

# BROADBAND BITS & BYTES



A BIF Bi-Annual Communique

## Data Security in a WFH Environment



Volume 1 | Issue 2  
JANUARY 2021

# CONTENTS

---

01 Foreword: Mr. Ashwani Rana

---

02 President's Message

---

03 Director General's Message

---

04 Spotlight: *Data Security in a Work from Home Environment* by Dr. Kuldip Singh, Principal Advisor, BIF

---

06 Insights: *We need a data secured WFH environment* by Ms. Amrita Choudhury, Principal Advisor, BIF

---

09 Expert Speaks: *Data Security in a WFH Environment* by Mr. Alok Gupta, Principal Advisor – Cybersecurity, BIF

---

14 Perspective: *DNS Security Threats in the Work-From-Home Environment* by Mr. Samiran Gupta, Head of India, ICANN

---

16 Perspective: *Policy Imperatives for DoT to Support WFH and Industry 4.0* by Prof. Rekha Jain, Principal Advisor, BIF

---

19 Viewpoints: Mr. Sanjeev Bedekar, Mr. Satya N. Gupta, Mr. Harish Krishnan, Mr. Karthik Madhava

---

21 Notice Board

---

23 Policy Update

---

24 Activities & Engagements

---

26 Events and Meetings

---

34 Mediascape

---

36 Members

---

37 Hi Level Committees

---

38 Publications

---

39 Partnerships & Engagements

**Ashwani Rana**

*Vice President – BIF, Chair of BIF's ICAG (Internet, Content, Applications & Governance) Committee and Director of Public Policy @ Facebook (India, South & Central Asia)*



It is but trite to say that COVID-19 is not the only pandemic that is currently raging across the globe.

The increase in cybersecurity attacks across the world has been as exponential as the curve of the pandemic with more and more sensitive business sectors moving to work-from-home settings.

The Data Security Council of India has observed that 90-95% of the 4.36 million Indian technology workforce has successfully transitioned to a work-from-home model in a very short time, possibly one of the largest remote work projects anywhere in the world. This has happened almost overnight with the sudden onset of the pandemic and lockdown, meaning that business continuity planning has become critical for organisations across the country as they handle this transition.

The increase in cybersecurity threats during this period has demonstrated that the need for data security is greater than ever – including protection against external bad actors and internal threats, technology that ensures end to end data protection across different environments, innovative methods of authenticating transactions as well as monitoring of the work environment while employees work off remote servers. The DSCI has identified the key needs in the post pandemic model of work as digitization and cloud adoption, cybersecurity investments, and remote working models with zero trust security architecture.

Companies have discovered that they need robust cybersecurity policies with clear incident response and reporting mechanisms in place. Organizations which had not made sufficient investments prior to the pandemic are now struggling to adopt to the challenges of a remote workforce.

In the Indian context, what is encouraging to note is that cybersecurity firms and companies offering cybersecurity products, including start-ups, have sprung to action to address the emerging needs of the workforce. Security firms have assisted their clients in risk profiling of users, enhancing security systems and updates, monitoring end points, and advising on necessary controls to operate securely in a work from home environment.

Important contributions have also been made by traditional technology firms which have invested in high end communication platforms to mirror day to day interactions within the workplace and to ease interactions between service providers and clients. Communication platforms have invested in the

introduction of new features, which several companies are currently using to enable business communication at an unprecedented scale. Even traditional institutions where in-person communication was considered indispensable till a few months back, such as courtrooms and arbitration centres, have shifted to new modes of communication. It goes without saying that the need for secure communication channels is extremely high for such institutions, and it is encouraging to observe how well various technology services from across the world have risen to the occasion to meet this need.

This is also a pivotal moment testifying to the nature of the internet as being truly borderless. Just as cybersecurity attacks have increased from all corners of the world, the offerings which have eased the transition such as secure communication applications and cybersecurity solutions have emerged from multinational corporations and Indian start-ups alike. Supported by these innovations, several companies have been able to put employee safety at the forefront of their operations and declare work from home for an indefinite period, with minimal disruptions to business continuity.

Any Government policy to facilitate these interactions and transitions, should be mindful of the ways in which knowledge sharing and cross border data flows have been crucial in responding to this crisis. To ease this transition, infrastructural limitations on telecommunication services should be reconsidered, barriers to cross border flow of services should be removed, and various corporate, tax and labour reforms to enable remote work may be considered. Further, an Adobe survey in July revealed that in India, challenges related to cloud computing have been a top priority for CIOs, indicating the need for a supportive framework enabling cloud businesses to take off in India.

Internet Governance in the future should also be mindful of the lessons from this critical time. This represents an opportunity for us at Broadband India Forum to collate these lessons and enable engagement within the industry and with government stakeholders.

The future of work may be unpredictable, but the capacity of Indian industry to handle unpredictability has been impressive so far. It can be safely assumed that with concerted efforts from government and industry, the transition to the new normal will be eased considerably.



**TV Ramachandran**  
President,  
Broadband India Forum



## Dear Readers,

**T**he world is adapting to a new reality - the need to ensure social distancing and enable business continuity at the same time. Several organisations have declared work-from-home (WFH) as the new normal. While data connectivity has not always been the primary focus in residential areas, it has now emerged as a critical necessity to enable WFH. Online education, m-health, updating and dissemination of critical information and messages, etc. have been enabled by these services and the economy is still ticking despite the challenging circumstances owing to the efforts of these players - TSPs, ISPs, IT & ITES, as well as content service providers.

The Government's mission to facilitate the IT/ITES Sector by looking to institutionalize Work from Home, or rather it's evolved form of Work-from-Anywhere (WFA) through the recent introduction of liberalised guidelines for OSPs is a step in the right direction, which we appreciate and fully support. The guidelines, released on November 5, 2020, will make it easier for BPOs and ITES firms in many ways, such as cutting down on the cost of location, rent for premises and other ancillary costs such as transport, electricity and water bills. It is truly praiseworthy as it will improve the ease of doing business, create jobs and that too in small towns, encourage growth of overseas investments and see an overall contribution to the economy from one of our premium business sectors (*India's IT-BPM industry contributed around 7.7 per cent to the country's GDP in FY20, and is expected to contribute 10 per cent of India's GDP by 2025*).

At the same time though, it is imperative that the critical aspect of data security be addressed and upheld as a highest priority. The OSP registration guidelines already ensure elaborate compliance to security aspects, including storage of call data records up to one year, session logs, prohibition of certain activities by the OSP, security conditions regarding access to equipment, and compliance to safety and other statutes/rules/regulations including provision of

CDR/IPDRs to security agencies. To further strengthen the overall network security, some additional security measures that may be envisaged could be:

- ▶ Deploying a robust encryption system
- ▶ Authentication, Authorisation and Accounting - by using multi-factor authentication
- ▶ A multi-factor authentication could be a combination of the following –
  - a. Something known to the user (user ID, PIN, or a secret question)
  - b. Security key, token or card that the user possesses physically or can be sent to the registered mobile number of the user
  - c. Biometric identification (if supported by the user's device).

While these are just a few observations and suggestions, this edition of BIF's bi-annual communique - Bits & Bytes, deep-dives into the critical aspects of this issue, providing the most interesting and informative perspectives, insights and viewpoints from highly experienced industry experts; apart from providing a sneak-peek into the latest activities and updates of the Forum.

I would also like to take this opportunity to thank each and every esteemed member, our valued associates and partners, our honourable advisors, and the dedicated Directorate team, for their invaluable support and contributions in keeping the BIF flag flying high, as we aspire towards greater objectives and achievements. I feel there is much to be done to help establish India as a Connected, Knowledge Economy, as well as a global leader in the Digital Communications arena, and I am positive that with the support and participation of the entire BIF family, we shall be able to achieve the same.

I hope you find this communique to be an interesting read, and we welcome suggestions/comments for improvements.



**Rajat Mukarji**  
*Director General,  
Broadband India Forum*



*Dear All,*

Cyber-crime is fast emerging as a global menace, with an estimated loss of USD 6 trillion in the first 9 months of 2020, as per the Government of India's National Cybersecurity Coordinator. If likened to an economy, this massive figure would represent the third largest economy in the world, after the USA and China. Specialist firms expect global cybercrime costs to escalate further over the next five years, to the tune of over USD 10 trillion/annum by 2025. This would perhaps be the greatest transfer of economic wealth in history, and exponentially larger than the economic damages incurred due to natural disasters in any given year. Such cybercrime costs generally include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. The gravity of the issue, thus presents itself most vividly.

With Covid19 forcing the new reality of Work-from-Anywhere (WFA) worldwide, the reason for concern and awakening in the cybersecurity domain heightens substantially. As we witness the massive shift of work practises and usage trends of most people from larger to smaller, and from corporate to personal devices, the vulnerability factor rises. This offers huge opportunities for the cyber criminals to exploit the technologies, and commit numerous kinds of thefts, felonies, frauds and anti-social activities. It is therefore imperative, that we step up in our understanding, awareness and knowledge in the best practices for cybersecurity and hygiene, in a pressing manner.

In fact, it is owing to the above-mentioned concerns and its critical relevance, that BIF has taken a proactive measure in forming the Cyber Trust & Safety Working Group. The objective of this WG is to explore various avenues for knowledge, awareness and capacity building for combating the rising threats to citizens from online/cyber-crimes and frauds via suitable outreach mediums to different components of the ecosystem – Government, LEAs, NGOs, Academic Institutions, Civic Bodies, general public, etc. Being driven by a few domain experts, and with the support of the members, we are positive that this initiative from BIF will be productive and add much value to its purpose.

In the same vein, this particular edition of BIF's Bits & Bytes also explores a vital aspect of this subject, articulating the key issues and solutions to help combat, on an urgent basis, this growing menace. My sincere thanks and compliments to the participants, experts, advisors and members, for their contributions and support, and for taking the time out to share their invaluable insights and knowledge on this very critical subject.

I would also like to take this opportunity to thank the BIF leadership, especially the President, for his dynamic leadership and guidance in driving the Forum's progress and many achievements. My compliments and thanks also to our most efficient Directorate team, for their unfettered dedication, consistent efforts and the gradual but marked success in establishing BIF as the leading Think Tank for the Digital Communications ecosystem in the country.

# Data Security in a Work from Home Environment

**Dr. Kuldip Singh**  
Principal Advisor, BIF



***For the purpose of data security in the WFH environment, the enterprises must develop suitable security policies and security audits.***

Covid 19 pandemic has changed the way we live, work, entertain and socialize. The post pandemic world is not going to be the same as it was before. While even before the pandemic, some companies offered the option to work from home to its employees in a limited way as a convenience to them, the same has become a norm due to the lockdowns imposed during the pandemic. Most of the companies, especially in the IT, Software Development, Customer Support, E Commerce, etc. have asked their employees to continue working from home even after the lockdowns have been lifted. WFH has many advantages and is likely to be the new norm in the post pandemic world.

While WFH has many advantages such as time saved on commuting, decreasing the load on the public transport infrastructure, cost savings on physical infrastructure for the business houses etc. just to name a few, it also has its challenges especially in the security of data related to the enterprises as well as the customers.



***As part of the security policy, people working from home must be provided with basic security knowledge. They must be made aware of the phishing methods and malicious software used by hackers.***

WFH requires computers at home, modems to connect these computers with the network, and the network to connect these to the enterprise servers. All these elements become additional points of vulnerability so far as the security of data is concerned. The main risks are due to Hacking, which is an illegal intrusion into the target computers by means of software written for the purpose, malicious software such as Virus, Worms, Trojan Horses, Spyware etc., and Phishing to get a variety of information, login IDs, passwords, etc. by imitating a web site or an email that otherwise looks authentic. The resulting data related risks are interception of Data, Data theft and modification of Data.

For the purpose of data security in the WFH environment, the enterprises must develop suitable security policies and security audits.



As part of the security policy, people working from home must be provided with basic security knowledge. They must be made aware of the phishing methods and malicious software used by hackers. Use of public Wi-Fi hot spots should be avoided. Default passwords of modems/Wi-Fi routers that come factory installed, must be changed. Strong and random passwords of minimum eight characters length and containing both alpha-numeric and special characters should be used for Wi-Fi routers and access control. Storage of data on removable media such as USB sticks should be prohibited.

The data movement between the computers at home and the enterprise servers must be through a secure VPN tunnel. The VPNs should use suitable algorithms to encrypt the data during transit and hide the user's IP address.

Regular security audits should be part of the security policy. These audits must check that the computers are sufficiently protected against malicious software by Anti-Virus programs that are regularly updated, check for strong passwords and provide for two-factor authentication for access control.

WFH is the new norm that is likely to be there even in the post pandemic world. Obviously, it has many advantages both for the employees and the business houses. Working in Cyberspace has always posed security challenges. These security challenges and the risk to data increases many fold in the WFH environment. However, this risk can be minimized by putting suitable security policies in place and carrying out regular security audits. A well implemented WFH environment may ultimately prove to be a win-win solution for all the stakeholders.



***The data movement between the computers at home and the enterprise servers must be through a secure VPN tunnel. The VPNs should use suitable algorithms to encrypt the data during transit and hide the user's IP address.***



# We need a data secured WFH environment



**Ms. Amrita Choudhury,**  
Principal Advisor, BIF



**T**he COVID-19 pandemic has brought a paradigm shift in our lives, making us more reliant on the Internet. Almost all activities of our lives have moved online: our social interactions, the way we access health and education, professional working pattern, doing business, shopping, access support services or financial transactions, etc.

Though the economy is opening up, many of us are still working from home or have adopted to a mix of WFH and going to office on a rotation basis. Most organisations today are trying to reflect on the experience of the last six months to develop an effective strategy to adapt to this 'new normal' in the long term.

While WFH has several advantages both for employers and employees in terms of saving on commuting time, providing flexibility, health safety, etc., it has ushered in few challenges too. The transition to WFH not only requires a designated space, trying to focus on work without family interruptions, but also a shift in the mindset in how the work life balance can be maintained.

Besides this, safety and security of the network, and security of data during WFH has emerged as a major concern. While in office, employees work in a secured environment, but in the home environment, the devices, software used, connectivity are mostly not secured. Many a times, employees access official



***For promoting a data secured WFH environment, it is important that employers lay down guidelines or best practices for employees post reviewing the existing policies and practices. This could include carrying out a Data Protection Impact Assessment (DPIA) to ascertain the necessary controls, technical and others, needed to safeguard the data.***

information from their mobiles, shared family devices, which in most cases do not have the adequate security software installed. Also, people tend to be more relaxed on security aspects at home. As a result, during COVID times, investigative agencies such as Interpol, FBI and Indian agencies including CERT-In have reported a surge in data breaches and cyberattacks on home networks as it has become a new touch point of vulnerability.

For a data secured WFH environment, apart from a few organisations in the tech space who had WFH policy even before COVID times, most other businesses have now formulated, or are in the process of formulating guidelines for their employees.

Looking at the security threats, WFH guidelines or advisories have been issued by international organisations such as [ILO](#), [WHO](#), etc. In the Indian context the [Indian government](#) and industry associations such as DSCI have issued guidelines on how to make WFH more secure.

For promoting a data secured WFH environment, it is important that employers lay down guidelines or best practices for employees post reviewing the existing policies and practices. This could include carrying out a Data Protection Impact Assessment (DPIA) to ascertain the necessary controls, technical and others, needed to safeguard the data. Employers should carry out trainings for employees on threats online viz. phishing and malware attacks, viruses, downloading, etc., and sensitizing them on privacy and data security issues, making them aware and mindful of data obligations and liabilities. Additionally, ensuring strict user identity and access management to enhance security - such as allowing only verified and authenticated devices and users with multi-





***It is also important for both employers and employees to know, what to do, how to report and seek help, in case there is a cyberattack or data breach. In India, while there are provisions in the Information Technology Act 2000 for dealing with issues related to cybercrime and breaches, unfortunately we do not yet have a data protection law or a dedicated law on cybersecurity. The lack of specialised privacy law at times acts as a deterrent in data privacy issues.***

factor authentication; encouraging the use of VPNs, encrypting data, extending patch management to all remote devices and end points, using two factor authentications when accessing company information using mobile device, etc. can help to keep the processes safe.

Employees working from home have a larger role now of adhering to the data privacy and security policies, including respecting the rights associated with data, especially those handling sensitive information or personal data of customers. It is advocated that employees comply with security policies of the employer, use authorised hardware and software, do not access company information for shared devices, abide by standard cyber security tips such as updating antivirus, do not open suspicious mails or attachments, etc.

It is also important for both employers and employees to know, what to do, how to report and seek help, in case there is a cyberattack or data breach. In India, while there are provisions in the Information Technology Act 2000 for dealing with issues related to cybercrime and breaches, unfortunately we do not yet have a data protection law or a dedicated law on

cybersecurity. The lack of specialised privacy law at times acts as a deterrent in data privacy issues.

Therefore, from the policy perspective, it is important that India implements a robust data protection regime at the earliest as that will help to protect the privacy and rights of the citizen. It may be mentioned that the current draft Personal Data Protection Bill is being reviewed by the Joint Parliamentary Committee on PDP Bill 2019 and is yet to be tabled in the Parliament. Additionally, for securing data and communication, India must formulate an Encryption law.

To conclude, WFH is here to stay. In fact the government recently [modified the WFH and Work From Anywhere \(WFA\) guidelines](#) for companies, which is expected to benefit the IT industry, primarily the business process outsourcing (BPO) sector. The need of the hour for businesses is to ensure that proper guidelines or best practices are formulated, the employees are sensitized on the issues and threats, employees comply to safety protocols and take adequate measures to ensure data security, and the policy makers work to ensure India has a robust data protection law in place at the earliest.



# Data Security in a WFH Environment- Cyber Hygiene and Awareness



**Mr. Alok Gupta**

Principal Advisor –  
Cybersecurity, BIF

**C**COVID-19 changed the world abruptly, forcing the workforce to work from home wherever possible. With businesses moving their operations online, there is a growing concern about malware threats, online scams, and identity theft. Although, businesses had established mechanisms and controls to protect their infrastructure and data from cyber-attacks, the sudden shift to remote work opened a large surface for attacks. That means the perpetrators now focus on individuals who are more vulnerable as they may be less aware or do not have the controls to support securing their systems. The cyber-attacks not only



lead to a substantial economic damage but also have a direct and indirect social consequence for the victims.

While the world struggles with the impact of COVID-19 on business and lives, hackers and cybercriminals see it as an opportunity. As per credible surveys and studies, there has been an exponential rise in cyber-attacks, breaches, and coronavirus-themed spam post March 2020.

Work from Home (WFH) or remote working throws its own challenges of cyber security preparedness and maintaining a good cyber security hygiene.

Business, IT, Security & Risk leaders were in any case quite aware and prepared in dealing with breaches and attacks in the pre-Covid19 era. However, now with this “New Normal” of Work from Home, their preparedness has been found inadequate, which is quite obvious since it's a war like situation and no one was prepared for the scale and enormity of risk this pandemic has presented.

Homes are traditionally not designed to conduct business and carry out office work, therefore availability of robust & secured IT and connectivity infrastructure was never sought or provisioned, the way they would do it for offices. Inconsistent or poor connectivity, lack of cyber hygiene, unprotected personal/home computers not only effects the performance but leads to both workers and business at risk of cyber threats, attacks, and breaches.

Business/IT leaders are a worried lot now since they need to now protect sensitive business critical data, Intellectual property, privacy of workforce and customer confidential information from leakage or theft. Businesses who are prepared or get themselves prepared for this new normal will be able to sail through and thrive in future, while organizations that are insufficiently prepared will fail to survive.

## Vulnerabilities in the Current Work Environment

Working from home has increased the risks manifold and made both the organisations as well as the workforce more vulnerable due to introduction and usage of various WFH technologies such as web/video calling/conferencing, project and time management trackers, digital assistants such as amazon echo and employee activity tracking tools, etc.

For example, with surge in WFH activity video/audio conferencing tool Zoom quickly became the video meeting app of choice. “Zoom-bombing” (where uninvited attendees break into and disrupt meetings) was one such incident experienced and reported by many users. Security researchers also reported bugs that could allow hackers to take control of webcams and microphones on Zoom users' Macs.

Attention tracking feature in Zoom allowed host to enable a built-in option which alerts them if any attendees go more than 30 seconds without Zoom being in focus on their screen leading to virtually monitor a worker's inattention. Zoom's cloud recording feature which allows the meeting recording to be saved on cloud could be accessed by other people in the organisation who may have not attended the



***Homes are traditionally not designed to conduct business and carry out office work, therefore availability of robust & secured IT and connectivity infrastructure was never sought or provisioned, the way they would do it for offices. Inconsistent or poor connectivity, lack of cyber hygiene, unprotected personal/home computers not only effects the performance but leads to both workers and business at risk of cyber threats, attacks, and breaches.***

meeting at all. Subsequently some of these bugs, flaws and concerns were addressed by Zoom after they were exposed.

Since the on-premises concept vanished due to remote working, the applications and services had to move to cloud servers leading to risks arising due to public and hybrid cloud adoption.

One major change which the employers need to cope is use of inconsistent and less secured personal devices, Wi-Fi routers/modems and internet connections at home of employees.

It is a double whammy since any vulnerability exploited by hackers in WFH environment can lead to loss of confidential and sensitive work data as well as breach of privacy for the user due to leakage of personal information and data residing on personal devices used for work.

Another big factor noticed during the pandemic was to attack the WFH employees with social Engineering, Phishing and ransomware attacks, leading home users to malicious websites luring them to offer information or advice about the pandemic.

As an example, in February 2020 a malicious executable file named CoronaVirus\_Safety\_Measures.exe was being delivered to the victim's machine as an email attachment. Then came the coronavirus scare tactic which was used across mobile ecosystem in the form of Remote Access Trojan (RAT) and an application called 'coronavirus'. Once the user installed this mobile app the Trojan would access sensitive information on the phone.

"Scareware" a kind of ransomware which would take advantage of the fear factor and demand a ransom to unlock/release the encrypted data once a victim is compromised were rampantly used by hackers.

During the early days of pandemic and even now, the cyber-attackers are creating websites that spread misinformation about coronavirus, falsely claiming how to build immunity or prevent corona to infect the victim via downloads on social media, emails, weblinks on SMS and WhatsApp. The malware Azorult.Rk masqueraded as an application providing diagnosis support, even including a screenshot of a popular interactive tool that maps 'Covid-19 cases and exposure'.

One must remember to strike a balance between delivering efficiency, productivity, customer experience etc. in haste while deploying security and privacy protection measure to prevent another catastrophe.

## Cyber Hygiene

Much like the physical hygiene, remote users must follow online safety guidelines and maintain a good cyber hygiene. These practices are necessary to ensure the safety of identity and loss of sensitive data. Following a routine cyber hygiene procedure for computers, networking devices and software will aid both maintenance and security. Systems tend to become vulnerable with outdated programs and files. Periodic maintenance routine will spot these issues making software to run at its peak and less vulnerable to cybersecurity risks.



- ***To prevent credential theft, passwords should be changed periodically with complex words or phrases.***
- ***Automatically/Regularly updating and patching the software used should be part of regular hygienic review.***
- ***Older computers and smartphones will have limitations in using the latest software versions. Therefore, it is important to update them with the safest version, else they should be removed from usage. Hackers always target the weak and vulnerable devices to compromise.***
- ***Provide a privileged access only to administrators and limit access to all other users.***
- ***To prevent loss of data due to corruption, encryption by ransomware and virus attacks, always keep a backup of data to an offline secondary storage repository.***
- ***Deploy CIS Controls, NIST Cyber Security Framework or other credible frameworks to ensure security.***





Predicting cyber threats is challenging. But, preventing them is feasible with sound cyber hygiene practices. A well-documented Cyber Hygiene policy is necessary to be followed by all remote users. Here are some of the steps that should be part of a cyber hygiene policy:

- ▶ To prevent credential theft, passwords should be changed periodically with complex words or phrases.
- ▶ Automatically/Regularly updating and patching the software used should be part of regular hygienic review.
- ▶ Older computers and smartphones will have limitations in using the latest software versions. Therefore, it is important to update them with the safest version, else they should be removed from usage. Hackers always target the weak and vulnerable devices to compromise.

- ▶ Provide a privileged access only to administrators and limit access to all other users.
- ▶ To prevent loss of data due to corruption, encryption by ransomware and virus attacks, always keep a backup of data to an offline secondary storage repository.
- ▶ Deploy CIS Controls, NIST Cyber Security Framework or other credible frameworks to ensure security

Once the policy is created, appropriate timeframes should be set for each of the routines. For example, checking for security updates at least once per week, changing passwords every 30 days. Such sound cyber hygiene practices carried out in conjunction with enterprise-wide security practices, will aid the organization in maintaining a strong security posture.

## Cyber Security Awareness Training

For many users who solely used to work from their offices/workplaces, it is a new experience for them to work from home and adapt to this new normal. This means transitioning their work routine and habits to home environment. Same is the case for students who are taking their classes online, from home.

To help with this transitional period, there is need to provide an online cyber safety awareness training to each such user. Security awareness is an integral part of people's conduct when they work out of offices, however they tend to change their security habits when they change their work routines. So, it is essential to design and impart WFH specific cyber security awareness training programs for remote users which can lay emphasis on the following measures:

- ▶ Use a secure connection to connect to the company network. Ensure the company Virtual Private Network (VPN) is configured to use multi-factor authentication.
- ▶ Do not share work data and information with the personal data store spaces, applications, or personal devices.
- ▶ Ensure that latest applications, operating systems, and network tools are installed on the computer along with the malware protection and anti-spam software.
- ▶ Create new and strong passwords for your laptop, corporate mobile device, and email.
- ▶ Use only approved cloud applications for sharing and storing data.
- ▶ Do not click on links from unsolicited emails, since clickjacking is a common method to install backdoors and spywares.

The organization should promote security awareness best practices via newsletters, short videos, and mock phishing simulation campaigns to impart awareness training. Cybercriminals use disguise as legitimate health authorities and government departments to prey on fears about novel coronavirus. A robust cyber security awareness will protect from phishing and other cyber threats.

The remote work setting requires remote access of critical IT infrastructure, enterprise data and use of collaboration tools for team interactions. This is throwing up several new risks and challenges to businesses and the boards and top management need to worry and ramp up their cyber security efforts to become more resilient.



***Security awareness is an integral part of people's conduct when they work out of offices, however they tend to change their security habits when they change their work routines. So, it is essential to design and impart WFH specific cyber security awareness training programs for remote users which can lay emphasis on the following measures.***



**1. IT & Security Audit & Assessment:**

Assess and evaluate the current system's internal control design and effectiveness against relevant standards, best practices and remote working including design, architecture, implementation, performance, efficiency, security protocols and IT governance. Design and review the incident response plan and check organization's preparedness and readiness for a revised cyber insurance.

**2. Vulnerability Assessment & Penetration Testing:**

Vulnerability Assessment scans should be performed on network, applications, web infrastructure and end points to check critical and exploitable vulnerabilities. Thereafter Penetration tests exploitation can be conducted to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat. A detailed report with recommendations will help management and IS teams mitigate such risks, vulnerabilities, and flaws.

**3. Red Team Exercise:**

Red Teaming emulates real-world adversaries to measures the effectiveness of people, processes, and technology to defend the organizations. This includes conducting Red Team exercises and guiding organization's blue teams.

**4. Enable Multifactor Authentication:**

Social engineering remote privileged employees will allow hackers to know and steal credentials allowing them to access business

critical information as insiders. Deploying Multifactor Authentication System will allow remote employees to leverage convenient & flexible tokens for secondary authentication of all end points, trusted devices, VPN, on-premise and cloud applications, to prevent credential theft and unauthorized access while meeting the regulatory needs.

**5. 24x7 Continuous Monitoring & Threat Intelligence:**

24x7 Log & network monitoring correlated with threat feeds to not only meet the compliance requirements of continuous monitoring, but at the same time giving an organization instant alerts and intuitive dashboard for governance as well as remediation via Managed Security Services & SOC Platform.

**6. Secure Configuration Management:**

Misconfigurations can lead to breaches and cyber incidents. Compliance requires organizations to continuously check and remediate configuration issues in physical servers and VMs and provide audit-ready reports. Continuously and comprehensively identify and automatic remediation.

**7. Phishing Campaign Assessment:**

Sophisticated threat actors mostly target senior leadership, privileged users, and those with payment authority. Very convincing campaigns and phishing attacks are launched to lure such users. Get scenario based simulated campaigns conducted for phishing assessment and employee awareness.





# DNS Security Threats in the Work-From-Home Environment



**Mr. Samiran Gupta**

Head of India – Internet Corporation for Assigned Names and Numbers (ICANN)

## Introduction

The COVID-19 pandemic has led to the acceleration of digitization across the global economy. One of the most noticeable trends is that of “Work from Home” (WFH) which has extended to many segments of the enterprise sector and academia. Employees are asked to work from home and months have gone by without offices resuming full staffing. Students are attending schools and colleges from their homes as well. In response to this new trend, telecoms service providers have had to prioritize provisioning of Internet resources to households. We now read articles about WFH becoming a permanent feature in the post-pandemic scenario as well. The new normal of WFH has led to potential enterprise security risks entering homes. As such, awareness and practices need to be strengthened to mitigate these threats. ICANN supports this process by providing research on DNS security threats patterns.

### Domain Name System (DNS) Security Threats and ICANN:

ICANN's mission is to ensure the stable and secure operation of the Internet's unique Identifier Systems. A key role that the ICANN organization plays is to improve trust in the working of the Domain Name System (DNS). This trust is the key element to the security and stability of a decentralized and interoperable Internet. Since ICANN's remit excludes regulation of Internet content, one of the areas in which we focus is on efforts specific to “DNS security threats” that concern ICANN.



ICANN organization defines DNS security threats as five broad categories of harmful activities:

- **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
- **Botnets** are collections of Internet-connected computers that have been infected with malware that can be commanded to perform activities under the control of a remote administrator. Typically, a botnet command and control server instructs elements of its botnet to extract information from their host systems or engage in malicious action such as a distributed denial-of-service attack.
- **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.
- **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to the attacker's site instead of the one initially requested. DNS poisoning causes a DNS server or resolver to respond with a false IP address bearing malicious code. Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.
- **Spam** is an unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was



***To help the community address DNS security threats better, ICANN provides objective data, and the context to help the community draw conclusions from the data. ICANN's Domain Abuse Activity Reporting (DAAR) Project produces monthly reports that provide aggregated statistics and time-series analysis about most of the security threats identified above, namely phishing, malware, spam, and botnet command-and-control (we have no way of obtaining data about pharming). Data derived from DAAR can help the community to track the state of DNS security threats and the effects of policy changes.***

sent as part of a larger collection of messages, all having substantively identical content. While spam alone is not a DNS Security Threat, it was included in the five key forms of DNS Security Threats since it is very frequently used as a delivery mechanism for the other four forms of DNS security threats. In other words, generic unsolicited e-mail alone does not constitute a DNS security threat, but it would if that email is part of a phishing scheme, malware distribution, pharming activity, or botnet command and control.

To help the community address DNS security threats better, ICANN provides objective data, and the context to help the community draw conclusions from the data. ICANN's Domain Abuse Activity Reporting (DAAR) Project produces monthly reports that provide aggregated statistics and time-series analysis about most of the security threats identified above, namely phishing, malware, spam, and botnet command-and-control (we have no way of obtaining data about pharming). Data derived from DAAR can help the community to track the state of DNS security threats and the effects of policy changes.

## Conclusion

ICANN also provides technical education to relevant stakeholders including law enforcement agencies, registries and registrars, to help mitigate DNS security threats. To know more about ICANN's mission to ensure a stable and secure operations of the Internet's unique identifier system, please do visit [www.icann.org](http://www.icann.org).

# Policy Imperatives for DoT to Support WFH and Industry 4.0



**Prof. Rekha Jain**  
Principal Advisor, BIF

## Introduction

The mobile technology revolution embodied in 5G and beyond is complemented by accelerating Wi-Fi evolution. Due to the increasing throughput, lower latency embedded in the newer standards of Wi-Fi (from Wi-Fi 4 to Wi-Fi 6), more than 70% of all Internet traffic is offloaded to Wi-Fi networks. The low cost and easy connectivity through Wi-Fi has enabled proliferation of technologies such as smart homes, AR/VR/smart cities. Wi-Fi is increasingly being used by TSPs for mobile offloading due to the availability of carrier grade Wi-Fi.



Due to the pandemic, the WFH scenario has become mainstream. In the residence, there is need for high bandwidth, reliable communication in a situation where multiple devices connect to the Internet. Video applications, whether they are for surveillance or for education are driving higher bandwidth demand. In the enterprise sector, demand for high bandwidth, reliable connectivity is driven by the requirement of training using virtual reality, providing connectivity between different equipment and devices to the Internet etc. New developments and standards such as Wi-Fi 6 and the availability of 6 GHz as an unlicensed, shared band make this possible. Wi-Fi 6 implemented in 6 GHz (Wi-Fi 6E) opens up opportunity for innovation.

- **Wi-Fi and IoT**

With increasing focus on Industry 4.0 and Wi-Fi support for a variety of IoT devices with differing characteristics to be on the same network, facilitates enterprise IoT connectivity. Since different IoT systems have varying protocols, managing these disparate performance requirements and standards is challenging. For example, a video app connected to security service will require broadband access, low latency and high availability, whereas another app for monitoring temperature may require narrowband communication. Wi-Fi helps in addressing the issue of streamlining the same as it is a standard technology.

- **Wi-Fi in India**

In relation to the developed world, India's use of Wi-Fi had been low at around 6-10% of usage elsewhere. Partly, this has been due to the very low mobile data cost, in relation to the rest of the world and poor penetration of smartphones. The WFH situation brought out by the pandemic saw increase in demand for connectivity in the home and the consequent evolution of a dongle rental system, allowing multiple devices to be connected to the Internet through Wi-Fi.



***In relation to the developed world, India's use of Wi-Fi had been low at around 6-10% of usage elsewhere.***



In 2018, nearly 32% were Wi-Fi 5 devices. By 2019, this number was expected to go up to 65%. India sold over 204 mn Wi-Fi enabled devices in 2018, expected to grow 8% in 2019. Mobile phones were the most used Wi-Fi enabled devices (65% contribution in the total sales)<sup>1</sup>. This indicates a growing demand for Wi-Fi in the new bands.

## Global Developments

With the FCC's announcement of unlicensing 1200 MHz of spectrum in the 6 GHz band, 6E enabled devices have started becoming available although as of now, very few<sup>2</sup> and limited to a few countries such as UK, S. Korea that have also unlicensed this band for shared use with existing incumbent users.

In order to remain harmonized in spectrum use with respect to other countries, it is important for India to adopt new use patterns at tandem with the world. Further, since service provision in the unlicensed band is less expensive, a lot of innovation takes place. In order to spur Atmanirbhar Bharat, it is imperative that developers and users get access to the same spectrum as is being made available in large parts of the world.

Despite these global developments, DoT has been reluctant to consider the 6 GHz band for unlicensing, partly due to the pressure from incumbents. Further, its concern has been whether the nearly 600 MHz unlicensed in 5 GHz in 2018 has been utilized fully, before making "additional" spectrum available?

<sup>1</sup> <https://www.india.com/technology/india-sold-over-204-million-wi-fi-enabled-devices-in-2018-reports-3699588/>

<sup>2</sup> <https://www.cnet.com/how-to/wi-fi-6-is-the-fastest-yet-but-wi-fi-6e-will-be-even-better-6-ghz/>







***In order to remain harmonized in spectrum use with respect to other countries, it is important for India to adopt new use patterns at tandem with the world. Further, since service provision in the unlicensed band is less expensive, a lot of innovation takes place. In order to spur Atamirbhar Bharat, it is imperative that developers and users get access to the same spectrum as is being made available in large parts of the world.***



***Given the twin requirements of residential Internet and broadband and enterprise requirements of Industry 4.0 characterized as above, DoT should start considering the need to unlicense the 6 GHz band.***

## Imperatives for DoT

The following points need to be considered by DoT

- It is imperative for DoT to ensure optimum use of all spectrum, including exploiting shared use where possible. Spectrum being a natural resource for which DoT is the trustee for Indian citizens, its role has to be to maximize value from it for the citizens. If shared use leads to greater value, then DoT must take initiatives for facilitating it.

To give comfort to incumbent users, DoT must start co-existence studies and review the outcomes of such studies in other parts of the world, where regulators have given the go-ahead for shared use.

- While Wi-Fi 6 can also be implemented in the 5 GHz band, but, the 6 GHz band enables leveraging the unique characteristics of the standard: 160 MHz channels. This band will allow streaming at 8k, greatly improving the quality of educational content, interactions and providing for real time immersive AR/VR gaming, and training. Wi-Fi in 6 GHz complements 5G by providing high speed tethering, low congestion due to lack of legacy equipment, low latency, high speed and ultra-reliable, high availability network for supporting IoT and mMTC.
- Given the twin requirements of residential Internet and broadband and enterprise requirements of Industry 4.0 characterized as above, DoT should start considering the need to unlicense the 6 GHz band. It needs to adopt a more open, facilitating perspective by being a steward for spectrum availability in the best interest of Indian citizens. This will enable India to keep pace and lead in technological developments with global developments.
- The metrics of evaluation of outcomes cannot be utilization of unlicensed spectrum, always a contentious parameter. The outcomes need to be evaluated on whether Indian citizens and enterprises had access to technology, otherwise available globally and whether DoT played an active supportive role in it. Today's fast paced policy environment does not give a space of 15 years, to design a policy outcome - the time it took to make 5.8 GHz unlicensed for outdoor use!



## QUESTION?

## ANSWER!

## Data Security in a WFH Environment



**Mr. Sanjeev Bedekar**

CEO, RANext  
(a Spaceworld company)  
& Chair of BIF's FTTX  
Committee

As work from home (WFH) becomes the new normal, organisations need to put in place more structured WFH policies to ensure security of internal/client data. In allowing WFH, including mission-critical work, they become intermediaries under the IT Act 2000 and are duty-bound to comply with the parameters of due diligence and other compliances under the Act.

The absence of any data protection/cybersecurity/privacy law in India poses further challenge, since companies continue to be liable for breach in client data even when employees work out of home. In these transient times, they have to do far more capacity building among their employees working from home.

Businesses need to ensure that they have virtual private networks and cloud solutions so that basic security is taken care of even in a WFH

environment. All security protocols relating to using authorized antivirus & security software, not sharing of passwords, adhering to prudent security & encryption practices, and not using unsecured networks should be rigorously maintained.

The most promising solution would be to enable remote employees to work on their personal devices, while staying connected to the home office security network. This can be done via cloud-based IT management platforms like [Cloud Management Suites](#), which enable firms to connect, monitor and secure their assets on the cloud, without any geographical boundaries. With this kind of solution, one can see exactly where their assets are situated on the map, and ensure from afar that their remote employees are compliant with the self-defined security regulations.

## QUESTION?

## ANSWER!

## Data Security in the Liberalised WFH Connectivity



**Mr. Satya N. Gupta**

NGNguru, , Treasurer,  
BIF and Chairman of the  
Board, Bluetown India

Work from home (WFH), renamed as WFA (Work from Anywhere), has become the New Normal, which necessitates utmost priority be given to keep the workforce productive, while also keeping personal as well as customer data secured. In light of these compulsions, there is an urgent need to create VPN, explore the available security options, self-protect by DIY (Doing It Yourself) or work with innovative IT services providers.

**"One of the best practices that businesses, especially SOHOs, can implement when it comes to securing the data of remote workforce is to use a VPN (Virtual Private Network) - a secure communication tunnel carved out of the public network connectivity (like Internet) between multiple online locations."**

In the landmark liberalised guidelines to enable WFA, DoT has done away with the mandate to use SPPVPN, which was to be provided by the TSP/ISP at home location, which was expensive

but secured. This relaxation has shifted the onus of data security to users with the expectation of self-regulation.

Any data transfer made for business purpose, therefore, should be performed through a VPN which either leverages SSL (Secure Sockets Layer) or IPSec (Internet Protocol Security) to encrypt communications from the remote teleworker's machine.

When it comes to Self-Provisioned VPN, the New Internet Protocol (IPv6) comes as a tailor-made solution, doing away with the need for NAT (Network Address Translation), enabling the security layer to be managed at end-user level and dedicated/private IP address for each device/machine. Also, the IPSec feature is built-in IPv6, enhancing the security by using ESP (Enhanced Security Payload) and AH (Authentication Header).

Hence to protect your data from attackers and hackers use self-provisioned VPN using IPv6.

## QUESTION?

## ANSWER!

## Data security in the present work-from-home scenario



**Mr. Harish Krishnan**

Managing Director,  
Public Affairs & Strategic  
Engagements, Cisco  
Systems India Pvt. Ltd.

The world is gripped with the news of a possible vaccine rollout soon. We cannot be sure of the timeline of the rollout, but we can rest assured that work-from-home is a long-term strategy for most companies in the world. Even after the pandemic tides over, we can expect a hybrid model of where employees may continue to work from anywhere, making enterprises realize that "Work is an activity and not a place". Several companies may have transitioned well to the work-from-home model but need to strengthen secure remote working requirements to sustain this model.

This was highlighted in a recent study by Cisco - [Future of Secure Remote Work](#). The report surveyed 3,000 IT decision makers across industries from 21 regions. Over 60% respondents said more than half the workforce transitioned to

working from home; 37% expect it to continue even after the pandemic ends. About 68% of the organizations faced cybersecurity challenges when supporting remote workers and 84% of the organizations feel that cybersecurity is now a top priority for them.

Enabling work-from-anywhere for employees requires organizations to reassess their IT architectures across assets, network, cloud access, etc. The basic tenet of the work-from-home architecture must rely on Zero Trust approach to data security. This approach assumes that all environments are hostile, and therefore identifies and prevents any threat, by safeguarding customer's data across all endpoints.

Successful enterprises must recognize cybersecurity as a top priority. This will play a crucial role in their success in the new normal.

## QUESTION?

## ANSWER!

## Data Security in the present WFH environment



**Mr. Karthik Madhava**

Founder & CTO,  
Lavelle Networks

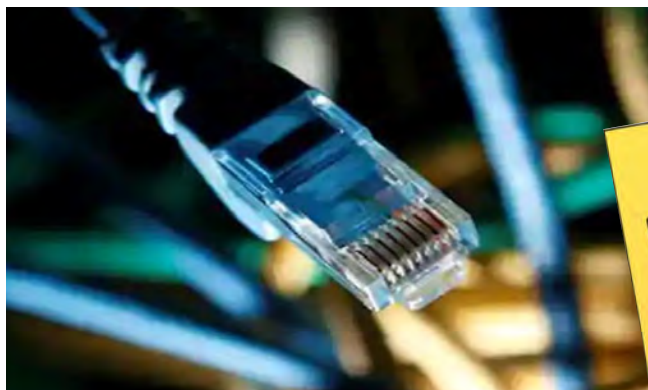
Working from home (WFH) used to be a luxury for the relatively affluent white-collared workers before coronavirus. This is not the case anymore. The pandemic is forcing more people to work from home in an unprecedented way.

We certainly do not need to know rocket science to be able to work from home or work from anywhere. Just by following some best practices, we can work from anywhere in a safe and efficient manner. Some of these best practices include avoiding unauthorized software and hardware, using office emails, securing home networks, using VPN clients to access work data, regularly updating security tools, avoiding potentially harmful websites and apps, collaborating securely, and using different networks for IoT devices, etc.

The coronavirus pandemic and the resulting need to work from home is

the epitome of the real-life use case for cloud-based for software-defined networks. By encrypting traffic and segmenting the network, IT teams are increasingly relying on SD-WAN to help improve network security and prioritize traffic. Most SD-WAN incorporates security solutions such as firewalls, anti-spam, and web filtering. These solutions help in preventing remote employees from accidentally leaking data or causing network security disruptions. In today's environment where MPLS is no longer feasible, and cloud usage has literally exploded, SD-WAN is a critical solution in improving a company's overall security posture. Offering solutions based on SASE architecture would be probably the best solution for companies to go completely remote and allow employees to work from anywhere.





## Membership and Associates:

- New members who joined the BIF family:
  - Patrons: **CISCO India, Lightstorm Communications and OneWeb**
  - Startups, Academia & Professionals: **Lekha Wireless Solutions, Mithril Telecommunications Pvt. Ltd.**
- **Ms. Amrita Choudhury, Director CCAOI and Brig. Anil Tandan (retd.) former CTO of Idea Cellular, joined BIF as Honorary Principal Advisors. .**



## Awards & Recognitions:

- Dr. Rishi Mohan Bhatnagar, Chairman of BIF's AI & IoT Committee, has been recognised as the **"IoT CEO of the Year 2020"** at **National Awards Excellence in IoT** on 14th October 2020
- Prof. Kiran Kuchi, Chairman, BIF Working Group on Academia & Standards, has been given additional responsibility in the role of **Dean R&D, IIT Hyderabad**
- **Ms. Amrita Choudhury, Principal Advisor, BIF has been appointed as an esteemed member of the Multistakeholder Advisory Group (MAG) for 2021 of the United Nations' (UN) Internet Governance Forum (IGF), as announced by UN Secretary-General António Guterres at the conclusion of the latest IGF**

### BIF Committees:

- **New Specialist Committee on FTTX formed, Chaired by Mr. Sanjeev Bedekar, Space TeleInfra, with Mr. Dhiraj Sharma, Jio as Co-Chair**
- **Content & Applications Committee retitled as Internet Content, Applications & Governance Committee (ICAG) to integrate a wider range of aspects pertinent to the sector**
- **The Technology, Media & Telecom (TMT) Committee has been merged with the ICAG Committee**
- **Cyber Trust & Safety Working Group formed – chaired by Ms. Amrita Choudhury, Principal Advisor, BIF. The objective of the WG is to explore various avenues for knowledge, awareness and capacity building for combating the rising threats to citizens from online/cyber-crimes and frauds via suitable outreach mediums to different components of the ecosystem – Government, LEAs, NGOs, Academic Institutions, Civic Bodies, general public, etc.**

### White Papers/Reports:

- A BIF White Paper on '[Proliferation of Broadband Through Wi-Fi](#)' authored by Mr. Punit Chawla, CMD, RailTel; Mr. Manohar Raja, Executive Director, RailTel; and Mr. TV Ramachandran, President, BIF; was released during The Digital Dialogues series on "The Role of Wi-Fi in Broadband Proliferation" held on 19<sup>th</sup> June 2020
- BIF White Paper on '[Priorities for a COVID-19 World: ICT Accessibility for Persons with Disabilities in India](#)' - authored by Dr. Nirmita Narasimhan, Chair of BIF's High-Level Specialist Committee on ICT for Inclusive Ability (for PwDs) and co-authored by Ms. Chandana Balasubramanian, Principal Consultant, Research & Content, advisory@TVR, released during a special session of The Digital Dialogues held on 10<sup>th</sup> August 2020
- A BIF White Paper on '[Internet Governance & Digital Cooperation: A Recommended Way Forward for India](#)' - co-authored by Ms. Amrita Choudhury, Director, CCAOI and Mr. TV Ramachandran, President, BIF, released during a special event held on 19<sup>th</sup> August 2020, to celebrate the 25th anniversary of the Internet in India
- BIF released its report on the legacy issues pertaining to spectrum auctions in India, titled '[Spectrum Pricing in India: Legacies, Challenges and Way Forward](#)' – authored by Mr. TV Ramachandran, President, BIF
- Mozark White Paper on '[Connected Experiences](#)' was released at The Digital Dialogues session on "Quality of Experience in Broadband" held on 14<sup>th</sup> September 2020

### White Papers/Reports in the Pipeline:

- A BIF White Paper on "Satellite Broadband Opportunities in 5G" is being developed.
- A comparative study on Internet and Broadband in Rural India is being developed with ICRIER



## Major Policy Developments:

- **Liberalisation of Space Activities including Satellite Communications:**
  - The Ministry of Finance, as part of the Economic Stimulus Package announced to combat the Covid19 pandemic, allowed participation of the private sector with a provision of a level playing field in commercial space activities, including the all-important Satellite Communications.
  - Satellite communication will play a vital role in Broadband proliferation across the nation, not only in those areas where terrestrial technologies find it unaffordable or extremely difficult to reach, but also as a vital essential backup in other areas.
  - This historic announcement marks a watershed moment in the country's space sector, which would attract huge FDI, lead to large employment generation due to several components of this activity manifesting itself as 'Make in India', will be open to healthy competition and a vibrant market, resulting in immense customer benefits besides manifold increase in govt revenues.



- **PM WANI Public Wi-Fi Scheme:**
  - In a landmark move, the Union Cabinet approved the establishment of Public Wi-Fi networks across the country under the Prime Minister Wi-Fi Access Network Interface (PM-WANI), based on the TRAI Recommendations on Proliferation of Broadband through Public Wi-Fi Networks.
  - This is aimed towards seamlessly delivering Wi-Fi services to the citizens via public data offices (PDOs), public data office aggregators (PDOAs) and app providers, thereby elevating seamless wireless internet connectivity in the country.
  - This will result in creation of millions of Wi-Fi hotspots to enable seamless delivery of affordable Wi-Fi services to the citizens at the grassroots level via unlicensed entities, thereby also propelling socio-economic growth by providing employment opportunities for small, local or village-level entrepreneurs (VLEs), besides propelling inclusion and rural digital connectivity.





## BIF Submissions and Interactions with Government

- BIF wrote to various Ministries on **disruption in the clearance of imported Electronics Manufacturing Industry goods** at various ports
- BIF wrote to the Department of Telecommunications (DoT) on **NDCP implementation and requesting to reinforce the speedy implementation of the released TRAI Recommendations on Proliferation of Broadband through Public Wi-Fi Networks**
- BIF wrote to the Ministry of Electronics and Information Technology (MeitY) and the Department of Empowerment of Persons with Disabilities (DePWD), Ministry of Social Justice & Empowerment, Government of India), **complimenting their efforts to make Aarogya Setu App accessible to Persons with Disabilities**
- BIF has written to **Hon'ble Minister of Communications requesting guidance and direction to help achieve the expeditious implementation of NDCP 2018**
- BIF also approached the **Hon'ble Minister of Communications regarding expediting the proliferation of Broadband via landline to facilitate Competition and Consumer benefits**
- BIF wrote to **DoT requesting for review and clarifications to DoT's Order dated 29-Aug-2018 on Public Procurement (Preference to Make in India) as well as on the proposed Telecom Manufacturing Production-Linked Incentives**
- BIF submitted request to **DoT to permit resumption of Aadhaar based e-KYC customer authentication at the earliest and waive off the e-KYC authentication charges levied by UIDAI**
- BIF submitted its comments and suggestions to MIB on **decriminalization of minor offences under the Cable Television Networks (Regulation) Act, 1995**
- BIF submitted its inputs to **DoT on Experimental Spectrum Committee Report** pertaining to Spectrum Regulatory Sandbox
- BIF submitted its inputs to DoT on **PMI-PP** w.r.t. to the discussion held regarding the same over a meeting held on 13<sup>th</sup> August with DoT
- BIF submitted its response to DoT on **New Framework for IP**
- BIF has written to DoT on issues pertaining to **WPC approvals for VSAT Service Providers**
- BIF submitted its response to DoT on the **pricing structure for usage of 'Indigenous 5G Test Beds'**
- BIF submitted its inputs to **DOT's Draft Report of the 5G Policy & Regulation Committee** which included a reference to International Best Practices on Common Ducts as well, besides a report on Small Cells (to be submitted later)
- BIF wrote to DoT on **opening up of E & V band spectrum**
- BIF had a virtual meeting with National E-Governance Division (NeGD) and MeitY to discuss the measures required on promoting ICT

accessibility **measures/initiatives for Persons with Disabilities (PwDs)**. BIF submitted a brief recommendation to MeitY w.r.t. to the meeting

- BIF had a virtual meeting with Registrar, Copyrights Office to discuss the **issues around the import and export of accessible format books in India**
- BIF comments were submitted to Directorate General of Civil Aviation (DGCA) on **Draft Revision to CAR Section 5 Series X Part I - Safety Hazard - Use of mobile/cellular telephones inside the flight**
- BIF submitted **Pre-Budget Recommendations on the Digital Communication Sector** to Finance Ministry and various other Ministries for FY 2021-22
- BIF provided its inputs to DoT on the Consultation on **PMI policy for telecom sector**
- BIF submitted its Comments on Discussion Paper for the **development of Indian Artificial Intelligence stack** to Telecom Engineering Centre (TEC)
- BIF inputs on the **draft Spacecom Policy - 2020 and Spacecom NGP (Norms, Guidelines and Procedures) 2020** were provided to Department of Space and other concerned Departments
- BIF submitted letter to DoT requesting for a **balanced Public Procurement Policy**
- BIF submitted a letter to Ministry of Housing and Urban Affairs (MoHUA), seeking advice on a **proposed Workshop on improving In-Building Solutions**. Consequently, BIF met with TCPO, MoHUA and discussed the various possibilities of improving In-Building Solutions in India

- BIF submitted its suggestions on the **Draft Data Center Policy** to MeitY
- BIF wrote a letter to DoT and ISRO seeking guidance and technical support to the BIF planned **co-existence study in the 6 GHz spectrum band**
- BIF submitted its interim suggestions/inputs as requested by DoT on the NDCP 2018 item no. 2.2. (a) (iv) **"Encourage use of Open APIs for emerging technologies"**
- BIF submitted its inputs/suggestions on **potential amendments to the Copyright Act, 1957**, as sought by the Registrar of Copyrights (RoC)

### TRAI Interactions/Submissions

- BIF wrote to TRAI regarding intervention in the Satcom sector w.r.t. the Hon'ble Finance Minister's **economic stimulus announcement on Space Activities**
- BIF made a detailed presentation to Chairman, TRAI on "Indian Digital Communications – Accelerators for Growth", highlighting the key issues of the sector and BIF's position on the same on 22<sup>nd</sup> October 2020
- BIF participated actively in the OHDs held virtually by TRAI on:
  - ▶ [Traffic Management Practices \(TMPs\)](#) & its effect on Net Neutrality held on 24<sup>th</sup> June 2020
  - ▶ [Framework for Technical Compliance of Conditional Access System \(CAS\) and Subscriber Management Systems \(SMS\) for Broadcasting & Cable Services](#) on 25<sup>th</sup> June 2020
  - ▶ [Methodology of applying SUC under the weighted average method of SUC assessment, in cases of Spectrum Sharing](#) on 9<sup>th</sup> July 2020
- BIF made submissions to TRAI Consultation/pre-consultation papers on the following issues:
  - ▶ [Enabling Unbundling of Different Layers Through Differential Licensing](#)
  - ▶ [Roadmap to Promote Broadband Connectivity and Enhanced Broadband Speed](#)
  - ▶ [MIB back reference on TRAI's Recommendations dated 19.11.2014 on 'Regulatory Framework for Platform Services' and MIB reference on TRAI's Recommendation on 'Platform Services offered by DTH Operators' dated 13.11.2019](#)

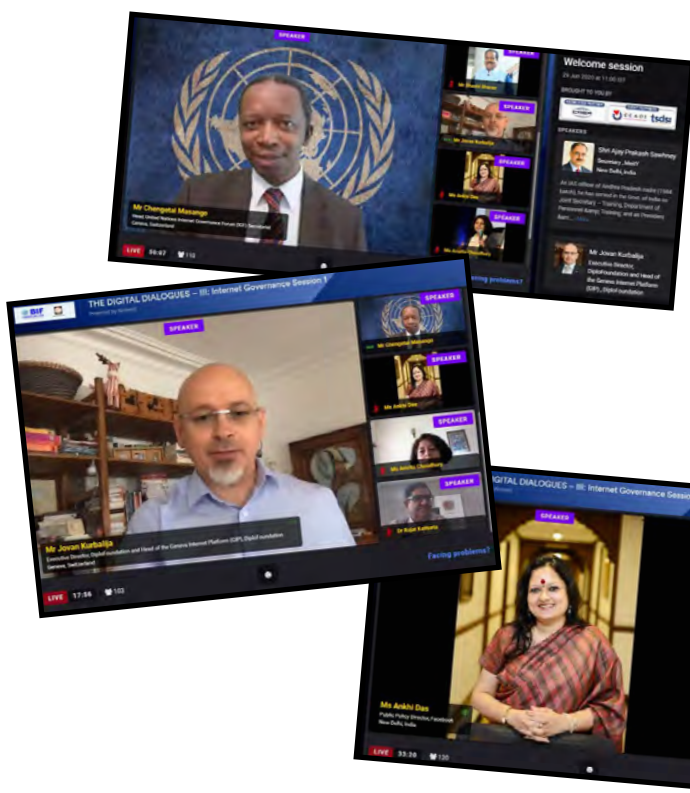
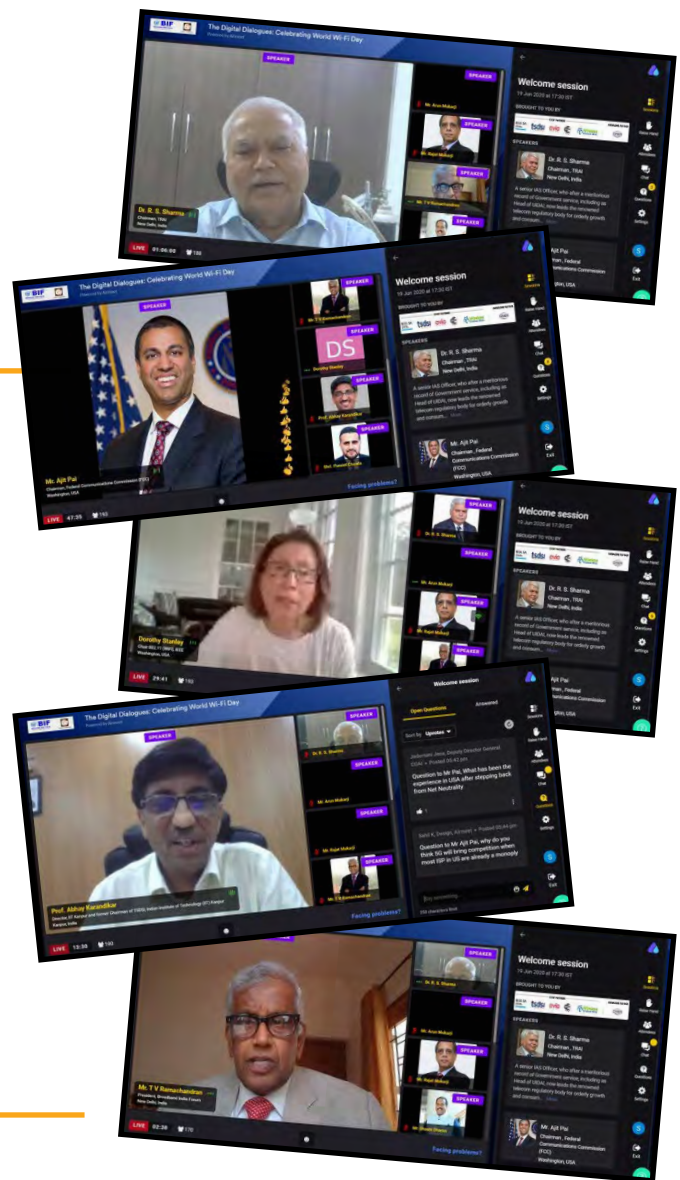




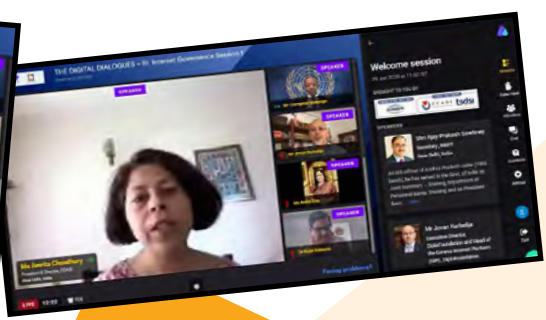


## (June, 2020)

**19<sup>th</sup> June 2020:** In celebration of the **World Wi-Fi Day**, BIF and Bharat Exhibitions, organised the **second of The Digital Dialogues series on “The Role of Wi-Fi in Broadband proliferation”** in association with TSDSI, IEEE, AVIA, WBA and Wi-Fi Alliance as Event Partners, and ICRIER as Knowledge Partner. In a high-level session, **Dr. RS Sharma, Chairman, TRAI**; and **Mr. Ajit Pai, Chairman, FCC, USA**; addressed the virtual conference on the vital issue as Session Chair and Chief Guest respectively. **Ms. Dorothy Stanley, Chair of Wi-Fi Working Group, IEEE**; and **Professor Abhay Karandikar, Director, IIT Kanpur and former Chairman of TSDSI**; also addressed the session as Special Guests of Honour



**29<sup>th</sup> June 2020:** The **Digital Dialogues series on Internet Governance** started with Session 1: Introduction to Internet Governance: Actors, Issues, Trends & Opportunities organised virtually partnership with CCAOI, TSDSI and ICRIER as Knowledge Partner. **Mr. Chengetai Masango, Head - United Nations Internet Governance Forum (IGF) Secretariat**; **Mr. Jovan Kurbalija, Director of Diplo Foundation and Head of the Geneva Internet Platform** and **Ms. Ankhi Das, Director - Public Policy, Facebook** joined as **Special Guests of Honour**. **Dr. Rajat Kathuria, Director and Chief Executive, ICRIER**, moderated the session





29<sup>th</sup> June – 3<sup>rd</sup> July 2020: AVIA's OTT Virtual Summit 2020 organised supported by BIF

## (July, 2020)

1<sup>st</sup> July 2020: Mr. Debashish Bhattacharya, DDG, BIF participated as Speaker/Panelist on behalf of Mr. TV Ramachandran, President, BIF; at the virtual **OFC Networks in India** event organised by **India Infrastructure**

3<sup>rd</sup> July 2020: Second Session of The Digital Dialogues series on Internet Governance on **Role of Internet Governance Platforms: ICANN & ISOC/IETF** organised in partnership with CCAOI, TSDSI and ICRIER as Knowledge Partner. **Dr. Gulshan Rai, Distinguished Fellow, ORF; Mr. Anupam Agarwal, Chair - India Internet Foundation; Shri T Santhosh, Scientist E, MeitY; Mr. Rajnesh Singh, Regional Vice President, Asia-Pacific, Internet Society; Mr. Samiran Gupta, Head of India, ICANN; and Mr. Molay Ghosh, General Manager – Network Planning & Architecture**, participated as eminent guest speakers



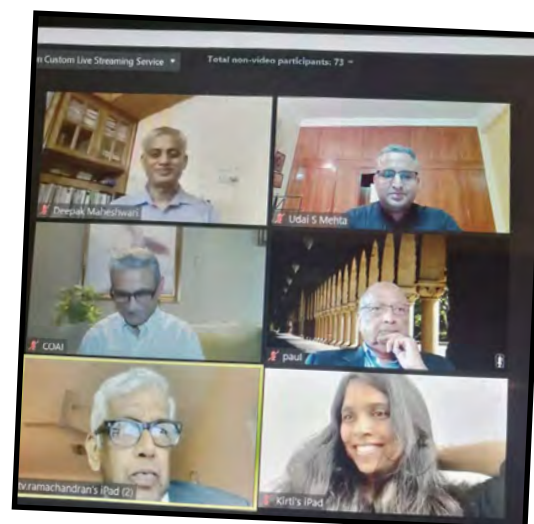
6<sup>th</sup> July 2020: Third & Final session of the Digital Dialogues series on Internet Governance on the **“Role of Internet Governance Platforms: APNIC”** held with participation from **Mr. K Ramchand, Member (T), Department of Telecommunications**, as Chief Guest; along with **Mr. Sanjay Goel, Joint Secretary, MeitY and CEO, NIXI; Mr. Ramesh Chandra, Vice President – Network Planning & Engineering, Reliance Jio; and Mr. Paul Wilson, Director General, APNIC** as eminent Guest Speakers



**8<sup>th</sup> July 2020: Mr. TV Ramachandran, President, BIF participated as a speaker in a Webinar on Myths and Realities of 5G in India** organised by CUTS International

**15<sup>th</sup> July 2020: “IEEE P2872TM, Standard for Interoperable and Secure Wireless Local Area Network (WLAN) Infrastructure and Architecture (ISAWANI)” Kick-Off Meeting** held Mr. Debashish Bhattacharya, DDG, BIF attended the meeting and will further participate in the development of the standard

**25<sup>th</sup> July 2020: Webinar on “An update on the Telecom Sector in India”** organised by Mr. Vijay Pahwa, wherein Mr. TV Ramachandran, President, BIF participated as a speaker and made a presentation on the topic



### (August, 2020)

**7<sup>th</sup> August 2020:** Mr. Umang Das, Chair of BIF's GPR Committee, moderated a webinar discussion by ET Telecom on **Shifting Telecom Gears from Evolution to Revolution: The Journey towards 5G**, with participation from Mr. TV Ramachandran, President, BIF and other senior Industry and Government representatives

**10<sup>th</sup> August 2020:** The Digital Dialogues IV on **ICT Accessibility for Persons with Disabilities** held with **Dr. Malcolm Johnson, Deputy Secretary-General, ITU**, present as **Chief Guest** accompanied by **Shri JS Deepak, Former Ambassador to WTO & Former Secretary - DoT**, as **Special Guest of Honour**; **Shri K Ramchand, Member (T), DoT** as **Guest of Honour**; with **Shri H K Mahajan, DDG (SR & E), DoT** and **Shri Vinay Thakur, COO, National eGovernance Division, MeitY** as eminent Guest Speakers





**19<sup>th</sup> August 2020:** BIF organised a high-profile virtual program to **celebrate the historical milestone of the completion of 25 years since the launch of Public Internet in India** with **Dr. RS Sharma, Chairman, TRAI as Chief Guest**; along with **Shri BK Syngal, Principal Advisor, BIF**; **Mr. Sanjay Mashruwala, Managing Director, Reliance Jio**; **Mr. Ashwani Rana, Vice President, BIF and Chair of BIF's Internet Content, Applications & Governance (ICAG) Committee**; and **Mr. Randeep Raina, Chief Technology Officer, Nokia India**



**26<sup>th</sup> August 2020:** Special Focused Session held with relevant stakeholders on **Use of Open Source Software** to help combat COVID-19 with presentation by **Prof. Ryosuke Shibasaki of Shibasaki Labs, University of Tokyo**

**27<sup>th</sup> August 2020:** Virtual Conference on **100 Smart Cities India 2020** organised by BE, wherein BIF participated as Knowledge Partner and Welcome Address was delivered by BIF President Mr. TV Ramachandran



**(September, 2020)**

**9<sup>th</sup> September 2020:** AGM (2019-2020) of IPTV Society (BIF)



**9<sup>th</sup> September 2020:** The Digital Dialogues on **"Digital Highway to 2025 - Suggested Milestones"** held with **Dr. RS Sharma, Chairman, TRAI** on the occasion of BIF AGM and 5<sup>th</sup> Anniversary Celebration





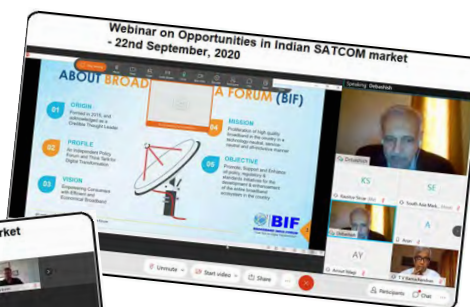
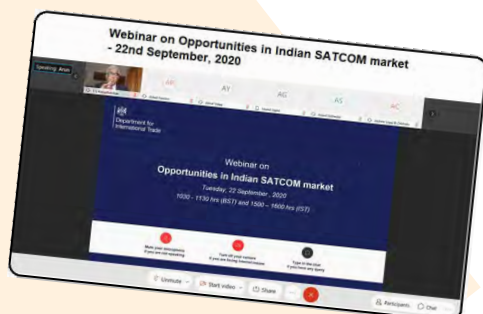
**14<sup>th</sup> September 2020:** The Digital Dialogues on “Quality of Experience in Broadband” organised with **Shri SK Gupta, Secretary, TRAI** as Chief Guest and **Dr. Rajat Kathuria, Director & CE, ICRIER**; **Mr. Bharat Bhargava, ASEAN Industry Market Leader (TMT), EY**; and **Mr. Udai Mehta, Deputy Executive Director, CUTS International** as Guest Speakers



**16<sup>th</sup> September 2020:** Wi-Fi Now organised a Special Virtual Event on **6 GHz Wi-Fi for India**, wherein BIF President **Mr. TV Ramachandran** participated as Guest Speaker



**22<sup>nd</sup> September 2020:** Focused stakeholder meeting held with the **UK High Commission** and **its members** on **Satcom opportunities** in India. Mr. T.V. Ramachandran delivered the keynote address



**24<sup>th</sup> September 2020:** IEEE organised a session for BIF Members on IEEE P1930.1 Standard on Recommended Practice for Software Defined Networking (SDN) based Middleware for Control and Management of Wireless Networks, and its status

**29<sup>th</sup> September 2020: Mr. TV Ramachandran, President, BIF** participated as a panelist along with other government and industry stalwarts in **Voice & Data's TLF Dialogue** on **"Network is the Lifeline of Our Society"**



**30<sup>th</sup> September 2020: Mr. Rajat Mukarji, DG, BIF** moderated a session on **'Exploring Community Networks'** at the Connected India Virtual 2020 event

## (October, 2020)

**14<sup>th</sup> October 2020:** The Digital Dialogues session on **'Digital Transformation: The Path to Exabyte Era'** held with participation from **Prof. Bhaskar Ramamurthi, Director, IIT Madras; Mr. Himanshu Kapania, Vice Chairman ABFRL & Director - Telecom, Aditya Birla Management Corporation; Dr. C S Rao, Chairman & Co-Founder, QuadGen Wireless Solutions Pvt. Ltd.; and Mr. Mohit Lohani, Sales Head - South Asia, Mozark**



**16<sup>th</sup> October 2020:** Mr. TV Ramachandran, President, BIF, participated as an expert speaker in a roundtable on **"Regulatory Design for a Trillion Dollar Digital Economy"** organised by the **Observer Research Foundation (ORF)** and **FICCI** at the **CyFy 2020**

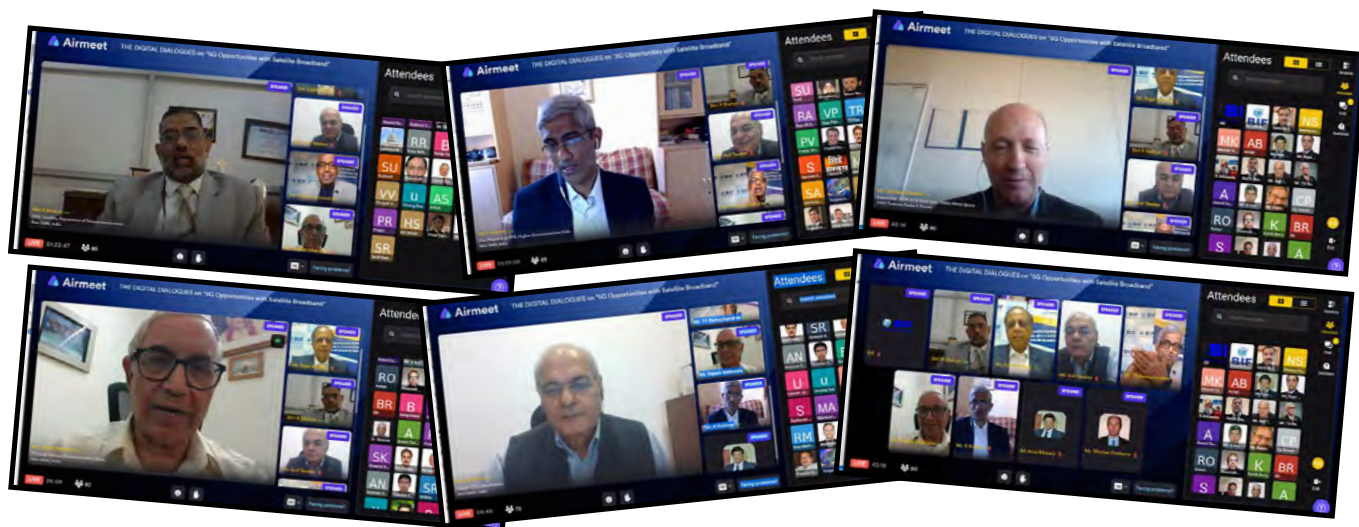
## (November, 2020)

**4<sup>th</sup> November 2020:** **5G India 2020** was organised by BE with BIF as Knowledge Partner





**17<sup>th</sup> November 2020:** The Digital Dialogues session on **5G Opportunities with Satellite Broadband** held with participation from **Mr. R Shakya, DDG, Satellite, DoT** as Chief Guest; **Mr. K Krishna, VP & CTO, Hughes Communications India;** **Mr. Nicolas Chuberre, Rapporteur, 3GPP Satellite Group;** **Mr. Rajesh Mehrotra, Principal Advisor, BIF** and **Mr. Anil Tandan, Former CTO, Idea Cellular** as Expert Speakers



**18<sup>th</sup> November 2020:** BIF, in association with ACTO and Khaitan & Co., co-hosted a webinar on **'New OSP Guidelines: A Game Changer for India's BPO Industry?'** with **Mr. TV Ramachandran, President, BIF**, participating amongst the eminent speakers



## India SatCom 2020:

**24<sup>th</sup> – 25<sup>th</sup> November 2020:** BIF's flagship annual **India SatCom 2020 Conference** organised successfully with over 500 participants/viewers across the Digital and Social Media platforms over the two days. Prominent participants in the **2-day event** included **Dr. K. Sivan, Chairman, ISRO & Secretary, Department of Space** as the Chief Guest; with **Shri K. Ramchand, Member (T), Ministry of Communications;** **Shri G. Narayanan, CMD, New Space India Ltd.;** and **Ms. Gita Krishnankutty, DIT, British High Commission** as Special Guests of Honour. Other speakers and esteemed participants included **Shri SK Gupta, Secretary, TRAI;** **Shri UK Srivastava,**

**Sr. DDG & Head, TEC;** **Dr. (Ms.) Archana Goyal Gulati, Joint Secretary, Communications, NITI Aayog;** **Shri R Shakya, DDG (Satellite), DoT;** **Shri Radhakrishnan D, Executive Director, NSIL;** besides leading industry stalwarts and experts from **Nelco, Hughes, Inmarsat, Telesat, SES, Methera, etc.**



## DAY 1: INAUGURAL SESSION







**DAY 2: Session 1 – Making IFMC services a major success in India**



**DAY 2: Session 2 – Rural Broadband – Satcom's Role**



**(December, 2020)**

**16<sup>th</sup> December 2020: Mr. TV Ramachandran, President, BIF and Dr. CS Rao, Chief Mentor – Technology, BIF participated in DigiAnalysys E-conference on “Growing Digital Industry Ecosystem, The Aatma Nirbhar Way” along with other eminent Government and Industry Panellists**



**17<sup>th</sup> December 2020: 7th edition of Data Centre India 2020 was organised by BE with BIF as Knowledge Partner**





# Mediascape

## Snapshots of some prominent Media Coverage received by BIF during July-December 2020

### Non-personal data regulations

#### Muzzling the roar of Make-in-India?

**RAMACHANDRAN TV**

India must not let itself away from the market-friendly approach that fuelled its explosive growth. It should incentivise data exchanges instead of mandating them.

In the world of intense competition, where only self-select apps that use to save and store sensitive personal data, the decision of a security agency platform to regulate user data will help users that these network and transfer more with a single hand app.

The growth of the media and industry is inseparable and very important for the country's progress. We need to ensure that the regulatory framework is not too strict and does not hamper the growth of the industry. The regulatory framework should be flexible and should allow the industry to innovate and grow.

From here, other players have begun to project similar transactions in India. The value of the total value of the transactions has increased. The value of the transactions has increased. The value of the transactions has increased.

### OTT Regulation

#### The brilliance of an unconventional approach

**RAMACHANDRAN TV**

TRAI has rightly determined that there is no need to regulate OTT players at this time - and in doing so, is one of the first in the world to champion this approach.

OTT players have been a part of the digital ecosystem for a long time. They have been a part of the digital ecosystem for a long time. They have been a part of the digital ecosystem for a long time.

OTT players have been a part of the digital ecosystem for a long time. They have been a part of the digital ecosystem for a long time. They have been a part of the digital ecosystem for a long time.

### Spectrum of Change

#### Unleashing V Band potential

**RAMACHANDRAN TV**

To realise the promise of the 60 GHz band and short range devices, India should declassify the band and avoid mandates on specific channelisation.

The 60 GHz band is a very important band for the future of the digital ecosystem. It is a very important band for the future of the digital ecosystem. It is a very important band for the future of the digital ecosystem.

The 60 GHz band is a very important band for the future of the digital ecosystem. It is a very important band for the future of the digital ecosystem. It is a very important band for the future of the digital ecosystem.

### Cashless Economy

#### Better digital security will make India a world leader

**RAMACHANDRAN TV**

Investing heavily in encryption and other security measures will be paramount to securing private data of all Indians.

The cashless economy is a very important part of the digital ecosystem. It is a very important part of the digital ecosystem. It is a very important part of the digital ecosystem.

The cashless economy is a very important part of the digital ecosystem. It is a very important part of the digital ecosystem. It is a very important part of the digital ecosystem.

### Global Satellite Industry (December 2020)

Global Satellite Industry (December 2020)

Country	Revenue (\$Bn)	Profit (\$Bn)	Market Share (%)
USA	1.2	0.3	35
Europe	0.8	0.2	25
Asia	0.5	0.1	15
Latin America	0.3	0.05	10
Africa	0.2	0.02	5
Middle East	0.1	0.01	3

### DoT should focus on ease of business, industry profitability, says Broadband India Forum

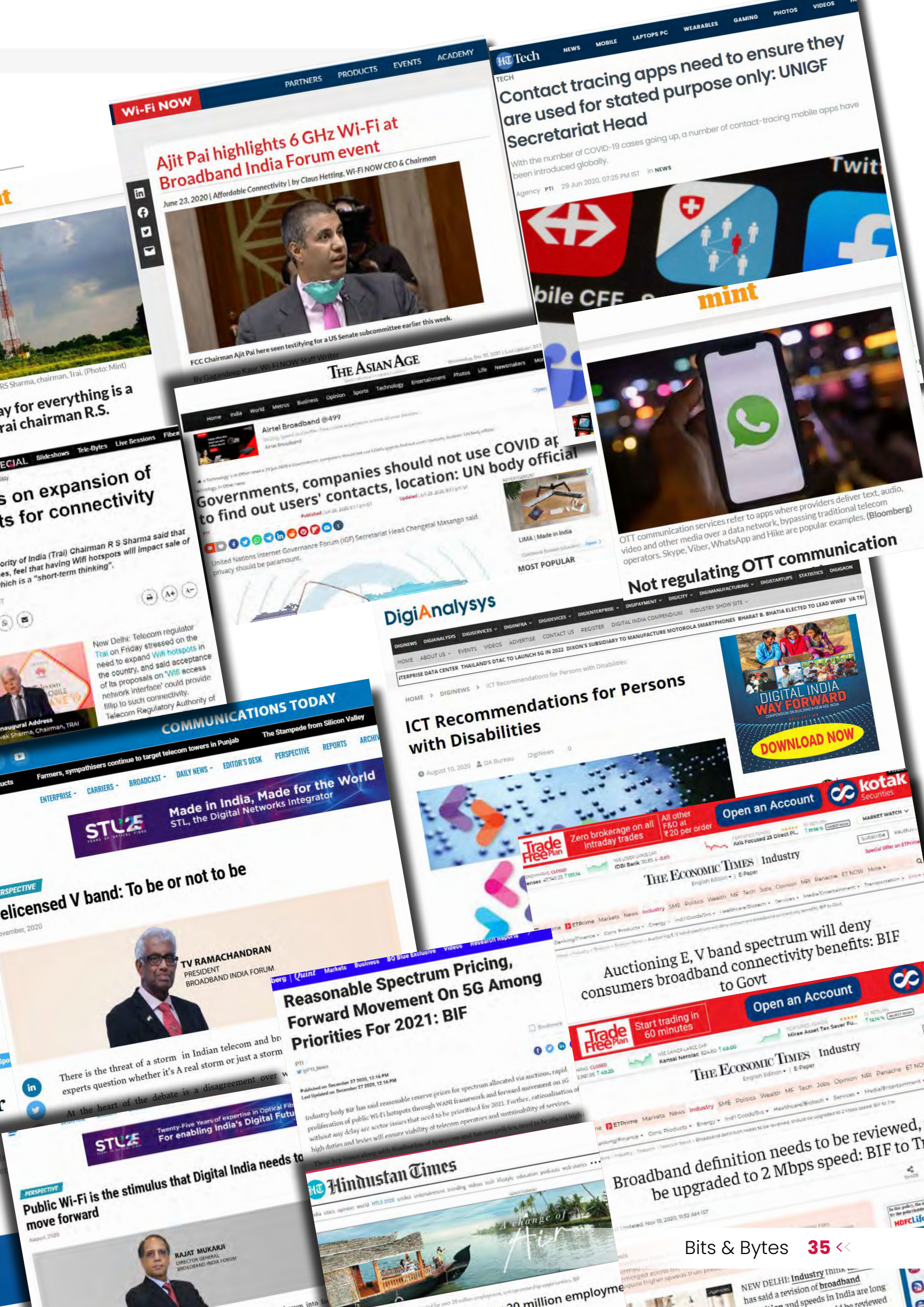
**34 Bits & Bytes**

DoT should focus on ease of business, industry profitability, says Broadband India Forum.

DoT should focus on ease of business, industry profitability, says Broadband India Forum.

DoT should focus on ease of business, industry profitability, says Broadband India Forum.





# Wi-Fi NOW

## Ajit Pai highlights 6 GHz Wi-Fi at Broadband India Forum event

June 23, 2020 | Affordable Connectivity | by Claus Hetting, Wi-Fi NOW CEO & Chairman



FCC Chairman Ajit Pai here seen testifying for a US Senate subcommittee earlier this week.

# 10 Tech

## Contact tracing apps need to ensure they are used for stated purpose only: UNIGF Secretariat Head

With the number of COVID-19 cases going up, a number of contact-tracing mobile apps have been introduced globally.

Agency PTI 29 Jun 2020, 07:25 PM IST in NEWS



ay for everything is a  
rai chairman R.S.

## on expansion of ts for connectivity

ity of India (Trai) Chairman R S Sharma said that  
es, feel that having Wifi hotspots will impact sale of  
hich is a "short-term thinking".

New Delhi: Telecom regulator  
Trai on Friday stressed on  
the need to expand Wifi hotspots in  
the country, and said acceptance  
of its proposals on 'Wifi access  
network interface' could provide  
fillip to such connectivity.  
Telecom Regulatory Authority of

## Airtel Broadband @499

Building Speed and better fibre-optic performance across all your devices.

Surf Broadband

## Governments, companies should not use COVID app to find out users' contacts, location: UN body official

United Nations Internet Governance Forum (IGF) Secretariat Head Chengeat Masango said  
privacy should be paramount.

Published: Jun 23, 2020 11:37 pm IST

Updated: Jun 23, 2020 11:37 pm IST



# DigiAnalysys

DIGINews DIGIServices DIGINFRA DIGIDEVICES DIGENTERPRISE DIGIPAYMENT DIGICITY DIGIMANUFACTURING DIGISTARTUPS DIGISTATISTICS DIGISOCIAL

HOME ABOUT US EVENTS VIDEOS ADVERTISE CONTACT US REGISTER DIGITAL INDIA COMPENDIUM

ENTERPRISE DATA CENTER THAILAND'S DTAC TO LAUNCH 5G IN 2022 DIXON'S SUBSIDIARY TO MANUFACTURE MOTOROLA SMARTPHONES BHARAT B. BHATTIA ELECTED TO LEAD WWRF VA TO

## ICT Recommendations for Persons with Disabilities

August 10, 2020 DA Bureau DigNews 0



## COMMUNICATIONS TODAY

The Stampede from Silicon Valley

ENTERPRISE - CARRIERS - BROADCAST - DAILY NEWS - EDITOR'S DESK PERSPECTIVE REPORTS ARCHIVE

STU2 YEARS OF OPTICAL FIBRE

Made in India, Made for the World  
STL, the Digital Networks Integrator

There is the threat of a storm in Indian telecom and broadband experts question whether it's a real storm or just a storm

At the heart of the debate is a disagreement over whether

TV RAMACHANDRAN  
PRESIDENT  
BROADBAND INDIA FORUM

There is the threat of a storm in Indian telecom and broadband experts question whether it's a real storm or just a storm

At the heart of the debate is a disagreement over whether

Public Wi-Fi is the stimulus that Digital India needs to move forward

RAJAT MUKARJI  
DIRECTOR GENERAL  
BROADBAND INDIA FORUM

Public Wi-Fi is the stimulus that Digital India needs to move forward

Public Wi-Fi is the stimulus that Digital India needs to move forward

Public Wi-Fi is the stimulus that Digital India needs to move forward

Trade Free Plan Zero brokerage on all intraday trades All other F&O at ₹20 per order

THE ECONOMIC TIMES Industry English Edition | E-Paper

Auctioning E, V band spectrum will deny consumers broadband connectivity benefits: BIF to Govt

Trade Free Plan Start trading in 60 minutes

THE ECONOMIC TIMES Industry English Edition | E-Paper

Broadband definition needs to be reviewed, be upgraded to 2 Mbps speed: BIF to T

Hindustan Times

A change of...

20 million employees



## PATRON MEMBERS



## CORPORATE MEMBERS



## STARTUP & PROFESSIONAL MEMBERS



## ACADEMIA/RESEARCH INSTITUTIONS









# REPORTS & PUBLICATIONS



# Partnerships & Engagements



Supported by





## ORIGIN

Formed in 2015



## PROFILE

An Independent Policy Forum and Think Tank for Digital Transformation



## VISION

Empowering Consumers with Efficient and Economical Broadband



## MISSION


Proliferation of high quality broadband in the country in a technology-neutral, service-neutral and all-inclusive manner



## OBJECTIVE

Promote, Support and Enhance all policy, regulatory & standards initiatives for the development & enhancement of the entire broadband ecosystem in the country



The background of the entire page is a night-time photograph of a city skyline, featuring several illuminated skyscrapers. Overlaid on this image are three sets of concentric circles, each centered on a different building, with thin lines radiating from these centers across the sky. A large, stylized yellow arrow graphic is positioned on the right side of the page, pointing towards the left.

**Disclaimer:** BIF has used its best efforts in collecting and preparing this Newsletter and accepts no liability of the content of this Newsletter, or for the consequences of any actions taken on the basis of the information provided for any incorrect information supplied to by our Newsletter.

BIF does not assume and hereby disclaims any liabilities for any loss and damage caused by errors omissions in preparing this Newsletter, whether such errors or omissions result from negligence, accident or other causes.

BIF reserves all rights herein. This document is to be used for internal use only by intended person. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited without the written permission of the publisher.

For information regarding permission, write to Mr. Rajat Mukarji, Director General, Broadband India Forum, Suites - 215 & 216, DBS Office Business Centre, 1st Floor, World Trade Tower, Barakhamba Lane, New Delhi-110001



**Newsletter Development Team:**

Kaustuv Sircar, Neema Sunil Kumar and Seema Santosh

**Publisher:**

Rajat Mukarji, Director General, Broadband India Forum, Suites - 215 & 216,  
DBS Office Business Centre, 1<sup>st</sup> Floor, World Trade Tower, Barakhamba Lane, New Delhi-110001

Find us on:



broadband-india-forum



@ConnectBIF



broadband india forum



[www.broadbandindiaforum.com](http://www.broadbandindiaforum.com)