#

# Chief Executive Board

# Briefing Note on Cybersecurity:

# UNDP Position

**Background**

At its 17-18 October 2013 meeting, the CEB endorsed the paper “Towards a UN-wide framework on Cybersecurity and Cybercrime.” The CEB agreed to form a Steering Group on Cybersecurity and Cybercrime consisting of the Executive Heads of UNDP, UNESCO, UNODC, UNEP and ITU and the Chairs of HLCP, HLCM and UNDP.  A support group of SMEs for the Steering Group has also been formed with Paul Raines, BOM, and Raul Zambrano, BDP, representing UNDP.

The next conference call of the CEB will be 20 March 2014.

# Comments

The CEB discussion on cybersecurity and cybercrime will be framed by the following five questions. At the recent conference call of the support group of 3 March, it was suggested that **UNDP could lead on questions Q2 and Q3 below**.

The UNDP position is provided *in italics* after each question:

1. **How can the system ensure effective internal preparation against cyber threats, among agencies and across the UN system, including policy obstacles may prevent agencies from acting together to jointly protect the UN system better through, for example, the inclusion of cyber security in risk assessment and risk management frameworks?**

*The ICT Network and the HLCM have endorsed the creation of a UN system-wide computer security incident response team (CSIRT) that would provide cyber-incident handling and coordination on behalf of the participating UN agencies. The UNDP CISO, Paul Raines, is chairing the working group of UN agency CISOs that will provide the road map for the creation of this group. The CSIRT is envisaged to provide Information security incident response and technical assistance, cyber security awareness information to the UN System and keep executive UN management informed through regular reports of threats, incidents and the adequacy of defense measures. The road map is currently being considered for endorsement by the ICT Network.*

1. **How can agencies better integrate and mainstream cyber security and counter cyber-threats as part of programme planning and, in particular, the post-2015 development agenda?**

*UNDP is well positioned to put forth a vision for including cybersecurity as a cross-cutting issue for both development programming and the post-2015 development goals. UNDP has been a pioneer in the use of ICTs as enablers for development and thus has considerable experience and knowledge here. By the end of 2013, UNDP supporting close to 100 programme countries with over 220 ICT for Development and e-governance projects to the tune of 220 million USD. Many of these programmes however are not factoring in cybersecurity issues for a wide variety of reasons ranging from basic awareness to lack of local capacities to effectively address the new challenges. UNDP's approach to mainstream cybersecurity into developing programming should be one of integrating the issue into key development programmes and goals -and not one that ends up adding new priorities to already crowded and seemingly competitive development agendas. UNDP should also take a human rights based approach to the issue to foster a proper balance between security and privacy and ensure people are at the center of the issue.*

*In this light, the areas where assistance could be provided by UNDP include: 1) assisting in national policies and regulations that advance cybersecurity including national strategies for key assets and an enabling environment for e-commerce and data protection, among others; 2) enhancing local capacities to ensure policies and regulations are effectively implemented while increasing both awareness on the issue and cross-country cooperation; 3) building a network of experts to provide technical expertise and advise on the issue based on local contexts and local needs; 4) linking cybersecurity issues to overall development agendas and goals at the local level to mainstream the issue at the national level; 5) promoting a multi-stakeholder approach where all sectors and actors are part of the process and the governance of national ICT assets is transparent; and 6) bringing forward a human rights approach to cybesecurity to ensure that security is not at odds with privacy and the protection of people's fundamental rights, including online freedom.*

*These areas fall within three of UNDP’s core areas of work: 1) crisis prevention and recovery; 2) building democratic societies and 3) growing national capacities.*

1. **How can agencies of the system ensure coherence and coordination in its assistance to Member States and avoid duplication of efforts?**

*This question should be best handled through the UNDG in order to ensure coherence and cooperation amongst the various agencies providing programmatic assistance.* ***UNDP should advocate for being the executive lead in providing cybersecurity advisory services to developing nations as part of our mandate to prevent conflict, foster democratic societies and enhance national capacities.***

1. **How can agencies facilitate discussions with member states that ensure that the international community arrives at a common understanding of, and takes action on, the need for a comprehensive and inclusive international framework for cooperation in the field of cyber security?**

*The UN system should facilitate conferences with member states to raise awareness, promote a common understanding and, if necessary, take joint action on issues to prevent and deter cybercrime. The ITU should be designated as the lead UN agency for this effort.*

1. **When conducting their work, how can agencies balance the need for privacy and confidentiality with the transparency that stakeholders demand?**

*By taking a human rights based approach to development, UNDP could be a major contributor here. UNDP has already taken a leading role in promoting transparency through the IATI initiative. Increased transparency, however, is not inherently at odds with privacy and confidentiality. Instead, the focus should be on being transparent with the information that donors and member states demand, whilst protecting the agency sensitive information that might cause financial, productivity and reputational loss or jeopardize the safety and security of its employees.*