

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection

Draft Common Understandings and Positions

**Hanoi, Vietnam
28-31 August 2007**

.....

Common Understandings and Positions

- The Workshop identified four common understandings and positions:
 - Need for National Framework(s)
 - Need for Capacity Building and Education/Awareness
 - Need for Enhanced Cooperation at Local, National, Regional and International Levels
 - Need for Technical Standards and Best Practices

Need for National Framework(s)

- Each country should take into consideration the development of a national framework for cybersecurity and critical information infrastructure protection (national framework) that includes, *inter alia*:
 - a national strategy;
 - adoption of appropriate legal frameworks including deterring cybercrime;
 - incident management;
 - government-private sector collaboration;
 - development of a culture of cybersecurity.

Need for National Framework(s)

- In order to achieve the development of a national framework, there is a need for high-level political support for the development of the national framework.
- Participants in the development of the national framework could include relevant ministries, government agencies, and a broad and diverse participation from the private sector, including business, other organizations, and individual users, each according to their relevant roles.

Need for Capacity Building and Education/Awareness

- Capacity building and education/awareness are required to support each participant in their respective responsibilities and roles.
- Each country and different stakeholders will have different needs, and will be at different levels. Therefore, the training and resources should be flexible enough to be adaptable to unique situations and needs of the country and its relevant participants.

Need for Enhanced Cooperation at Local, National, Regional and International Levels

- Enhanced cooperation will be needed both among participant groups, and across sectors; e.g. government and private sector; law enforcement and ISPs, etc., appropriate to their roles.
- Cooperative efforts will be dynamic, and will vary according to the circumstances.
 - For example, law enforcement and CSIRTS may require ongoing cooperative interaction in incident mediation and resolution.
 - ISPs and law enforcement may primarily interact around incident reporting and investigations. Other flexible interaction models may emerge.

Need for Enhanced Cooperation at Local, National, Regional and International Levels

- Efforts to educate all participants may occur on a more consistent and ongoing basis. Enhanced cooperation initiatives are needed at national, regional, and international levels, and will cross the full range of technical training, experience sharing, and incident investigation, cooperation in legal remedies, user awareness, and policy making.

Need for Technical Standards and Best Practices

- Development of appropriate technical standards and best practices is important to the successful implementation and operation of national strategies and will facilitate regional and international cooperation initiatives.

Need for Technical Standards and Best Practices

- There is a need for increasing awareness of existing and emerging technical standards from the broad set of relevant standards development organizations (SDOs) and best practice approaches in policy and procedures, which may include, *inter alia*, training in investigatory techniques, cyber space forensics, how to set up or manage a CSIRT, examples of successful user awareness programs, etc. be developed across all elements of the national framework.

Main Approaches and Activities

1. Design model examples for convening a national framework development process, including identifying potential categories of participants, outline of a national framework, etc.
2. Identify a core set of activities in the form of a 'check list' or model framework examples, that countries could use to self assess their cyber security readiness, and identify areas for enhancement;

Main Approaches and Activities cont'd

3. Facilitate information sharing, knowledge and know-how transfer among countries, both governmental and private sector, ISPs, appropriate intergovernmental entities, etc.
4. Facilitate interactions with and among experts and expert entities from relevant areas identified in the national framework, such as legal, technical, etc.

Main Approaches and Activities cont'd

5. Develop resources that provide examples of best practices, training and education opportunities, including:
 - Identify relevant standards; and publish user friendly guides with translation and easy to use descriptions of how to implement standards and best practices
 - Take consideration of ITU Resolution 123 (Rev. Antalya, 2006) relating to "Bridging the standardization gap between developing and developed countries".
 - Such efforts should include ITU-T SG 17, ITU-T SG 13, and other relevant Standards Development Organizations (SDOs), such as W3C and IETF, regarding relevant and applicable standards

Main Approaches and Activities cont'd

6. Develop models of capacity building resources that can be adapted to a country's needs.
7. Balance is needed between diversification, competition, and coordination on activities undertaken by various stakeholders. Maximizing benefits and making best use of limited resources should be a key goal.



International Telecommunication Union

Helping the World Communicate