



गेल (इंडिया) लिमिटेड

(भारत सरकार का उपक्रम – महारत्न कंपनी)

GAIL (India) Limited

(A Government of India Undertaking - A Maharatna Company)

गेल भवन,
16 भीकाएजी कामा प्लेस
नई दिल्ली-110066, भारत
GAIL BHAWAN,
16 BHIKAJI CAMA PLACE
NEW DELHI-110066, INDIA
फोन/PHONE: +91 11 26182955
फैक्स/FAX: +91 11 26185941
ई-मेल/E-mail: info@gail.co.in

ND/GAIL/SECTT/2021

10.06.2021

1. Listing Compliance National Stock Exchange of India Limited Exchange Plaza, 5th Floor, Plot No. C/1, G Block, Bandra-Kurla Complex, Bandra (East) Mumbai – 400051 Scrip Code: GAIL-EQ	2. Listing Compliance BSE Limited Floor 1, Phiroze Jeejeebhoy Towers Dalal Street Mumbai – 400001 Scrip Code: 532155
---	---

**Sub.: Newspaper Publication of the Audited Financial Results for the quarter/year ended
31st March, 2021 Regarding**

Dear Sir,

This is in compliance of Regulation 30 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.

With reference to the subject cited above, please find the attachment.

The above is for your information and records.

Thanking you,
Yours faithfully,


(A.K. Jha)
Company Secretary


Bug bounty hunters working to keep firms cyber secure

SHIVANI SHINDE
Mumbai, 9 June

Take any security research report and you will find India topping the list of data breaches and cyberattacks. In February 2021 — almost a year since the pandemic landed on Indian shores — there were 377.5 million brute-force attacks globally. India accounted for 9.04 million of those. The total number of cyberattacks recorded in India during January and February 2021 was around 15 million, according to a Kaspersky report.

While many of the companies targeted had robust technology in place to prevent such incidents or mitigate their risk, security experts say the recent spate of data breaches is not just about technology. “In our world, we say security has three components: People, process and technology. While everyone is focusing on the tech part, there is very little importance given to people and the awareness of security,” says Sandeep Sengupta, managing director of Kolkata-headquartered Indian School of Ethical Hacking (ISOEH).

This is where an army of independent ethical hackers — also called “bug bounty hunters” — comes in. Many of them are certified cybersecurity professionals or security researchers. They crawl the web, scanning the systems for gaps through which hackers can sneak in and alert the companies. In return, they are rewarded with cash or kind.

Not leaving it to chance for such gaps to be discovered, some companies now actively employ the services for bug bounty hunters.

Online brokerage firm Zerodha is one of them. Its Chief Technical Officer Kailash Nadih says in-house teams alone cannot make the system fully secure. “Having ethical hackers or security engineers is essential. Though we have an internal security team, we also have a bug bounty programme and employ external white-hat (ethical) hackers to regularly test our systems from the outside,” says Nadih. “We have so far managed to stave off serious cyberattacks.”

This happened with Upstox, a leading player in the stockbroking segment and Zerodha’s competitor. A breach had targeted the data of



Warding off hackers

► Bug Bounty programme allows hackers (white-hat hackers) to receive compensation for reporting bugs, vulnerabilities and possible exploits

► In 1983, the first bug bounty programme was started by Hunter and Ready for their real-time executive operating system. The reward for finding a bug was a Volkswagen Beetle

► In 1995, Netscape Communications Corporation launched the first bug bounty programme for Netscape Navigator 2.0 beta browser

► 2013 onwards Facebook started paying researchers to find and report security bugs

► Facebook and Microsoft in 2013 partnered and sponsored The Internet Bug Bounty programme

► In 2016, after security breach, Uber, which paid a ransom of \$100,000 to get its data back, reworked its bug bounty programme with partner HackerOne

► Several companies and countries today support the bug bounty programme

some 2.5 million of its customers. The retail broking firm had then immediately alerted the customers while assuring them that their funds and securities were safe.

Sourajeet Majumder, a Class XII student, is a part-time bug bounty hunter. In his spare time, he crawls through company websites to find vulnerabilities and report them. In return, he either gets paid in cash or is rewarded in kind (with t-shirts or bags etc). He recently found a vulnerability in West Bengal’s health ministry website. Had the bug not been fixed, data of over 8 million people could have been leaked on the dark web.

Majumder started out hunting bugs for large corporations as a pastime. He found his first bug in the social media microblogging website Tumblr, for which he was paid ₹15,000. “I have found vulnerabilities

in many of the government sites, too, and I try to report them to the people concerned,” he says.

Bug bounty programme is well-known in the US and Europe. Started in 1983, it caught on after 2013 when companies like Facebook, Yahoo, Google started to leverage it. US and India are now among the top countries from where researchers submit bugs.

Anand Prakash, founder of PingSafe, a Bengaluru-based cybersecurity company, is counted among the world’s leading bug bounty hunters. He says one reason for a spike in data breaches in India is the rise of the unicorns and the start-up ecosystem. “India is suddenly in news for the rising numbers of unicorns, so cyber criminals have their eye on it,” he says, adding, “If you see some of the latest hacks, they are all in new-generation firms like

BigBasket, Upstox, Domino’s etc.” The first security bug that Prakash spotted was in Facebook. He has since been rewarded and acknowledged by Facebook, Twitter, Google, Red Hat, Dropbox, Adobe and others. “Most companies say they are 100 per cent secure; that’s far from reality,” he says. Cybersecurity cannot be managed by just a handful of people. “In that sense, having a bounty programme is useful.”

The challenge, however, is that even today few companies understand or acknowledge the work that these ethical hackers do. “India has a peculiar situation. When we find and report a bug/vulnerability to a company, we are often treated as black-hat (unethical) hackers and they take legal action against us,” says Prakash.

A recent example is when security researcher Rajshekhar Rajaharia posted what he said were the details of MobiKwik user data available on the dark web. While the company denied the breach, Twitter temporarily blocked Rajaharia’s account. Prakash has had a similar experience as a bug hunter when an Indian company took legal action against him for letting them know that there was a vulnerability. “They said, ‘Why were you checking our systems?’”

Also, Indian bug hunters who are globally rewarded for finding vulnerabilities are poorly paid in their own country. “In India, a billion-dollar company will pay just about a few thousand rupees. Some bug hunters get disillusioned and take advantage of the information they have,” says Prakash.

Sengupta of ISOEH points to the demand-supply gap. “According to a Nasscom survey, India needs 500,000 ethical hackers in the next five years,” he says, adding that currently it has barely 70,000.

Dipesh Kaura, general manager, Kaspersky (South Asia), adds: “In general, data breaches happen due to weaknesses in technology and user behaviour. While enterprises build a robust security infrastructure for their networks, they often fail to protect themselves from the two other equally important aspects: Human error and third-party services/providers.”

A lotus-shaped landing field in Navi Mumbai

GVK group reveals airport design as it bids adieu to airport sector



ANEESH PHADNIS
Mumbai, 9 June

The Navi Mumbai international airport will boast three interconnected multi-level terminals with a lotus-inspired design, according to the master plan prepared by its outgoing developer. The GVK group, which completed 15 years of airport business, shared the first look of the Navi Mumbai airport on Tuesday.

The group in 2018 had commissioned British firm Zaha Hadid Architects to design the main terminal and air traffic control tower. The master plan of the airport was approved by the City and Industrial Development Corporation (CIDCO) in 2019.

The airport will be developed in four phases. After the first phase it will be able to handle a minimum of 10 million passengers. According to the master plan, the airport’s main terminal (T1) that will be built in phase one would have two floors with very few level changes and minimum walking distances. The

airport would eventually have a passenger handling capacity of 90 million per year.

The airport will be built over 1,160 hectares, over 95 per cent of which has been acquired from local villagers. Hill cutting and land filling works are on. The site had a cluster of villages with ponds full of lotuses and that inspired the terminal design.

Last August, the GVK group announced an exit from the airport sector selling its stake in Mumbai airport to the Adani group. The actual handover is, however, yet to happen.

According to the concession agreement between CIDCO and GVK, the date of commercial operations of the Navi Mumbai airport was fixed at this year-end. This would need to be amended. Also, given the changed business environment and sharp fall in traffic last year, the Adani group may review and revisit the construction plans.

Both Adani and GVK groups declined to respond to queries on the matter.



The airport will be developed in four phases. After the first phase, it will be able to handle a minimum of 10 mn passengers



Kant to telecom gear firms: Have atma vishwas

SURAJEET DAS GUPTA
New Delhi, 9 June

Niti Aayog CEO Amitabh Kant, in a straight talk with leading and potential global telecom equipment-makers such as Ericsson and Nokia, made it clear today that Free Trade Agreements (FTAs) with ASEAN countries are here to stay. Indian companies, he said, should not promote protectionism but build scale and size to compete with the world.

Kant was responding to the demand by telecom equipment-makers that the government should rectify the “anomaly” that has occurred due to India’s FTAs with Southeast Asian countries that allow them to export telecom components to India duty-free, thus obviating the need for them to set up plants here. Telecom equipment players pointed out that these have made it difficult for them to increase value-addition in telecom equipment. And this also does not allow foreign



Indian companies, the Niti Aayog CEO said, should not promote protectionism but build scale and size to compete with the world

globalised world today and FTAs, bilateral trading relationships will stay. But saying that everything is getting imported through FTAs is not a right approach. Problem is that Indian manufacturers should not promote protectionism.”

He told the telecom equipment-makers that they “should have the guts and the courage” to take on global competition and advised the telecom companies to “have atma vishwas (self-confidence).”

Kant pointed out that the global supply chain is in a flux

as most countries are looking at alternatives and reducing their dependence on one country (meaning China). “We will never be able to seize this opportunity if we don’t move.” Telecom equipment-makers also demanded that the production-linked incentive scheme be linked to the preference to Make in India (PMI) scheme as

global players with manufacturing facilities in India are finding it difficult to participate in government procurement orders. They suggested that the PMI scheme should be leveraged to enable exports — one way being to grant points to the total value of exports that can be used by them to qualify more easily for government procurement contracts.

Kant said that a meeting with telecom equipment-makers will be called next week on this demand.



GAIL (India) Limited

(A Govt. of India Undertaking)

ENERGIZING POSSIBILITIES FOR A RESILIENT NATION



Extract from the Audited Standalone and Consolidated Financial Results for the Quarter and Financial Year Ended 31st March 2021

(₹ in crore Except EPS)

Sl. No.	Particulars	Standalone				Consolidated			
		Quarter Ended		Financial Year Ended		Quarter Ended		Financial Year Ended	
		31st March 2021	31st March 2020	31st March 2021	31st March 2020	31st March 2021	31st March 2020	31st March 2021	31st March 2020
		Audited	Audited	Audited	Audited	Audited	Audited	Audited	Audited
1.	Total income from operations	15,549.07	17,755.01	56,737.79	71,885.63	15,757.16	17,938.08	57,428.26	72,576.98
2.	Net Profit / (Loss) for the period (before Tax, Exceptional and/or Extraordinary items)	2,611.59	2,555.70	6,385.81	7,943.36	3,218.85	3,598.70	7,725.45	10,428.94
3.	Net Profit / (Loss) for the period before tax (after Exceptional and/or Extraordinary items)	2,611.59	2,555.70	6,385.81	7,943.36	3,218.85	3,598.70	7,725.45	10,428.94
4.	Net Profit / (Loss) for the period after tax (after Exceptional and/or Extraordinary items)	1,907.67	3,018.20	4,890.18	6,620.63	2,534.64	4,813.88	6,142.82	9,514.64
5.	Total Comprehensive Income for the period [Comprising Profit / (Loss) for the period (after tax) and Other Comprehensive Income (after tax)]	2,635.44	1,375.69	6,172.57	3,820.67	3,140.18	3,259.88	7,468.77	6,781.75
6.	Paid up Equity Share Capital (Face value of ₹10/- each)	4,440.39	4,510.14	4,440.39	4,510.14	4,440.39	4,510.14	4,440.39	4,510.14
7.	Reserve excluding Revaluation Reserves as per balance sheet			39,043.09	37,529.45			42,792.37	42,888.15
8.	Earning Per Share (Face value ₹10/- each)								
	(a) Basic	4.24	6.69	10.85	14.68	5.52	10.48	13.61	20.89
	(b) Diluted	4.24	6.69	10.85	14.68	5.52	10.48	13.61	20.89
	(EPS for the quarter not annualized)								

Notes:-

- The above is an extract of the detailed format of financial results for the Quarter and Financial Year ended 31st March 2021 filed with the Stock Exchanges under Regulation 33 of SEBI (Listing and Other Disclosure Requirements) Regulations, 2015. The full format of the financial results are available on the Stock Exchanges website (www.nseindia.com, www.bseindia.com) and Company's website (www.gailonline.com).
- The above results are in accordance with the Companies (Indian Accounting Standards) Rules, 2015, (Ind AS) prescribed under Section 133 of the Companies Act, 2013, read with the relevant rules issued thereunder and other accounting principles generally accepted in India.
- Figures for the previous periods have been regrouped, wherever necessary, to conform to the current period's classification.

Place : New Delhi
Date : 9th June, 2021

(CIN: L40200DL1984GOI018976)

For GAIL (India) Limited
Sd/-
(A K Tiwari)
Director (Finance) & CFO
(DIN: 07654612)

www.gailonline.com | Regd. Office : 16, Bhikaiji Cama Place , R.K. Puram, New Delhi - 110 066 | Follow us on [f](#) [in](#) [t](#) [w](#)



