रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-29082024-256727
CG-DL-E-29082024-256727

असाधारण
EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (i)
PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 481] नई दिल्ली, बुधवार, अगस्त 28, 2024/ भाद्र 6, 1946
No. 481] NEW DELHI, WEDNESDAY, AUGUST 28, 2024/ BHADRA 6, 1946

संचार मंत्रालय

(दूरसंचार विभाग)

अधिसूचना

नई दिल्ली, 28 अगस्त, 2024

सा.का.नि. 520(अ).— निम्नलिखित मसौदा नियम जिसे केंद्रीय सरकार दूरसंचार अधिनियम, 2023 (2023 का 44) की धारा 56 की उप-धारा (2) के खंड (V) के साथ पठित धारा 22 की उप-धारा (1) के तहत प्रदत्त शक्तियों का प्रयोग करते हुए बनाने का प्रस्ताव करती है, को इससे प्रभावित होने वाले सभी व्यक्तियों की सूचना के लिए प्रकाशित किया जाता है और एतद्वारा नोटिस दिया जाता है कि उक्त मसौदा नियमों पर उस तारीख से तीस दिन की अवधि की समाप्ति के पश्चात् विचार किया जाएगा जिस तारीख से सरकारी राजपत्र में यथा प्रकाशित इस अधिसूचना की प्रतियां सर्वसाधारण को उपलब्ध कराई जाती हैं;

यदि कोई आपत्ति अथवा सुझाव हो तो संयुक्त सचिव (दूरसंचार), दूरसंचार विभाग, संचार मंत्रालय, भारत सरकार, संचार भवन, 20, अशोक रोड, नई दिल्ली-110001 को भेजा जा सकता है;

केंद्रीय सरकार द्वारा उपर्युक्त अवधि की समाप्ति से पूर्व उक्त मसौदा नियमों के संबंध में किसी व्यक्ति से प्राप्त आपत्तियों अथवा सुझावों पर विचार किया जाएगा।

1. संक्षिप्त नाम, प्रारंभ और व्यावृति

(1) इन नियमों को दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 कहा जा सकता है।

(2) ये सरकारी राजपत्र में प्रकाशन की तिथि से प्रवृत्त होंगे।

(3) ये नियम भारतीय तार अधिनियम, 1885 (1885 का 13) के तहत मोबाइल डिवाइस उपकरण पहचान संख्या की छेड़छाड़ की रोकथाम नियम, 2017 और मोबाइल डिवाइस उपकरण पहचान संख्या (संशोधन) नियम, 2022 का अधिक्रमण करेंगे परन्तु उन नियमों के तहत की गई कार्रवाई के निबंधन और शर्तों को अधिभूत नहीं करेंगे जिनमें उन नियमों के अनुसार किए गए पंजीकरण भी शामिल हैं।

2. परिभाषाएँ

(1) इन नियमों में जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,

(क) "अधिनियम" से दूरसंचार अधिनियम, 2023 (2023 का 44) अभिप्रेत है;

(ख) "मुख्य दूरसंचार सुरक्षा अधिकारी" से इन नियमों के नियम 6 के तहत नियुक्त दूरसंचार संस्था के अभिनामित कर्मचारी अभिप्रेत है।

(ग) "दूरसंचार नेटवर्क और दूरसंचार सेवाओं की साइबर सुरक्षा" अथवा "दूरसंचार साइबर सुरक्षा" का अभिप्राय उपकरण, नीति, सुरक्षा अवधारणा, सुरक्षा संबंधी उपाय, दिशा-निर्देश, जोखिम प्रबंधन दृष्टिकोण, कार्रवाई, आश्वासन और प्रौद्योगिकी है जिनका उपयोग दूरसंचार नेटवर्क और दूरसंचार सेवाओं की सुरक्षा करने और साथ ही व्यक्तियों की परिसंपत्तियों के लिए किया जा सकता है जिनमें साइबर एनवायरनमेंट; संबंधित सुरक्षा जोखिमों के लिए कनेक्ट किए गए दूरसंचार उपकरण, दूरसंचार सेवाएं, अवसंरचना, एप्लीकेशन और समग्र प्रेषित और/या एकत्रित सूचना शामिल है;

(घ) "नियमों" से दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 अभिप्रेत है;

(ङ) "सुरक्षा घटना" से ऐसी घटना अभिप्रेत है जिसका दूरसंचार साइबर सुरक्षा पर वास्तविक या संभावित प्रतिकूल प्रभाव पड़ता हो;

(च) "दूरसंचार संस्था" से इस अधिनियम की धारा 3 की उप-धारा (।) के अंतर्गत प्राधिकार प्राप्त प्राधिकृत कंपनी अथवा इस अधिनियम की धारा 3 की उप-धारा (3) के अंतर्गत प्राधिकार की आवश्यकता से छूट प्राप्त व्यक्ति सहित दूरसंचार सेवाएं उपलब्ध कराने अथवा दूरसंचार नेटवर्क स्थापित करने, उसका प्रचालन रखरखाव अथवा विस्तार करने वाला कोई व्यक्ति अभिप्रेत है।

(छ) "दूरसंचार उपकरण पहचान संख्या" से दूरसंचार पहचानकर्ता अभिप्रेत है जिसमें एक या एक से अधिक निम्नलिखित विशेषताएं मौजूद हैं:

i) अंतर्राष्ट्रीय मोबाइल उपकरण पहचान (आईएमईआई) संख्या; या

ii) इलेक्ट्रॉनिक क्रम संख्या (ईएसएन); या

iii) अन्य कोई संख्या या संकेत जो यूनिक दूरसंचार उपकरण को चिन्हित करता है।

(ज) "ट्रैफिक डेटा" से दूरसंचार के प्रकार, राउटिंग, अवधि या समय से संबंधित डेटा सहित दूरसंचार नेटवर्क में सृजित, प्रेषित, प्राप्त या संग्रहित कोई डेटा अभिप्रेत है।

(2) उन शब्दों और पदों जिनका उपयोग इन नियमों में किया गया है और जिन्हें परिभाषित नहीं किया गया है परन्तु जिन्हें अधिनियम में परिभाषित किया गया है, के वही अर्थ होगें जो अधिनियम में विनिर्दिष्ट किया गया है।

3. डेटा संग्रह, शेयरिंग और विश्लेषण

(1) केंद्रीय सरकार या केंद्रीय सरकार द्वारा इस संबंध में प्राधिकृत कोई एजेंसी सुरक्षा प्रयोजन से और दूरसंचार साइबर सुरक्षा सुनिश्चित करने के लिए:

(क) इस प्रयोजन के लिए केंद्रीय सरकार द्वारा यथा अधिसूचित प्रारूप और ढंग से दूरसंचार संस्था, ट्रैफिक डेटा और अन्य किसी डेटा की मांग कर सकती है; या

(ख) किसी दूरसंचार संस्था को विनिर्दिष्ट पॉइंट से इस प्रकार के डेटा का संग्रह करने और उसे उपलब्ध कराने के लिए आवश्यक अवसंरचना और उपकरण संस्थापित करने के लिए निर्देश दे सकती है जो इसके प्रोसेसिंग और भंडारण को समर्थ बनाये।

(2) उप-नियम (1) के तहत संग्रहित डेटा का विश्लेषण दूरसंचार साइबर सुरक्षा बढ़ाने के उपाय करने के लिए किया जा सकता है और यदि केंद्रीय सरकार सुरक्षा प्रयोजन से और दूरसंचार साइबर सुरक्षा सुनिश्चित करने के लिए ऐसा करना निश्चित करती है, वह

(क) कानून प्रवर्तन और सुरक्षा संबंधी गतिविधियों में शामिल केंद्रीय सरकार की किसी भी एजेंसी को इसका प्रसार कर सकती है; और

(ख) दूरसंचार संस्थाओं या प्रयोक्ताओं के साथ शेयर किया जा सकता है;

(3) केंद्रीय सरकार और इन नियमों के तहत डेटा संग्रह करने के लिए केंद्रीय सरकार द्वारा प्राधिकृत कोई एजेंसी और साथ ही ऐसे व्यक्ति जिनके साथ उप-नियम (2) के तहत इस प्रकार का डेटा शेयर किया जाता है, ऐसे डेटा तक किसी भी अनधिकृत पहुंच को रोकने के प्रयोजन से केंद्रीय सरकार द्वारा यथा अधिसूचित किसी भी विशिष्ट सुरक्षा संबंधी उपायों सहित पर्याप्त सुरक्षा संबंधी उपाय लागू करें।

(4) इन नियमों के तहत संग्रहित डेटा का उपयोग या खुलासा दूरसंचार साइबर सुरक्षा सुनिश्चित करने के अलावा अन्य किसी प्रयोजन के लिए नहीं किया जाएगा।

4. दूरसंचार साइबर सुरक्षा से संबंधित दायित्व

(1) कोई भी व्यक्ति दूरसंचार साइबर सुरक्षा को खतरे में नहीं डालेगा।

(2) दूरसंचार नेटवर्क या दूरसंचार सेवा का उपयोग करके कोई भी संदेश नहीं भेजा जाएगा जो दूरसंचार साइबर सुरक्षा पर प्रतिकूल प्रभाव डालता हो।

(3) उप-नियम (1) और उप-नियम (2) की व्यापकता पर प्रतिकूल प्रभाव डाले बिना कोई भी व्यक्ति दूरसंचार उपकरण या दूरसंचार पहचानकर्ता या दूरसंचार नेटवर्क या दूरसंचार सेवाओं का उपयोग नहीं करेगा जिसमें निम्नलिखित शामिल हैं:

(क) जालसाजी, धोखाधड़ी या प्रतिरूपण;

(ख) किसी भी ऐसे संदेश को प्रेषित नहीं करेगा जो जालसाजी पर आधारित हो;

(ग) किसी भी सुरक्षा घटना को अंजाम नहीं देगा या सुरक्षा घटना घटित करने का आशय नहीं रखेगा, या

(घ) ऐसे किसी अन्य उपयोग के लिए प्रयोग नहीं करेगा जो फिलहाल लागू किसी भी कानून के किसी भी प्रावधान के विपरीत हो।

(4) केन्द्रीय सरकार समय-समय पर दूरसंचार साइबर सुरक्षा सुनिश्चित करने के लिए दूरसंचार आइडेन्टिफाइअरों या दूरसंचार नेटवर्क या दूरसंचार सेवाओं के दुरुपयोग की रोकथाम के लिए निर्देश और मानक जारी कर सकती है, जो उन सभी व्यक्तियों पर बाध्यकारी होगी जिन पर यह लागू है।

(5) प्रत्येक दूरसंचार कंपनी दूरसंचार साइबर सुरक्षा सुनिश्चित करने के लिए निम्नलिखित उपायों का अनुपालन सुनिश्चित करेगी:

(क) दूरसंचार साइबर सुरक्षा नीति अपनाएं, जिसमें निम्नलिखित पहलू शामिल होंगे:

(i) दूरसंचार साइबर सुरक्षा को बढ़ाने के लिए सुरक्षा उपाय, जोखिम प्रबंधन दृष्टिकोण, कार्य, प्रशिक्षण, सर्वोत्तम प्रणाली और प्रौद्योगिकी;

(ii) दूरसंचार नेटवर्क परीक्षण, जिसमें हार्डनिंग, भेद्यता मूल्यांकन और प्रवेश परीक्षण शामिल हैं;

(iii) जोखिम मूल्यांकन, पहचान और सुरक्षा घटनाओं की रोकथाम;

(iv) सुरक्षा घटनाओं से निपटने के लिए त्वरित कार्रवाई प्रणाली जिसमे ऐसी घटनाओं के प्रभाव को सीमित करने के लिए शमन उपाय शामिल है;

(v) ऐसी घटनाओं से सीख सुनिश्चित करने और दूरसंचार साइबर सुरक्षा को और सुदृढ़ करने के लिए सुरक्षा घटनाओं का फोरेंसिक विश्लेषण;

(ख) केंद्र सरकार को उप-अनुच्छेद (क) के तहत उल्लिखित ऐसी नीति को अपनाने पर पुष्टि करें, जैसा कि इस उद्देश्य के लिए निर्दिष्ट किया जा सकता है;

(ग) सुरक्षा घटनाओं के जोखिमों की पहचान करना और उन्हें कम करना और ऐसी घटनाओं पर लिए समय पर प्रतिक्रिया सुनिश्चित करना;

(घ) सुरक्षा घटनाओं के समाधान के लिए उचित कार्रवाई करना, और उनके प्रभाव को कम करना;

(ङ) केंद्र सरकार द्वारा जारी किए गए निर्देशों और मानकों का कार्यान्वयन सुनिश्चित करना;

(च) दूरसंचार साइबर सुरक्षा के प्रति खतरों के लचीलेपन का आकलन करने के लिए अपने स्वयं के तंत्र के माध्यम से और इस उद्देश्य के लिए केंद्र सरकार द्वारा निर्दिष्ट प्रमाणित एजेंसी के माध्यम से आवधिक दूरसंचार साइबर सुरक्षा ऑडिट आयोजित करना;

(छ) किसी भी सुरक्षा घटना की सूचना केंद्र सरकार या केंद्र सरकार द्वारा इस निमित्त प्राधिकृत कोई भी अधिकारी को यथा समय देना, और नियम 7 में निर्दिष्ट तरीके से ऐसी घटनाओं से निपटने के लिए किए गए उपाय;

(ज) निम्नलिखित का समाधान करने के लिए केन्द्र सरकार द्वारा विनिर्दिष्ट समयावधि के भीतर स्वयं अथवा अन्य दूरसंचार कंपनियों के सहयोग से सुरक्षा प्रचालन केन्द्र (एसओसी) जैसी सुविधाएं स्थापित करना

(i) दूरसंचार साइबर सुरक्षा घटनाओं, प्रयासों, घुसपैठ, उल्लंघनों और दूरसंचार सेवा या दूरसंचार नेटवर्क के दुरुपयोग की निगरानी करना;

(ii) अपनी दूरसंचार सेवा, या दूरसंचार नेटवर्क को प्रभावित करने वाले खतरे के कर्ताओं का विवरण बनाए रखना;

(iii) प्रचालन और रखरखाव के कमांड लॉग बनाए रखना;

(iv) एसओसी (फ़ायरवॉल, घुसपैठ का पता लगाने वाली प्रणाली (आईडीएस) या घुसपैठ रोकथाम प्रणाली (आईपीएस), या सुरक्षा सूचना और घटना प्रबंधन (एसआईईएम) या ऐसे अन्य समाधान) के लॉग बनाए रखना;

(v) दूरसंचार सेवाओं या दूरसंचार नेटवर्क में शामिल तत्वों के लॉग बनाए रखना या दूरसंचार सेवा या दूरसंचार नेटवर्क की सुरक्षा के लिए आवश्यक किसी अन्य तत्वों के लॉग बनाए रखना;

(vi) केंद्र सरकार द्वारा विनिर्दिष्ट अवधि के लिए यहां निर्दिष्ट सभी रिकॉर्ड, या लॉग का रख-रखाव करना और केंद्र सरकार द्वारा अधिकृत एजेंसी या व्यक्ति को उपलब्ध कराना;

(vii) सुरक्षा घटनाओं से संबंधित जांच के प्रयोजन के लिए केन्द्र सरकार या कानून प्रवर्तन एजेंसियों द्वारा अधिकृत एजेंसी या व्यक्ति को आवश्यक सहायता प्रदान करना।

5. दूरसंचार साइबर सुरक्षा को संरक्षित और सुनिश्चित करने के उपाय

(1) केन्द्रीय सरकार जैसा वह आवश्यक समझे डिजिटल और अन्य तंत्र स्थापित कर सकती है ताकि किसी व्यक्ति और अन्य हितधारकों को दूरसंचार साइबर सुरक्षा को खतरा पहुंचाने वाले किसी कार्य की पहचान करने और उसकी रिपोर्ट करने में सक्षम बनाया जा सके जिसमें नियम 4 के उप-नियम (3) के अंतर्गत सूचीबद्ध कार्य भी शामिल हैं।

(2) केन्द्रीय सरकार उप-नियम (1) के अधीन प्राप्त सूचना की प्रथम दृष्टया जांच के पश्चात् उस दूरसंचार आइडेन्टिफाइअर की पहचान करेगी जिसके उपयोग से दूरसंचार साइबर सुरक्षा को खतरा उत्पन्न होने का आरोप है और उस व्यक्ति की पहचान करेगी जिसे दूरसंचार कंपनी द्वारा ऐसा दूरसंचार आइडेन्टिफाइअर जारी किया गया है तथा ऐसे व्यक्ति को उसके ब्यौरे सहित नोटिस जारी करेगी।

(3) वह व्यक्ति जिसे उप-नियम (2) के अधीन नोटिस जारी किया जाता है ऐसे नोटिस की प्राप्ति के सात (7) कैलेंडर दिवस के भीतर केन्द्रीय सरकार को लिखित प्रत्युत्तर भेजेगा और यदि इस अवधि के भीतर कोई प्रत्युत्तर प्राप्त नहीं होता है तो केन्द्रीय सरकार उप-नियम (5) के अधीन आदेश जारी करने हेतु कार्रवाई करेगी।

(4) यदि उपनियम (2) के अधीन नोटिस के प्राप्तकर्ता से उसमें विनिर्दिष्ट समय के भीतर प्रत्युत्तर प्राप्त होता है तो केन्द्रीय सरकार ऐसे व्यक्ति को सुनवाई का उचित अवसर देने के पश्चात् उपनियम (5) के अधीन उस पर जैसा वह उचित समझे, आदेश पारित करेगी।

(5) केंद्र सरकार तथ्यों के अपने आकलन और उस व्यक्ति द्वारा किए गए प्रस्तुतीकरण यदि कोई हो, के आधार पर, जिसे उप-नियम (2) के तहत नोटिस जारी किया गया है, कारणों के साथ एक आदेश पारित करेगी, जिसमें दूरसंचार कंपनी को निदेश शामिल हो सकते हैं:

(क) दूरसंचार सेवाएं प्रदान करने के प्रयोजन के लिए संबंधित दूरसंचार आइडेन्टिफाइअर के उपयोग को अस्थायी रूप से निलंबित कर सकता है जिस तरीके से और जिस अवधि के लिए जैसा कि केंद्र सरकार द्वारा निर्दिष्ट किया जाए, या

(ख) दूरसंचार सेवाएं प्रदान करने के लिए संबंधित दूरसंचार आइडेन्टिफाइअर के उपयोग को समाप्त कर सकता है।

(6) उप-नियम (2) में उल्लिखित किसी बात के होते हुए भी यदि केन्द्रीय सरकार समझती है कि उप-नियम (5) के अधीन तत्काल कार्रवाई लोकहित में आवश्यक या समीचीन है तो किसी नोटिस की आवश्यकता नहीं होगी और ऐसी परिस्थितियों में वह इसके कारणों को दर्ज करते हुए एक आदेश पारित करेगी जिसमें दूरसंचार कंपनी को दूरसंचार सेवाएं प्रदान करने के प्रयोजनार्थ प्रासंगिक दूरसंचार पहचानकर्ता के उपयोग को अस्थायी रूप से निलंबित करने के लिए उचित निदेश दिए जाएंगे।

(7) उप-नियम (5) या उप-नियम (6) के तहत आदेश की प्रति ऐसे आदेश से प्रभावित व्यक्ति को प्रदान की जाएगी और ऐसा व्यक्ति, इसके जारी होने की तारीख से तीस (30) कैलेंडर दिनों की अवधि के भीतर, लिखित रूप में केंद्र सरकार को कारण अभिवेदन कर सकता है कि ऐसी कार्रवाई क्यों नहीं की जानी चाहिए। केंद्र सरकार ऐसे व्यक्ति को सुनवाई का उचित अवसर देने के बाद, लिखित रूप में दर्ज किए जाने वाले कारणों से उप-नियम (5) या उप-नियम (6) के तहत पारित आदेश को बरकरार रखने या संशोधित करने या रद्द करने का आदेश पारित करेगी। उप-नियम (6) के तहत आदेश के किसी भी संशोधन में दूरसंचार कंपनी को उप-नियम (5) के खंड (बी) के तहत निर्दिष्ट दूरसंचार सेवाएं प्रदान करने के प्रयोजन के लिए प्रासंगिक दूरसंचार आइडेन्टिफाइअर के उपयोग को समाप्त करने का निर्देश देने वाला आदेश भी शामिल हो सकता है।

(8) उप-नियम (5), उप-नियम (6) और उप-नियम (7) के अधीन दूरसंचार सेवा के निलंबन या समाप्ति का कोई आदेश उस व्यक्ति से संबद्ध अन्य दूरसंचार उपकरण या दूरसंचार आइडेन्टिफाइअर पर भी लागू किया जा सकेगा जिसका दूरसंचार आइडेन्टिफाइअर उप-नियम (2) के अधीन चिन्हित किया गया है या उप-नियम (2) के अधीन चिन्हित किए गए व्यक्ति को जारी किए गए अन्य दूरसंचार आइडेन्टिफाइअर पर भी लागू किया जा सकेगा।

(9) केंद्र सरकार ऐसे व्यक्तियों और दूरसंचार आइडेन्टिफाइअरों का रिपोजिटरी रख सकती है जिन पर उप-नियम (5) या उप-नियम (6) या उप-नियम (7) या उप-नियम (8) के तहत आदेशों के अनुसरण में कार्रवाई की गई है और दूरसंचार कंपनियों को ऐसे व्यक्तियों के लिए दूरसंचार सेवाओं तक पहुंच को प्रतिबंधित या सीमित करने का निर्देश दे सकती है जिसकी अवधि इस आदेश की तारीख से तीन (3) वर्ष से अधिक न हो।

(10) केन्द्रीय सरकार, यदि वह आवश्यक समझे, उप-नियम (5) या उप-नियम (6) या उप-नियम (7) या उप-नियम (8) के तहत आदेशों के अनुसरण में कार्रवाई की गई दूरसंचार आइडेन्टिफाइअरों की सूची को दूरसंचार आइडेन्टिफाइअरों का उपयोग करके सेवाएं प्रदान करने वाले अन्य व्यक्तियों के साथ साझा कर सकती है और ऐसे व्यक्तियों को भी निदेश दे सकती है कि वे अपने ग्राहकों की पहचान के लिए या उनकी

सेवाओं के वितरण के लिए ऐसे दूरसंचार आइडेन्टिफाइअरों के उपयोग को प्रतिबंधित या सीमित करें जैसा कि निर्दिष्ट किया जा सकता है।

(11) कोई भी दूरसंचार आइडेन्टिफाइअर जो इस नियम के अनुसार दूरसंचार सेवा के निलंबन या समाप्ति का विषय है ऐसे आदेश जारी होने की तारीख से एक (1) वर्ष की अवधि के लिए किसी अन्य व्यक्ति को पुनः आवंटित नहीं किया जाएगा जिसे विशिष्ट मामलों में तीन (3) वर्ष तक बढ़ाया जा सकता है।

6. मुख्य दूरसंचार सुरक्षा अधिकारी

(1) प्रत्येक दूरसंचार कंपनी एक मुख्य दूरसंचार सुरक्षा अधिकारी नियुक्त करेगा जिसका विवरण इस प्रयोजन के लिए निर्दिष्ट प्रपत्र में केन्द्रीय सरकार को लिखित रूप में उपलब्ध कराया जाएगा। ऐसे अधिकारी के किसी प्रतिस्थापन या परिवर्तन की सूचना तत्काल केन्द्रीय सरकार को ऐसे निर्दिष्ट प्रपत्र में दी जाएगी।

(2) मुख्य दूरसंचार सुरक्षा अधिकारी भारत का नागरिक और निवासी होगा तथा दूरसंचार कंपनी के निदेशक मंडल या समान शासी निकाय के प्रति उत्तरदायी होगा।

(3) मुख्य दूरसंचार सुरक्षा अधिकारी इन नियमों के कार्यान्वयन के लिए केन्द्रीय सरकार के साथ समन्वय करने के लिए उत्तरदायी होगा जिसमें निम्नलिखित का अनुपालन भी शामिल है इन नियमों के अंतर्गत किसी भी रिपोर्टिंग से संबंधित आवश्यकता जिसमें नियम 7 के अंतर्गत सुरक्षा घटनाएं शामिल हैं।

7. सुरक्षा घटनाओं की रिपोर्टिंग

(1) किसी दूरसंचार कंपनी को प्रभावित करने वाली किसी सुरक्षा संबंधी घटना के घटित होने पर ऐसी इकाई ऐसी घटना के छह (6) घंटे के भीतर इस प्रयोजन के लिए निर्दिष्ट रूप और तरीके से केन्द्रीय सरकार को इसकी रिपोर्ट करेगी जिसमें लागू होने वाली निम्नलिखित सूचना प्रस्तुत करना शामिल है:

(क) सुरक्षा संबंधी घटना से प्रभावित प्रयोक्ताओं की संख्या;

(ख) सुरक्षा संबंधी घटना की अवधि;

(ग) सुरक्षा संबंधी घटना से प्रभावित भौगोलिक क्षेत्र;

(घ) दूरसंचार नेटवर्क या दूरसंचार सेवा के कामकाज पर किस हद तक प्रभाव पड़ा है;

(ङ) आर्थिक और सामाजिक गतिविधियों पर प्रभाव की सीमा; और

(च) किए गए या किए जाने हेतु प्रस्तावित सुधारात्मक उपाय

(2) केन्द्रीय सरकार जहां यह निर्धारित करती है कि सुरक्षा घटना का खुलासा सार्वजनिक हित में है ऐसी सुरक्षा घटना के बारे में जनता को सूचित कर सकती है या प्रभावित दूरसंचार कंपनी को ऐसा करने के लिए आग्रह कर सकती है।

(3) केन्द्रीय सरकार प्रभावित दूरसंचार कंपनी से यह निम्नलिखित उपलब्ध कराने की मांग कर सकती है:

(क) दूरसंचार साइबर सुरक्षा उपायों सहित ऐसे दूरसंचार नेटवर्क और दूरसंचार सेवाओं की सुरक्षा का आकलन करने के लिए आवश्यक सूचना;

(ख) इस प्रयोजन के लिए निर्दिष्ट तरीके से ऐसी दूरसंचार कंपनी की लागत पर, केंद्र सरकार द्वारा निर्दिष्ट प्रमाणित एजेंसी द्वारा सुरक्षा जांच करना।

(4) केन्द्रीय सरकार किसी सुरक्षा संबंधी घटना के समाधान के लिए या किसी महत्वपूर्ण खतरे की पहचान होने पर उसे घटित होने से रोकने के लिए आवश्यक उपायों सहित निदेश जारी कर सकती है तथा प्रभावित दूरसंचार इकाई के लिए ऐसे निदेशों के कार्यान्वयन के लिए समय-सीमा निर्दिष्ट कर सकती है।

8. दूरसंचार आइडेन्टिफाइअर और दूरसंचार उपकरण से संबंधित दायित्व

(1) उपकरण का विनिर्माता जिसके पास इंटरनेशनल मोबाईल इक्विप्मन्ट आइडेंटिटी (आईएमईआई) संख्या है, भारत में निर्मित ऐसे उपकरण का आईएमईआई नंबर ऐसे उपकरण की पहली बिक्री से पहले ऐसे प्रयोजन के लिए निर्दिष्ट प्रपत्र में केन्द्रीय सरकार से पंजीकृत कराएगा।

(2) दूरसंचार उपकरण का आयातक जिसके पास आईएमईआई संख्या है, भारत में बिक्री, परीक्षण, अनुसंधान या किसी अन्य प्रयोजन के लिए आयातित ऐसे उपकरण का आईएमईआई नंबर ऐसे उपकरण के भारत में आयात से पहले ऐसे प्रयोजन के लिए निर्दिष्ट प्रपत्र में केन्द्रीय सरकार के पास पंजीकृत कराएगा।

(3) कोई भी व्यक्ति ऐसा नहीं करेगा:

(क) जानबूझकर विशिष्ट दूरसंचार उपकरण पहचान संख्या को हटाएगा, मिटाएगा, बदलेगा या परिवर्तित नहीं करेगा; या

(ख) यह जानते हुए कि इसे ऊपर निर्दिष्ट अनुसार कॉन्फ़िगर किया गया है, जानबूझकर दूरसंचार आइडेन्टिफाइअर या दूरसंचार उपकरण से संबंधित हार्डवेयर या सॉफ्टवेयर का उपयोग, उत्पादन, यातायात, नियंत्रण या अभिरक्षा या दखल अपने पास नहीं रखेगा।

(4) केंद्र सरकार टेम्पर किए गए दूरसंचार उपकरण या आईएमईआई नंबर के संबंध में आवश्यकतानुसार सहायता प्रदान करने के लिए आईएमईआई नंबर वाले दूरसंचार उपकरणों के निर्माताओं को निदेश जारी कर सकती है।

(5) केन्द्र सरकार दूरसंचार नेटवर्कों में या दूरसंचार सेवाएं प्रदान करते समय टेम्पर किए गए आईएमईआई नंबर वाले दूरसंचार उपकरणों के उपयोग को रोकने के लिए दूरसंचार कंपनियों को निदेश जारी कर सकती है।

9. इन नियमों का डिजिटल कार्यान्वयन

केंद्र सरकार इन नियमों के डिजिटल कार्यान्वयन के लिए उपयुक्त साधन निर्दिष्ट कर सकती है, जिनमें निम्नलिखित शामिल हैं:

(क) ट्रैफिक डेटा का संग्रह, साझाकरण और विश्लेषण,

(ख) नियम 5 के तहत नोटिस जारी करना और प्रत्युत्तर प्रस्तुत करना।

(ग) ऐसे व्यक्तियों और दूरसंचार आइडेंटिफायर्स की रेपोजिटरी संग्रह का अनुरक्षण करना जिनके विरुद्ध नियम 5 के तहत कोई कार्रवाई की गई है।

(घ) दूरसंचार आइडेंटिफायर्स या दूरसंचार नेटवर्क अथवा दूरसंचार सेवाओं के दुरुपयोग की रोकथाम के लिए निदेश, मानक जारी करना।

(ङ) दूरसंचार कंपनी द्वारा केंद्र सरकार को दूरसंचार साइबर सुरक्षा नीति प्रस्तुत करना।

(च) दूरसंचार कंपनी द्वारा सुरक्षा घटनाओं की रिपोर्टिंग जिसमें कोई अतिरिक्त सूचना प्रदान करना शामिल है।

(छ) भारत में विनिर्मित या आयातित उपकरण के आईएमईआई नंबर का पंजीकरण तथा

(ज) टेम्पर किए गए आईएमईआई नंबर वाले दूरसंचार उपकरणों के उपयोग को रोकना।

[फा. सं 24-05/2024-यूबीबी]

देवेंद्र कुमार राय, संयुक्त सचिव

MINISTRY OF COMMUNICATIONS

(Department of Telecommunications)

NOTIFICATION

New Delhi, the 28th August, 2024

G.S.R. 520(E).—The following draft rules, which the Central Government proposes to make in exercise of the powers conferred under sub-section (1) of section 22, read with clause (v) to sub-section (2) of section 56 of the Telecommunications Act, 2023 (44 of 2023), are hereby published for the information of all persons likely to be affected thereby and notice is hereby given that the said draft rules shall be taken into consideration after the expiry of

a period of thirty days from the date on which copies of this notification as published in the Official Gazette, are made available to the public;

Objections or suggestions, if any, may be addressed to the Joint Secretary (Telecom), Department of Telecommunications, Ministry of Communications, Government of India, Sanchar Bhawan, 20, Ashoka Road, New Delhi- 110001;

The objections or suggestions which may be received from any person with respect to the said draft rules before the expiry of the aforesaid period shall be taken into consideration by the Central Government.

1. Short title, commencement, and savings

These rules may be called the Telecommunications (Telecom Cyber Security) Rules, 2024.

(1) They shall come into force on the date of their publication in the Official Gazette.

(2) These rules shall be in supersession of the Prevention of Tampering of the Mobile Device Equipment Identification Number Rules, 2017 and the Mobile Device Equipment Identification Number (Amendment) Rules, 2022 under the Indian Telegraph Act, 1885 (13 of 1885), but shall not override the terms and conditions of actions taken under those rules, including registrations undertaken pursuant to those rules.

2. Definitions

(1) In these rules, unless the context otherwise requires:

(a) "**Act**" means the Telecommunications Act, 2023 (44 of 2023);

(b) "**Chief Telecommunication Security Officer**" means the designated employee of a telecommunication entity, appointed under rule 6 of these rules;

(c) "**cyber security of telecommunication networks and telecommunication services**" or "**telecom cyber security"** refers to tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, assurance and technologies that can be used to safeguard telecommunication networks and telecommunication services, as well as assets of persons, including connected telecommunication equipment, telecommunication services, personnel, infrastructure, applications, and the totality of transmitted and/or stored information, against relevant security risks in the cyber environment;

(d) "**rules**" means the Telecommunications (Telecom Cyber Security) Rules, 2024;

(e) "**security incident**" means an event having actual or potential adverse effect on telecom cyber security;

(f) "**telecommunication entity"** means any person providing telecommunication services, or establishing, operating, maintaining, or expanding telecommunication network, including an authorised entity holding an authorisation under sub-section (1) of section 3 of the Act, or a person exempted from the requirement of authorisation under sub-section (3) of section 3 of the Act

(g) "**telecommunication equipment identification number**" means a telecommunication identifier bearing one or more of the following characteristics:

(i) international mobile equipment identity (IMEI) number; or

(ii) electronic serial number (ESN); or

(iii) any other number or signal that identifies a unique telecommunication equipment.

(h) "**traffic data**" means any data generated, transmitted, received or stored in telecommunication networks, including data relating to the type, routing, duration or time of a telecommunication.

(2) Words and expressions used in these rules and not defined herein but defined in the Act, shall have the meaning assigned to them in the Act.

3. Collection, sharing and analysis of data

(1) The Central Government, or any agency authorised in this behalf by the Central Government, may, for the purposes of protecting and ensuring telecom cyber security:

(a) seek from a telecommunication entity, traffic data and any other data in the form and manner as notified by the Central Government for this purpose; or

(b) direct a telecommunication entity to establish necessary infrastructure and equipment for collection and provision of such data from designated points to enable its processing and storage.

(2) The data collected under sub-rule (1) may be analysed for taking measures to enhance telecom cyber security, and may, if so determined by the Central Government as necessary for protecting and ensuring telecom cyber security, be:

(a) disseminated to any agency of the Central Government engaged in law enforcement and security related activities; and

(b) shared with telecommunication entities or users.

(3) The Central Government and any agency authorised by the Central Government to collect data under these rules, as well as persons with whom such data is shared under sub-rule (2), shall put in place adequate safeguards, including any specific safeguards as may be notified by the Central Government for this purpose, to prevent any unauthorised access to such data.

(4) The data collected under these rules shall not be used or disclosed for any other purpose, except for ensuring telecom cyber security.

4. Obligations relating to telecom cyber security

(1) No person shall endanger telecom cyber security.

(2) No message shall be sent using telecommunication network or telecommunication service which adversely affects telecom cyber security.

(3) Without prejudice to the generality of sub-rule (1) and sub-rule (2), no person shall use telecommunication equipment or telecommunication identifier or telecommunication network, or telecommunication services, including through:

(a) fraud, cheating or personation;

(b) transmitting any message which is fraudulent;

(c) committing or intending to commit any security incident; or

(d) engaging in any other use which is contrary to any provision of any law for the time being in force.

(4) The Central Government may, from time to time, issue directions and standards for the prevention of misuse of telecommunication identifiers or telecommunication network or telecommunication services for ensuring telecom cyber security, which shall be binding on all persons on which it is applicable.

(5) Each telecommunication entity shall ensure compliance with the following measures to ensure telecom cyber security:

(a) adopt a telecom cyber security policy, which shall include:

(i) security safeguards, risk management approaches, actions, training, best practices, and technologies, to enhance telecom cyber security;

(ii) telecommunication network testing, including hardening, vulnerability assessment and penetration testing;

(iii) risk assessment, identification, and prevention of security incidents;

(iv) rapid action system to deal with security incidents, including mitigation measures to limit the impact of such incidents;

(v) forensic analysis of security incidents, to ensure learnings from such incidents and further strengthening telecom cyber security;

(b) confirm to the Central Government on the adoption of such policy as outlined under sub-paragraph (a), in the manner as may be specified for this purpose;

(c) identify and reduce the risks of security incidents and ensure timely responses to such incidents;

(d) take appropriate action for addressing security incidents, and mitigate their impact;

(e) ensure implementation of directions and standards as issued by the Central Government;

(f) conduct periodic telecom cyber security audits through its own mechanisms to assess resilience to threats to telecom cyber security, and through the certified agency as specified by the Central Government for this purpose;

(g) promptly report any security incident to the Central Government, or any officer authorised on this behalf by the Central Government, and measures taken to address such incidents in the manner specified in rule 7;

(h) establish facilities such as Security Operations Centre (SOC), by itself or in collaboration with other telecommunication entities, within the time period as specified by the Central Government, to address the following:

(i) monitor telecom cyber security incidents, attempts, intrusions, breaches and misuse of telecommunication service or telecommunication network;

(ii) maintain details of threat actors impacting its telecommunication service, or telecommunication network;

(iii) maintain command logs of operation and maintenance;

(iv) maintain logs of SOC (firewall, Intrusion Detection System (IDS) or Intrusion Prevention System (IPS), or Security Information and Event Management (SIEM) or other such solution);

(v) maintain logs of elements involved in telecommunication services, or telecommunication network or any other element required for security of telecommunications service or telecommunications network;

(vi) maintain all records or logs specified herein, for a period as specified by the Central Government and make available to the agency or person authorized by the Central Government;

(vii) provide necessary support to the agency or person authorized by the Central Government or the law enforcement agencies for the purpose of investigation related to security incidents.

5. Measures to protect and ensure telecom cyber security

(1) The Central Government may put in place digital and other mechanisms as it may consider necessary to identify, or for enabling any person and other stakeholders to identify and report any act that endangers telecom cyber security, including through actions listed under sub-rule (3) of rule 4.

(2) The Central Government shall, after a prima facie examination of the information received under sub-rule (1), identify the telecommunication identifier, the use of which is alleged to have endangered telecom cyber security and the person to whom such telecommunication identifier has been issued by the telecommunication entity, and issue a notice to such person, with details thereof.

(3) The person to whom notice is issued under sub-rule (2), shall send a written response to the Central Government, within seven (7) calendar days of receipt of such notice, and if no response is received within such period, the Central Government shall proceed to issue an order under sub-rule (5).

(4) If a response is received from the recipient of the notice under sub-rule (2) within the time specified therein, the Central Government shall, after giving such person a reasonable opportunity of being heard, make an order thereon as it thinks fit under sub-rule (5).

(5) The Central Government shall, based on its assessment of facts and submissions, if any, made by the person to whom notice is issued under sub-rule (2), pass an order, with reasons, which may include directions to the telecommunication entity to:

(a) temporarily suspend use of the relevant telecommunication identifier for the purpose of providing telecommunication services, in the manner and for a duration as may be specified by the Central Government, or

(b) terminate the use of the relevant telecommunication identifier for providing telecommunication services.

(6) Notwithstanding anything stated in sub-rule (2), no notice shall be required if the Central Government considers that immediate action under sub-rule (5) is necessary or expedient in the public interest, and in such circumstances, it shall pass an order recording the reasons therefor, with appropriate directions to the telecommunication entity to temporarily suspend use of the relevant telecommunication identifier for the purpose of providing telecommunication services.

(7) The copy of the order under sub-rule (5) or sub-rule (6) shall be provided to the person affected by such order, and such person, may, within a period of thirty (30) calendar days from the date of issuance thereof, represent to the Central Government in writing, with reasons why such action should not be

taken. The Central Government shall, after giving such person a reasonable opportunity of being heard, pass an order, either upholding or modifying or revoking the order passed under sub-rule (5) or sub-rule (6), for reasons to be recorded in writing. Any modification of the order under sub-rule (6) may also include an order directing the telecommunication entity to terminate the use of the relevant telecommunication identifier for the purpose of providing telecommunication services as specified under clause (b) of sub-rule (5).

(8) Any order of suspension or termination of telecommunication service under sub-rule (5), sub-rule (6) and sub rule (7) may also be extended to the other telecommunication equipment or telecommunication identifier linked to the person whose telecommunication identifier has been identified under sub-rule (2) or other telecommunication identifier issued to the person identified under sub-rule (2).

(9) The Central Government may maintain a repository of persons and telecommunication identifiers which have been acted upon pursuant to the orders under sub-rule (5) or sub-rule (6) or sub-rule (7) or sub-rule (8), and may direct telecommunication entities, to prohibit or limit the access to telecommunication services to such persons for a period not exceeding three (3) years from the date of such order.

(10) The Central Government may, if it considers necessary, share the list of telecommunication identifiers that have been acted upon pursuant to orders under sub-rule (5) or sub-rule (6) or sub-rule (7) or sub-rule (8), with other persons providing services using the telecommunication identifiers and direct such persons also to prohibit or circumscribe the use of such telecommunication identifiers for identification of their customers or for delivery of their services, in the manner as may be specified.

(11) Any telecommunication identifier which is the subject of suspension or termination of the telecommunication service pursuant this rule, shall not be reallocated to any other person for a period of one (1) year from the date of issuance of such order which may be extended upto three (3) years in specific cases.

6. Chief Telecommunication Security Officer

(1) Each telecommunication entity shall appoint a Chief Telecommunication Security Officer, whose details shall be provided in writing to the Central Government in the form as may be specified for this purpose. Any replacement or change of such officer shall be promptly notified to the Central Government, in such form as may be specified.

(2) The Chief Telecommunication Security Officer shall be a citizen and resident of India, and responsible to the Board of Directors or similar governing body of the telecommunication entity.

(3) The Chief Telecommunication Security Officer shall be responsible for coordinating with the Central Government for the implementation of these rules, including compliance with any reporting requirements under these rules, including of security incidents under rule 7.

7. Reporting of security incidents

(1) On the occurrence of any security incident affecting a telecommunication entity, such entity shall report the same to the Central Government within six (6) hours of such occurrence in the form and manner specified for this purpose, including the furnishing of the following information as applicable:

(a) the number of users affected by the security incident;

(b) the duration of the security incident;

(c) the geographical area affected by the security incident;

(d) the extent to which the functioning of the telecommunication network or telecommunication service is affected;

(e) the extent of impact on economic and societal activities; and

(f) the remedial measures taken or proposed to be taken.

(2) The Central Government may, where it determines that disclosure of the security incident is in the public interest, inform the public of such security incident, or require the affected telecommunication entity to do so.

(3) The Central Government may require the affected telecommunication entity to:

(a) provide information needed to assess the security of such telecommunication network and telecommunication services, including telecom cyber security measures;

(b) carryout security audit by a certified agency as specified by the Central Government at the cost of such telecommunication entity, in the manner specified for this purpose.

(4) The Central Government may issue directions including for the measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and may specify the time-limits for implementation of such directions to the affected telecommunication entity.

8. Obligations relating to telecommunication identifier and telecommunication equipment

(1) A manufacturer of equipment that has international mobile equipment identity (IMEI) number, shall register such IMEI number of such equipment manufactured in India with the Central Government, prior to the first sale of such equipment, in the form as may be specified for such purpose.

(2) An importer of equipment that has an IMEI number, shall register such IMEI number of such equipment imported in India for sale, testing, research or any other purpose with the Central Government, prior to the import of such equipment into India, in the form as may be specified for such purpose.

(3) No person shall:

(a) intentionally remove, obliterate, change, or alter unique telecommunication equipment identification number; or

(b) intentionally use, produce, traffic in, have control or custody of, or possess hardware or software related to the telecommunication identifier or telecommunication equipment, knowing it has been configured as specified above.

(4) The Central Government may issue directions to manufacturers of telecommunication equipment bearing IMEI number to provide assistance as required in relation to tampered telecommunication equipment or IMEI number.

(5) The Central Government may issue directions to telecommunication entities to block the use of telecommunication equipment with tampered IMEI number in telecommunication networks or providing telecommunication services.

9. Digital implementation of these rules

The Central Government may specify appropriate means for the digital implementation of these rules, including for:

(a) collection, sharing and analysis of traffic data;

(b) issuance of notice and submission of response under rule 5;

(c) maintaining repository of persons and telecommunication identifiers against which any action has been taken under rule 5;

(d) issuance of directions and standards, for the prevention of misuse of telecommunication identifiers or telecommunication network or telecommunication services;

(e) submission of telecom cyber security policy by the telecommunication entity to the Central Government;

(f) reporting of security incidents by the telecommunication entity including any additional information to be provided;

(g) registration of IMEI number of equipment manufactured or imported in India; and

(h) blocking the use of telecommunication equipment with tampered IMEI numbers.

[F. No. 24-05/2024-UBB]

DEVENDRA KUMAR RAI, Jt. Secy.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.