

|  |  |  |
| --- | --- | --- |
| C:\Users\lattion\AppData\Local\Microsoft\Windows\INetCache\Content.Word\DCAF_Blue.jpg |  |  |

**National Cybersecurity Strategy Workshop**

**For Europe on National Cybersecurity Strategies**

*26-28 June*

*Skopje, Republic of North Macedonia*

**TERM OF REFERENCE AND AGENDA**

**TABLE OF CONTENTS**

[1 INTRODUCTION 3](#_Toc10820974)

[2 Scope 3](#_Toc10820975)

[3 Methodology 4](#_Toc10820976)

[4 Who should ATTEND? 4](#_Toc10820977)

[5 Logistics 5](#_Toc10820978)

[6 agenda 6](#_Toc10820979)

# INTRODUCTION

At the national level, cybersecurity is a shared responsibility that requires coordinated action for prevention, preparation, response, and incident recovery on the part of government authorities, the private sector and civil society. For smooth operation and to ensure a safe, secure and resilient digital realm, a comprehensive framework or strategy is necessary, which for maximum effectiveness, has to be developed, implemented and executed with a multi-stakeholder approach. While many countries have such a framework or National Cybersecurity Strategy in place, many others do not.

The [Guide to Developing a National Cybersecurity Strategy](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf) was developed to help countries to create an effective national cybersecurity framework to protect their socio-economic development from cyber threats.

The Guide focuses on protecting civilian aspects of cyberspace. It is a comprehensive resource developed through a multi-stakeholder effort involving 12 partners[[1]](#footnote-2) from the public and private sectors: intergovernmental and international organizations, private sector, academia and civil society.

It gives countries a clear understanding of the purpose and content of a national cybersecurity strategy as well as providing actionable guidance for how to develop or improve their own. It contains a set of principles and good practices on the development, establishment and implementation of national cybersecurity strategies. It includes relevant models, references and resources as well as an overview of available assistance from a wide variety of organizations.

# Scope

The mission will be carried out from **26-28 June 2019** excluding travel dates. The ITU experts, in cooperation with the national counterparts of Western Balkan economies and in close collaboration with the relevant Ministries of the respective countries, will undertake the following activities on-site and off-site for Western Balkan economies:

1. Study and analyses the country’s current cybersecurity status and needs. Information will be gathered by the ITU Global Cybersecurity Index, as well as public sources. This activity will be done mainly off-site.
2. Study institutional and organizational requirements, and arrangements for developing a comprehensive National Cybersecurity Strategy.
3. Undertake a series of interactions and discussions with the relevant stakeholders to assess the level of readiness and the current situation at the national level. This activity will be performed mainly on-site.
4. Conduct training to impart the necessary knowledge on key concepts surrounding National Cybersecurity such as its development and production, as well as its implementation and long-term sustainability
5. Produce an assessment report as the main outcomes of the overall set of activities containing the key findings of the visit and provide recommendations of the way forward for the establishment of the National Cybersecurity Strategy.

# Methodology

The team assigned to carry out this exercise are knowledgeable in the field of cybersecurity, and in the use of the applicable international standards and best practices involved.

The ITU team will start its on-site activities with a brief opening meeting to review this “Assessment Plan” and confirm the on-site schedule. If necessary, this plan can be adjusted to suit the actual availability of the officials who will participate in the assessment. Following this meeting the team will undertake a brief tour of getting to know the area and other relevant personnel before starting the assessment process. The team will work together most of the time but may occasionally undertake short assessment sessions individually when this is required.

These findings will be recorded on a confidential checklist prepared by the team. The assessment methods will be meetings, trainings, interview sessions, and one-to-one or one-too-many discussions. A verbal report will be provided at the closing meeting to acquaint the officials with the findings and to offer preliminary recommendations.

# Who should ATTEND?

A National Cybersecurity Strategy is expected to provide a high-level understanding of the strategic direction that the concerned country is taking on cybersecurity, highlighting the main areas to be covered, to be then articulated in detail through an action plan.

Such plan must be implemented in close cooperation with other bodies within the country, work with relevant governmental agencies as well as interact with non-governmental entities.

It is therefore important to meet with key stakeholders to achieve initial consensus on the expectations, and the overall strategic direction.

Who should attend?

1. Representatives from relevant Ministries
2. Policy makers (parliamentarians)
3. Judiciary system
4. Regulatory bodies
5. National security agencies
6. Military establishment (the units in charge of information security and/or IT and ICT management)
7. Law enforcement agencies
8. Critical infrastructure providers (Water, Energy, Transport, etc.)
9. Central monetary agency and banks (most relevant public and commercial)
10. Telco’s and ISPs
11. Academia and national research bodies
12. Local industry (private sector) involved in security initiatives

The profile of the participants must be technical (staff that is dealing on their daily job with security, or at least with ICT and ICT networks). It is also important to engage managerial level staff, who are in charge of taking decisions.

On the policy making side, attendance should be ensured by officials in charge of drafting ICT national policies and strategies (including from the legislative perspective) as well as the representative of the entities in charge of implementation of such policies, legal frameworks and regulations.

One, maximum two representatives from each organization filling the above indicated profile should be present. If more representative are appointed, they are welcome to attend and contribute to the discussions.

For a regional workshop, it is understandable that less representatives may be expected as the travel and accommodation costs of all need to be considered.

# Logistics

Listed below are items that are required to be made available on-site to the ITU team to complete the mission successfully. The organizing team shall be responsible to make the items available.

1. Conducive training / seminar room [with desks]
2. Broadband Internet connectivity
3. LCD Projector
4. Projector screen
5. White board
6. Marker pens (multiple colors)
7. Printer
8. Sufficient power to connect laptops

# agenda

**Wednesday 26 June**

|  |  |
| --- | --- |
| [08:30 – 09:00] | Registration |
| [09:00– 09:15] | **Opening Ceremony**  **H.E. Damjan Manchevski,** Minister of Information Society and Administration, North Macedonia  **H.E. Ionut Andrei,** State Secretary, Ministry of Communication and Information Society, on behalf of Romanian Presidency in the Council of European Union, EU  **Mr. Marco Obiso,** Head of ICT Applications and Cybersecurity Division International Telecommunication Union, ITU  **Mr. Milan Sekuloski,** Senior Adviser, Europe and Central Asia - Geneva Centre for Security Sector Governance, DCAF |
| [09:15 – 09:30] | Group Photo |
| [09:30 – 09:50] | **Introductory session**   * Introduction of the ITU team and the participants * Short introduction to the Assessment Exercise - Methodology, Objectives, Outcomes |
| [09:50 –10:30] | **Training Session**  Common principles on National Strategies (what it is, mission, vision, etc) |
| [10:30 – 11:15] | **Presentation of the background research report - DCAF** |
| [11:15 – 11:30] | Coffee Break |
| [11:30 – 12:30] | **Assessment session - Lifecycle of National Cybersecurity Strategy**  Introductory presentation   * Phase I – Initiation * Phase II – Stocktaking and analysis * Phase III – Production of the National Cybersecurity Strategy * Phase IV – Implementation * Phase V – Monitoring and Evaluation |
| [12:30 – 13:00] | **Sharing session**  Sharing experiences from participants – DCAF coordinates |
| [13:00 – 14:30] | Lunch Break |
| [14:30 – 16:00] | **Hands-on exercise**   * Establishment of a governance structure to develop/maintain NCS. How to undertake stocktaking - ITU |
| [16:00 – 16:15] | Coffee Break |
| [16:15 – 17:00] | **Debrief and next steps for second day** |

**Thursday 27 June**

|  |  |
| --- | --- |
| [09:00 – 09:15] | Summary of Day 1 - Lifecycle of National Cybersecurity Strategy |
| [09:15 – 10:45] | **Hands-on exercise**   * NCS implementation - Establishment of an action plan - Deloitte |
| [10:45 – 11:00] | **Debrief** |
| [11:10 – 11:15] | Coffee Break |
| [11:15 – 12:45] | **Hands-on exercise**   * Monitoring and evaluation - How to monitor implementation, understanding gaps and apply corrective measures - DCAF |
| [12:45 – 13:00] | **Debrief** |
| [13:00 – 14:30] | Lunch berak |
| [14:30 – 15:30] | **Assessment session – Overarching principles**  Introductory presentation   * Vision * Inclusiveness * Fundamental human rights * Appropriate set of policy Instruments |
| [15:30 – 16:00] | **Sharing session**  Experiences from participants - DCAF |
| [16:00 – 16:15] | Coffee break |
| [16:15 – 17:15] | **Hands-on exercise** ITU, Deloitte, DCAF   * Vision * Inclusiveness * Fundamental human rights * Appropriate set of policy Instruments |
| [17:15 – 17:30] | **Debrief** |

**Friday 28 June**

|  |  |
| --- | --- |
| [09:30 – 10:30] | Assessment Session - National Cybersecurity Strategy Good practices   * Focus area 1 – Governance * Focus area 2 – Risk management in National cybersecurity * Focus area 3 – Preparedness and resilience * Focus area 4 – Critical infrastructure services and essential services * Focus area 5 – Capability and capacity building and awareness raising * Focus area 6 – Legislation and regulation * Focus area 7 – International cooperation |
| [10:30 – 11:00] | **Sharing session**  Experiences from participants |
| [11:00 – 11:15] | Coffee Break |
| [11:15 – 12:30] | **Hands-on exercise**   * Reflecting the good practises into the NCS text – Identyfing the key areas - Deloitte |
| [12:30 – 12:45] | **Debrief** |
| [12:45 – 14:00] | Lunch break |
| [14:00 – 15:30] | **Hands-on exercise**   * Focus areas - Deloitte |
| [15:30 – 15:45] | **Debrief** |
| [15:45 – 16:00] | Coffee Break |
| [16:00 – 17:30] | **Hands-on exercise**   * Focus areas - Deloitte |
| [17:30 – 18:00] | **Debrief and closing** |

1. Commonwealth Secretariat (ComSec), Commonwealth Telecommunications Organisation (CTO), Deloitte, the Geneva Centre for Security Policy (GCSP), the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, the International Telecommunication Union (ITU), Microsoft, the NATO Cooperative Cyber Defence Centre Of Excellence (NATO CCD COE), the Potomac Institute for Policy Studies, RAND Europe, The World Bank and the United Nations Conference on Trade and Development (UNCTAD). [↑](#footnote-ref-2)