Building Cybersecurity Capacity:

Overview of *Best Practices for Cybersecurity*

Workshop on Cybersecurity
International Telecommunication Union

September 17, 2007

Daniel C. Hurley, Jr.
Director, Critical Infrastructure Protection

U.S. Department of Commerce

An Approach

- Based on shared experiences
- Involves two-way flow of information
- Report on *Best Practices for Cybersecurity* can help to analyze issues, assess progress, and organize a national strategy
- Useful tools to help build capacity, e.g., *Self-Assessment*
- *Framework for National Cybersecurity Efforts* – quick summary

Perspectives

- High-level management/policy
- Already in progress; no country starting from zero
- No country has completed the journey
- Each country tailors approach to its unique needs and circumstances
- Part of assessment and re-evaluation process

Best Practices for Cybersecurity

- Structure
  - **A. Goals**
  - **B. Specific Steps** to Achieve Goals
  - **C. References** Relate to Specific Steps
    - Cited references can serve as core material for focused workshops

- "Living Document"
  - References evolve as updated or new sources appear
  - Helps place new issues in context

Best Practices for Cybersecurity

I. National Strategy for Cybersecurity
II. Government-Industry Collaboration
III. Deterring Cybercrime
IV. National Incident Management Capabilities
V. National Culture of Cybersecurity

National Strategy

- Create awareness at national policy level about need for national action and international cooperation on cybersecurity
- Identify roles, responsibilities, linkages and cooperative arrangements necessary for cybersecurity
- Highlight need for international cooperation to achieve national success

Government-Industry Collaboration

- Develop government-industry partnerships to effectively manage cyber risk

- Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to enhance cybersecurity at a national level

Deterring Cybercrime

- Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with the provisions of the Convention on Cybercrime (2001)

Incident Management Capabilities

- Develop a national cyberspace security response system to prevent, predict, detect, respond to, and recover from cyber incidents.
  - Watch, Warning, Response & Recovery

- Develop a national cyberspace incident management program in coordination with the intelligence and law enforcement communities.

- Participate in watch, warning, and incident response information sharing mechanisms.

Promoting a National Culture of Cybersecurity

- Promote a national culture of cybersecurity consistent with UNGA Resolutions
  - 57/239, *Creation of a global culture of cybersecurity*
  - 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*

Appendices and Annexes

- Appendices
  - 1. List of Acronyms
  - 2. Implementation Strategy and Performance Metrics

- Annexes
  - A. Case Studies (Technical and Countries)
  - B. Identity Management

Next Steps

- International Telecommunication Union, Development Bureau
  - Follow-up to Workshop on *Best Practices for Cybersecurity* and SG1 meetings
- Organization of American States
  - Using *Framework* in *Handbook to Improve Cybersecurity*
  - Will use *Framework* and *Best Practices* in future

Thank You

Questions?

»

U.S. Department of Commerce
www.ntia.doc.gov
dhurley@ntia.doc.gov