Common Market for Eastern and Southern Africa

International Telecommunication Union

# ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia, 25-28 August 2008[1]

Document RFL/2008/WG01-E

28 August 2008

Original: English

## Working Group 1: Regional Approach for the Development of a National Cybersecurity Strategy

### Recommendations from the Ad Hoc Forum Working Group on a Regional Approach for the Development of a National Cybersecurity Strategy

There is a need for the development of a model national cybersecurity strategy for addressing cybersecurity at the national level. Such a strategy can serve as a coordinating mechanism for the region. Because existing national capabilities vary and threats constantly evolve, the strategy should provide a flexible approach that can assist the nations of the region to review and improve their existing institutions, policies, relationships, and capabilities for addressing cybersecurity. The strategy should support national and regional cybersecurity efforts, the national IT policy, other national and regional policy goals, and the principles of freedom of speech, free flow of information and due process of law.

The strategy should support a comprehensive national approach to cybersecurity and address actions required in key elements, including;

- Promoting a National Culture of Cybersecurity;
- Deterring Cybercrime;
- Creating National Incident Management Capabilities; and
- Establishing National Government–Industry Collaboration.

The strategy should be flexible and able to respond to the dynamic risk environment. It should be developed cooperatively through consultation with representatives of all relevant participant groups including government agencies, industry, academia, and relevant associations. And, it should contain a statement of purpose and operational and implementation provisions. Such provisions are outlined below:

1. Recognize the importance of information and communication technologies to the nation,

2. Recognize the necessity for cybersecurity and that security is a continuing process not a destination.

3. Create awareness at the national policy level and among all national stakeholders of the issues of cybersecurity and the need for national action and regional and international cooperation.

4. Justify the need for national action to address threats to and vulnerabilities of the national cyber infrastructure and call for policy-level discussions and actions to achieve the stated goals in this cybersecurity policy statement.

5. Highlight the need to participate in regional and international cybersecurity efforts.

6. Identify the risks faced, establish the cybersecurity policy goals, and identify how these goals can be implemented.

7. Delineate roles and responsibilities, identify priorities, and establish timeframes and metrics for implementation.

8. Identify a lead person and institution to coordinate the overall national effort as well as lead institutions and cooperating partners, for each element of the national strategy.

9. Determine the location, function and role of a national watch, warning and response coordinating operation.

[1] ITU Regional Cybersecurity Forum website: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/

10. Identify cooperative arrangements and establish mechanisms for cooperation among all participants and between government and the private sector.

11. Identify international and regional counterparts and foster international and regional efforts to address cybersecurity, including information sharing and assistance.

12. Call for the development of an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity.

13. Call for periodic reassessments of the national strategy and its implementation.

14. Establish or call for the establishment of priorities in national cybersecurity efforts.

15. Identify training requirements and how to achieve them.

16. Identify available resources, expertise and budget and funding requirements.

17. Call for an initial broad review of the adequacy of current national practices and consideration of the role of all stakeholders (government authorities, industry, and citizens) in the process.

18. Be promulgated at the level of head of government to encourage the cooperation of all participants.

19. Be adaptive and integrate state, local, and community-based approaches to national needs and contexts.

**********