RSA NATIONAL CYBERSECURITY POLICY FRAMEWORK

1. OVERVIEW OF PRESENTATION

1. OUTLINE OF PPT
2. BACKGROUND
3. OBJECTIVES
4. CONCLUSION

2. BACKGROUND

- Dependencies on the internet, to govern, to conduct business and for other social purposes.
- Inherent sophisticated threats such as cybercrime, cyber terrorism, and cyber warfare and cyber espionage to the fore.
- Cyber attacks that target the infrastructure or economic wellbeing of a nation can reduce available state resources and undermine confidence in Government. Large scale cyber incidents have the potential to overwhelm Government as well as public and private sector resources and services, by disrupting the functioning of critical information systems.
- In light of these security challenges in cyberspace, South Africa adopted the National Cybersecurity Policy Framework (NCPF) in March 2012.
- The NCPF outlines broad policy guidelines on cybersecurity in the Republic and requires Government to develop detailed cybersecurity policies in line with the NCPF.

BACKGROUND

To counter cyber threats the RSA Government is committed to implementing a coherent and integrated cybersecurity approach which, amongst others, must:

- Promote a cyber-security culture and demand compliance with minimum security standards;
- Strengthen intelligence collection, investigation, prosecution and judicial processes, to prevent and address cybercrime, cyber espionage, cyber terrorism, cyber warfare and other cyber ills;
- Establish public-private partnerships for national and international action plans;
- Ensure the protection of national critical information infrastructure;
- Promote regional and international cooperation, and
- Promote and ensure a comprehensive legal framework governing cyberspace.

3. OBJECTIVES

To advance cybersecurity and national cyber interests through a Government-led coordinated approach.

To prevent and combat cybercrime

Traditional investigative methods are ineffective in addressing the detection, prevention, combating and investigation of cybercrime.

The policy therefore proposes a focused integrated and coordinated process in dealing with cybercrime

OBJECTIVES

To foster regional and international cooperation to address cybersecurity threats:

To advance South Africa’s position on the definition and elaboration of the global cybersecurity agenda in combating cybercrime and building confidence and trust in the secure use of ICT, it is proposed that South Africa participate in regional, African Union and international bodies The envisaged cooperation and collaboration amongst others is to take place through research and development, as well as through participation in international exercises.

OBJECTIVES

To advance National Critical Information Infrastructure (NCII) protection:

Sources of critical infrastructure now encompass systems of high economic value such as those that support electronic transactions, hold sensitive intellectual property such as biotechnology patents or other commercial data associated with major international trade negotiations, to name but a few.

These systems if rendered unavailable or compromised could result in a significant impact on South Africa's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security.

To establish a cyber warfare capacity:

The Department of Defence (DOD) has the overall responsibility for coordination, accountability and implementation of cyber defence measures within the Republic. To this end, the DOD will develop policies and strategies to address cyber defence nationally.

OBJECTIVES

To establish a secure online e-identity management system:

A secure online e-identity management system aims to maximise the effectiveness and interoperability of work across all levels of Government, to combat the misuse of stolen and assumed identities. The cybersecurity policy promotes the development of a holistic National E-Identity with authentication measures which will address the misuse of stolen and assumed identities.

Capacity building, Research and Development:

Cybersecurity challenges are constantly evolving it is thus crucial that there be continuous development of capabilities and requisite skills to address these challenges. This can be achieved through the coordination and prioritisation of cybersecurity Research and Development

OBJECTIVES

Training:

The goal of cybersecurity training is to improve the understanding, competence and skills among Government officials, the business community and citizens, with the ultimate aim being to create a strong appreciation of cyber usage know-how and cybersecurity among the relevant role players.

To promote Cybersecurity Awareness:

To attain a high level of cybersecurity, it is imperative that a comprehensive national awareness program be developed. This will be done through concerted cybersecurity literacy awareness and publicity campaigns.

OBJECTIVES

To foster Public-Private Partnerships:

The formalisation of public-private collaboration and partnerships will be addressed by the establishment of a Cybersecurity Hub under the auspices of the Department of Communications(DoC)

To develop and strengthen the legislative framework:

The development of a dynamic legislative framework subject to periodic review is necessary, to address constantly evolving cybersecurity challenges.

5. CONCLUSION

This policy presents measures proposed by Government to address challenges and opportunities brought to the fore by the dynamic nature of cyberspace.

Detailed additional policies and strategies will continuously be developed to address the challenges and opportunities presented by the use of ICT

It is envisaged this policy will be reviewed regularly to stay abreast of new technologies and new cyber threats

THANK YOU