WSIS
High Level Policy Sessions
March 23, 2021
9:00 AM CT

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
800-825-5234
www.captionfirst.com

***

This text is being provided in a realtime format. Communication Access Realtime Translation (CART) or captioning are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***

>> NINO: Good afternoon.
We would welcome and thank the participants who join us today for the high-level policy session number five on building confidence and the security for use of ICT.
We would like to play a short video.
>> The WSIS 2021 is off to a start.
As well as receiving a record number of submissions for the WSIS prizes with 1270 projects submitted.
You have until March 31st.
As the forum progresses, we encourage Stakeholders to keep an eye out for exciting workshops and ICT for development related special tracks.
Many of which have been inaugurated successfully.
The ICTs happiness track as well as ICTs and accessibility for persons with disabilities and Pacific needs track.
While many tracks have already begun, many exciting tracks have yet to open such as the opening of the high-level track opening the 22nd of March which will feature the WSIS forum chairman.
The policy sessions featured will be moderated by high level facilitators during the open consultation process.
Will gather over 100 high-ranking officials.

With over 35 ministers, deputies, ambassadors and 30 heads of regulatory bodies, private sector, civil society and the technical community.
Many other tracks will open soon.
All of which you can find more information about on our interactive agenda and web site.
In addition, on the title of this year's forum, we're hosting workshops where Stakeholders demonstrate how they are using ICTs to fight back against the Coronavirus pandemic.
The work of our Stakeholders will be displayed that was inaugurated on March 15th.
Various other networking and social events will be integrated with meet and greet opportunities and frequent social media posts and engagements.
In addition, registration for the aging better with ICTs hack-a-thon is now open with more than 650 registrants participating.
In addition to the exciting hack-a-thon, the special track will be initiating a special prize this year entitled the WSIS healthy aging innovation prize.
And we encourage you to submit related projects to this exceptional prize.
We look forward to your participation and thank Stakeholders for contribution in shaping with on-going support.
We received more than 500 inputs and suggestions to shape the agenda and program for the 2021 during virtual discussions and to the open consultation process.
Well balanced contributions.
Which is shown the positive commitment and the strengthening of the activities to achieve the sustainable development goals.
And a warm thank you to our partners without whom this forum would not be possible.
Thank you and we look forward to successful 2021 WSIS forum.
>> NINO: Thank you.
And welcome, again, for those that have just connected to this high-level policy session number five entitled confidence and the use of the session.
I'm NinO, president of the Italian association of management and coordinator for the data movement for the Emea region as well as researcher of the institution of technology.
And will moderate this session.
This session is mainly about trust.
And as we are in a digital age, trust is everything.
And cyber security is playing a crucial role and equitable access to connectivity.

We all know that use of information and communication technologies has many benefits such as enabling better management, better decision making, increasing productivity.
This also generates recent threat.
Cyber threat are growing concern.
And this pose a challenge for the incidents can compromise the availability and information.
And in addition to this, it is vital to announce cyber security culture.
This is what we are doing today to see what people in different part of the world are addressing the challenge.
So before we proceed, please let me share guidance for the way we will run the session today.
And the first one will have five minutes to address two questions we will pose to them.
And we will then have our Q and A moment at the end of the session if time permits.
And include your question into the tab.
During this, the microphones will be muted and sessions will be recorded as well as real time human captioning is available as well as the session being broadcast live.
I would now like to invite the director of the communication for opening remarks.
>> Dr. LEE: Thank you very much.
Colleagues and friends, welcome you to this WSIS 2021.
I hope all of you and your family in good health and good spirit.
It is my great honor and pleasure to welcome you to this session discussing about where we stand in our world to build confidence and security in the user.
Highlighted the critical importance of our digital infrastructure.
And the need to continue investing in our future.
ICTs have been an essential tool for daily life.
And the key helping services prevent cases.
Daily life will become dependent on remote collaboration tools.
So enabling access to education systems.
Healthcare and goods and services.
So now it's impossible without this ICT tools.
But this requires the people who need assistance.
So many devices and remote tools have a very good capabilities.
And all sectors looking to make smarter user data, this raises important questions around data processing and management.
Building trust and safety.
With large parts of social and economic activity.
Building confidence and the security in the user.
So build the confidence.

Cuts across all areas.
Incorporating the state of art in the security and privacy.
And creating a more sophisticated concept in relationships and the people they sought.
Topics of fast growing relevance to our security will include the services, transport systems, technologies such as block chain and confirmation technologies.
Entering new space with associated convergence in the responsibilities of different regulated authorities.
So we are all looking to protect the data and protect our customers and communities.
So inclusive standardization processes.
Digital transformation for energy and transportation for healthcare, since services and cities.
The pandemic highlighted ensuring all citizens and governments are able to benefit from these transformations.
So working together, we are reinforcing the new partnerships that will be essential to the year 2030 for the sustainable development.
The alliance -- so UN multi Stakeholder process that does global partnership to achieve the full potential for development.
The section lines are key framework for the collaboration required to achieve the SDGs.
So the question raised by the pandemic asking us how we plan to live together as an inter connected global society.
This session is fortunate to welcome an excellent panelists deeply invested in this debate.
How could we best work together to ensure that our inter connections help us to connect for each other better and be the better future for all.
So I look forward to hearing, learning this.
Thank you very much.
All the best for this session.
>> NINO: Thank you for your opening remarks.
Very insightful.
And I would like to welcome Mr. Preetam Maloor.
The floor is yours.
>> PR EETAM MALOOR: Thank you for the inspiring words.
Thank you for the opportunity.
I'm the technologies division of the ITU and focal point.
So in its role as action line facilitator, works hard to bring different Stakeholders together to forge meaningful partnerships.
The issue of security and trust challenges within ICTs.
And at this year's forum given the importance of the topic, we've organized a special cyber security track and in this

track, various sessions have been organized by Stakeholders as well as the secretariate.
And the issue of trust is in several other -- such as the one on imaging technologies for sustainable development.
Youth and children.
And several others.
The cyber security track started this year with the second open consultations on the global cyber security agenda which was held on March 1st.
And just to give you some background, the activities on cyber security organized around the five pillars of the framework which aims to advance the corporation on cyber security.
All the past year, we remarked on an exercise to draft guidelines for utilization of the ICU.
So also next month as part of the business forum, IT will launch the global cyber security index which is a market Stakeholder led by 2015.
Which has emerged from the commitment of countries to cyber security.
We have high level dialogues such as AI, quantum, smart sustainable cities and many others.
These are areas where ITU is very active in several streams of work going on.
And, again, security and many of these discussions.
So ready to take advantage of the conversations happening on security and trust in this 2021 edition.
And looking forward to your active engagement.
Thank you very much.
>> NINO: Thank you.
We will now start with the panelists.
We will kick off with five minutes of your statement which will be broadcast in Portuguese with English subtitle.
And new technologies.
What we ask was to respond to a couple of questions and to address his perspective of the main opportunity and challenges to the digital transformation on the society globally.
As well as which international initiative were considered important to help people to trust in technology.
We opened this session speaking about trust.
This is what we are going to look at this video.
[Video] [English captioning provided].
>> NINO: Now I will invite minister of public administration from the approved public of Slovenia.
More about the president's priorities in the cyber security.
The floor is yours, minister.
>> Thanks to the organizers for this important event on trust for the use of ICT.

We have seen the COVID-19 crisis has accelerated and at the same time exposed some short comings and risks of digital infrastructure.
We should be aware that country's economic and social well being democracy depend largely on how well the country can protect against cyber attacks.
Therefore, cyber security as part of strengthening resilience is one of the main priorities in the second half of this year.
Our goals are firstly to better harmonize minimal cyber security standards across the union.
Secondly, to strengthen our resilience to large scale cyber security with appropriate action plans and enhance cooperation, better information sharing and trust among new member states and other countries.
Now, how will we achieve this?
By join cyber unit which will facilitate information sharing and cyber crisis management across different areas and Stakeholders.
By the revision of the directive that will assure high level of standards.
Also, we will strive to further implement the toolbox.
Further more, will enhance cyber security corporation with countries in particular with the western region where our focus will be on cyber capacity building.
All these issues will be discussed at the international conference on cyber security that we will organize during our presidency in September this year.
Regarding the global international developments in the area of cyber security, I believe Slovenia is a reliable partner member of the United Nations organization for security cooperation in Europe and many other international and regional forums.
We have a very long tradition of technical capabilities responding to cyber incidents.
Our natural computer response team is currently chairing the use net for the overall 18 months of presidency.
The team has been very active in the cyber capacity building in the western -- and being NATO member and response to cyber incidents.
We have developed our policy and legal framework, set up our organizational structure, engaged in joint training and build necessary capacities.
Of course, the work is never not done.
It is a continuous process which requires permanent engagement at all levels, political commitment and closed for cooperation with others.
We will further strive to ensure the cyber space is governed with the full respect for the existing international law, particularly the UN charter, international humanitarian law.

As the up coming presidency, we will definitely do our best to ensure safe and efficient digital transformation for the union.
Thank you for attention.
>> NINO: Thank you, minister.
And with your up coming presidency from the 1st of July.
Thank you for your work.
Very assuring.
We move to the honorable Wilfredo Gonzalez.
If you would like to share with us consideration on how to be confidence and security in the use of the ITC and how it can contribute to the information society.
And given also the current pandemic, we know the current situation as global affected all of us, would be interesting if you can share what is Cuba doing to mitigate the affects of COVID-19.
And the speech will be in Spanish and we will have subtitle in English.
So people can follow.
Thank you.
>> Thank you for everyone.
Good afternoon.
I would like to introduce -- thank you for the support and thank you for speaking in Spanish.
Much better for me.
Thank you.
[Speaking in non-English language] [English language on screen].
>> NINO: Thank you.
And interesting to hear the parallels in between land security and cyber security.
So there's a community and need to ensure rights.
Thank you for your intervention.
Next is Mr. George Michaelidas.
To whom I would like to ask how the government ensure the safety and security of their citizens and as well as the business is more medium business when it comes to the use.
And when they are speaking about the citizens themself, how we can help the confidence on the use on the secure use on a daily basis of the IT infrastructure.
>> Well, thank you very much.
I would like to congratulate ITU for organizing such an important and interesting event.
It's a great deal that should be done given the rapid deployment of an extremely wide rain building of services that can be found in every aspect of our daily lives.
I would say there are five important elements that need to exist in the state level in order to secure environment.

This should have a holistic approach.
We have followed the holistic approach to cyber security at the national level since 2012.
The second important which, of course, should be part of the national strategy is the protection of the critical infrastructures.
It will create an issue to the citizens and to the economy of the state.
That also mentioned from previous speakers.
And the digital security authorities which should be tasked for the protection of the infrastructures as well as the state.
Of course, having mentioned all this, nothing should be of any significance unless that is a comprehensive awareness rising actions performed across a different levels starting from the cyber professionals to critical infrastructures through targeted awareness sessions, children, educators and parents.
No matter how, they will buildings strategy and organizations to provide such security.
If the state does not invent an awareness, then not much would be achieved.
Humans are always the weakest link.
And lastly which is also something mentioned by previous speakers to enhance the cooperation at the national level.
Now to the second question about the citizens, this is something that we have to take in a great seriousness.
And this is actually the question of test and how we can a-- trust and how we can achieve this trust.
The businesses in every country, high degree of confidence and security in their own personal use.
They have to be able to test the technology they are using regularly.
Beyond the actions, the type of actions at the national cyber security strategies, the focus on the cyber security resilience of the information structures, there is another area gaining significant traction in the past few years, set up to grow rapidly and we can also see that at the European level which is the cyber security certification to be able to addressing the issue of trust.
Through the use of the cyber security certification, companies doing business in the European union will benefit by certifying the products in one state and seeing their certifications to be recognized.
Independent and accredited board against the defined the criteria standards.
By issuing and indicate performance and therefore that would definitely improve the level of trust in making use in these products processes and services.

>> Thank you for noting the cyber security certification which is something is focus of the view at this stage.
Thank you for the reference.
We now move to Mr. Edmunds Belskis.
To whom I would like to ask how trusted the digital identity ensure citizens right of secure access and digital environment and how they are in support of the implementation of the sustainable development goals and secondly, how the democratization in all sector of the economy.
>> Yes.
Thank you very much.
It's a great pleasure to be again and present my country this time representing state on company or companies responsible for digital trusted signature and is a different cyber security issues.
We have to take into account we are learning in this pandemic which presents a different challenges how to work differently, how to think differently and organize our life in a new normal reality.
The learning and school of lives they have acquired online will benefit for the future of development and the use of new skills.
The office doors remains closed, millions of digital doors are open.
And we have to take those opportunities.
The skills we have inquired the speed of digital transformation, experience all of us to be more productive and efficient in the future.
Probably, this will be the time when we at the global level solve the problem of digital divide we discuss all the time and completely different and more effective way.
What kind of tools we can use and for sure, it is trusted digital identity tools introduced in different countries.
And speak about 17 development goals, many of them go hand in hand with trustable digital identity which ensure citizens access to -- or develop sustainable business or because digital is generally more cost effective.
Or opportunity on service provided by the government online and especially in this situation, access to digital governmental services becomes human rights issue at the moment.
And, of course, we can speak about green and nature issues when we reduce different emissions.
We eliminate any unuseful travelings to sign papers and access to any services.
So the expert community already made conclusions 2020 year has been the year of digital identity and related challenges.
And now 2021 and on-coming years, the importance of digital identification will continue to grow.

When we see our country more than ten years ago introduced trusted identity, we went through several evolution of governmental perceptions.
Now using tools and technologies today, we have one of the most advanced solutions for citizens digital identity including mobile applications and you do the hard work of several years.
Before pandemic, on the first day of COVID-19 pandemic effectively switch government activities economic relationships, citizens day-to-day activities to digital environment.
And during those last year we faced increased of usage especially for trusted digital identification procedures and actions and using digital signature by increase was around from 100 to 300% depending on the services.
And the very important part is this cross border acknowledgement and recognition of trust and digital signatures and identifications to access digital services in other countries.
But relating to the second question when we speak about democracy of technology which is a new trend, I remember what American philosopher Andrew Themburg said what human beings are and will become is decided in the shape of our tools.
We are using no less than actions of statement and political.
Let's emphasize those tools.
And why it increased different risks.
We are discussing today that the technologies know how to design and integration of different application, services, belong exclusively to IT industry in the previous years.
Relatively narrow.
Now many sectors are involved directly to ICT solutions and symbolically speaking, if there's a mistake, not enough knowledge in ICT, we can create a new tax and new treats for the systems.
However usage of technology is involved of everyday.
So we have to take into account those cyber security issues.
Take into account data system infrastructure, information security and integrity.
And finally, today, there is no place, tool, integration or application that can be called risk free zone.
The ICT sector must take on social responsibilities.
And I believe there will be a time when we find this exercise.
At the same time, I believe that it will be critical not only for well being of the industry but also as civil society.
And finalizing my speech, working together, we can create security chain without weak links and each link would be the strongest.
So the public interest has to be safeguarded during this movement.
Thank you very much.

>> Thank you.
We move to the next panelist.
We would like to start with what is the role of the agency in building confidence as already mentioned in the speech before about the need for this new digital didn't and citizenship in the use of ICT.
And the main challenges you have faced during the Covid pandemics in terms of confidence and security.
>> Thank you very much.
Excellencies, colleagues and participants, versus 2021 forum.
It is with great pleasure and honor that I greet you from -- on the republic of Serbia.
National computer emergency response team in charge of coordination and prevention and protection activities against security risks in ICT systems.
The national republic of Serbia established in 2016 in line with information security.
The national collects exchange information on securities in ICT systems including the incidents threatening the safety of ICT systems and it informs and advices the entities managing the systems in the global republic about incidents.
Some of the main tasks are the monitor incidents.
To analyze the risk and incidents and classify them according to the Civility loads.
Affected by the incidents.
And taking other necessary measure with each competence.
Teams on private public partnership model.
On international level with development and competent organizations in charge of information security.
To inform line ministry undertaken actions.
And in particular to raise confidence among citizens, companies and public administration bodies as well as to build awareness of importance of information security.
The national cert is adequately staffed and equipped with IT systems and infrastructure to perform activities within its competence and ability at all times.
In 2019, the national Cert was accredited by introducer.
And also in 2019, the national cert won the first fellowship award.
And in 2020, the national cert became the permanent member of the global forum first.
Which is the organization and recognized global leader in cyber incidents response.
Let me say a couple words about challenges we face during this pandemic.
During 2020 in the first months on 2021 when the states and people of the globe are coping with COVID-19 pandemic.

And most people are faced to stay at home and complete online most of the social and business activities including health related issues.
Computer emergency response teams are facing new challenges to ensure the security of the systems on the national and international levels.
And protect them from malicious cyber attacks.
In light of this new reality, has intensified in keeping the security public and private information communication systems.
The national cert introduced additional measure in providing early warning and responding to reported cyber attacks.
In the time of pandemic, the number of people forced to use online application services has rapidly increased and so has their ability to cyber attacks.
The government or the public started roll out of broadband infra structure.
Bringing applications and services to rural areas of Serbia.
In that respect, we have got respect to raise awareness of cyber security and empower a new population of ICT customers to gain confidence in the use of ICTs.
Thank you very much.
>> NINO: Thank you very much for the intervention.
We move to Dr. GIFT Kallisto.
And I would like to ask what are the common feels, organization and ordinary people can be stop for the use of ICT.
And what should be done in your opinion to overcome this fears from their roots to address them from their roots?
>> The rate at which ICTs have advanced have resulted in increased cyber attacks.
Criminals economic institutions and government web sites in order to extort money or advanced agenda.
Reported intrusions to developed and developing countries.
Enough to scare governments from adopting new technological applications.
A look at leaked sensitive information towards the gravity of cyber threats.
Publicized attacks in entities that were well versed in technology can make any ordinary person reluctant on connect to the internet let alone emerging technologies.
For governments, the greatest fears emanate from the threat of cyber terrorism, data breaches and espionage.
Fear keeps every nation more alert than the possibility -- can be executed, and easily be spotted coming.
For corporate entities, the fears include business secrets, sabotage in order to gain strategic advantage.
In the governments will more reluctant on embrace technology.

Breech of privacy, tracking of personal activity and information governments as well as from a composite of fears.
The most affected.
This explains the reluctance of social media.
Given the fears we have seen government departments lagging behind in computerizing their records and transaction systems.
Stories about build records, being dumped on the internet for all to see.
For 20 million accounts and running down.
And exacerbate these kind of fears.
To answer the second question, there are a number of ways and solutions that can be used.
There by building confidence and security in the use of ICTs.
For governments, trending of government officials on how to protect their ICT systems can improve the situation.
Such training includes training on pathway -- first line of defense.
Use of secure and sophisticated hardware as well as robust antivirus solutions can help not only allay fears of cyber terrorism, any breech of privacy but also provide real protection.
Overall, fears can be reduced through monitoring of data as it's creating effective plan which is well-known and owned by the employees.
Providing firewall security, securing Wi-Fi networks, limiting employee access to data and updating protective solutions Aztec knowledge gee -- as technology improves and changes.
Technical measures they can take is to have strong and robust legal framework that can protect users.
Perhaps the biggest confidence booster would be to ensure the level of knowledge is synchronized between those that create and use imaging technologies and those that regulate the technologies.
Having the framework gives assurance they are protected online.
The same way they are protected off line.
The cyber security bill and data protection bill are essential for building trust in the use for ICTs.
We have commissioned sizable local data center in the regional exchange point which gives assurance to users of telecommunications that the data does not get exported elsewhere.
The country is in the process of setting up additional response team.
This should go a long way.
I will leave you with one advice.
A customer base, reputation and even respect.
But it can take just one cyber incident on destroy its own.

If we do not take cyber security seriously.
I thank you for having me.