|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 15 February 2024 |
| **Ref:****Contact:**  | **TSB Circular 180****Vijay Mauree** | **To:**- Administrations of Member States of the Union- ITU-T Sector Members- ITU-T Associates- ITU Academia |
| **Tel:** | +41 22 730 5591 |
| **Fax:** | +41 22 730 5853 |
| **E-mail:** | tsbevents@itu.int | **Copy to:**- The Chairs and Vice-Chairs ofITU-T Study Groups;- The Director of the Telecommunication Development Bureau;- The Director of the Radiocommunication Bureau;- The Director of the ITU Regional Office for Asia Pacific Region |
| **Subject:** | **Regional Digital Financial Services (DFS) Security Clinic for Asia Pacific Region(24-25 April 2024, Seoul, Republic of Korea)** |

Dear Sir/Madam,

1 I am pleased to inform you that the International Telecommunication Union (ITU) is organizing a **Regional Digital Financial Services Security Clinic for Asia Pacific Region** on the **24-25 April 2024** at The Koreana Hotel in Seoul, Republic of Korea. The event is being held jointly with FNSV Korea and the Fintech Centre of Korea. Remote participation will be provided for this event.

2 People in Africa, Asia, and Latin America, and elsewhere are leapfrogging traditional brick-and-mortar banking in favour of mobile payments and other digital financial services. In recent years, regulators and financial sector supervisors have become increasingly aware that financial services aimed to address financial inclusion (FI) challenges around the world are becoming vulnerable to cyber threats, primarily due to the increasing role of digital services (including mobile and other technologies) in the delivery of financial services. As financial services become increasingly digitized, the volume of sensitive digital data grows exponentially and with it, the potential for personal and system impacts of data breaches. As such, the need for safeguards from cybersecurity threats to this data becomes increasingly important. The event is in line with the ITU Plenipotentiary Resolution 204 and [WTSA Resolution 89](https://www.itu.int/pub/T-RES-T.89-2022) that propose the use of ICTs to bridge the gap in financial inclusion.

3 The objectives of the workshop include:

* Providing a comprehensive overview of the security threats to fintech and digital financial inclusion;
* Identifying technical and organizational security and risk management best practices to mitigate the identified threats which are in the ITU DFS Security Recommendations;
* showcasing the [ITU digital financial services (DFS) security lab](https://www.itu.int/en/ITU-T/dfs/seclab/Pages/default.aspx) and the practical guidance provided to developing countries for digital financial services security;
* exploring the ITU Cyber resilience assessment toolkit so regulators can self assess the cyber resilience of critical infrastructure for digital financial services; and
* providing a platform for cybersecurity experts from the region to share lessons learned in fintech security, cyber resilience and coordination in response to safeguard critical infrastructure and respond to emerging threats in the fintech landscape.

4 The DFS Security Clinic is targeted at representatives from telecommunications regulators, national cybersecurity agencies, Central Banks, Financial Service Providers, Banks, ministries, service and IT security solution providers, Strong Authentication vendors, academia, R&D institutions and other organizations working on matters related to fintech security and digital financial inclusion. Participation is free of charge and is open to all stakeholders from ITU Member States, Sector Members, Associates and Academic Institutions and to any individual from a country that is a member of ITU who wishes to contribute to the work. Participation is free of charge and open to all. No fellowships will be granted for the Workshop.

5 All relevant Information pertaining to the Workshop including the draft programme will be made available on the event website here:
<https://www.itu.int/en/ITU-T/webinars/dfs/sc/20240424/Pages/default.aspx>

The event webpage will be updated regularly as more information becomes available. Participants are encouraged to check the webpage periodically for updates.

6 Registration is mandatory for all participants planning to attend the workshop. You are invited to complete the online registration form at: <https://www.itu.int/net4/CRM/xreg/web/Registration.aspx?Event=C-00013754>

as soon as possible. **Early registration is encouraged for onsite attendance** and due to limited capacity at the event’s venue, **registration for on-site attendance** is requested to be completed by **14 April 2024 at the latest**.Please note that pre-registration of participants for our events is carried out exclusively online.

7 I would remind you that citizens of some countries are required to obtain a visa to enter and spend any time in Republic of Korea. The visa must be obtained from the office (embassy or consulate) representing Republic of Korea in your country or, if there is no such office in your country, from the one that is closest to the country of departure. Visa processing and approval may take some time, it is therefore suggested to check directly with the appropriate representation and apply early. Additional information on visa requirements is available on the event website under the section “**Practical Information”**.

We look forward to your valuable participation and contributions.

Yours faithfully,

Seizo Onoe
Director of Telecommunication
Standardization Bureau