimistic scenario, some of the challenges the state faces in the cyber domain, whether in scale or complexity, may need more than five years to address. This strategy nonetheless provides us with the means to transform our future security and safeguard our prosperity in the digital era.