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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-18032021-225996
CG-DL-E-18032021-225996

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 1156] नई दिल्ली, बृहस्पतिवार, मार्च 18, 2021/फाल्गुन 27, 1942
No. 1156] NEW DELHI, THURSDAY, MARCH 18, 2021/PHALGUNA 27, 1942

इलेक्ट्रॉनिक और सूचना प्रौद्योगिकी मंत्रालय

आदेश

नई दिल्ली, 18 मार्च, 2021

का.आ. 1248(अ).—भारतीय मानक ब्यूरो अधिनियम, 2016 (2016 का 11) की धारा 25 की उप-धारा (3) के साथ पठित धारा 16 की उप-धारा (1) और (2) द्वारा प्रदत्त शक्तियों के अनुसरण में केंद्र सरकार का भारतीय मानक ब्यूरो से परामर्श करने के पश्चात यह मत है कि जनहित में ऐसा करना आवश्यक या समीचीन है, एतद्वारा निम्नलिखित आदेश बनाती है, यानि:-

1. संक्षिप्त नाम और प्रारंभ:- (1) यह आदेश "इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (आवश्यक पंजीकरण की आवश्यकता) आदेश, 2021" कहलाएगा।

2. मानक चिह्न का अनिवार्य प्रयोग:- निम्नलिखित अनुसूची के कॉलम (2) में विनिर्दिष्ट माल या सामान, कथित अनुसूची के कॉलम (3) में दिए गए तदनुरूपी भारतीय मानक के अनुरूप होंगे और भारतीय मानक (अनुरूपता मूल्यांकन) ब्यूरो विनियमावली, 2018 की अनुसूची-II की योजना-II के अनुसार भारतीय मानक ब्यूरो से एक लाइसेंस के तहत 'मानक' चिह्न रखेंगे बशर्ते कि इस आदेश में निर्यात के लिए निर्धारित कथित अनुसूची के कॉलम (2) में यथा-विनिर्दिष्ट ऐसे माल या वस्तुओं के निर्यात के संबंध में लागू नहीं होगा जो विदेशी खरीदकर्ताओं द्वारा आवश्यक विनिर्देशों के अनुरूप होंगे, जिसके लिए केंद्र सरकार ने विशिष्ठ रूप से लिखित रूप में रिकॉर्ड किए जाने के कारणों के आधार पर छूट पत्र जारी किया है।

3. समय सीमा: यह आदेश आधिकारिक राजपत्र में प्रकाशन के छह माह समाप्त होने के बाद लागू होगा।

4. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (अनिवार्य पंजीकरण की आवश्यकता) आदेश, 2012 के साथ समवर्ती संचालन : आदेश में ऐसे माल या वस्तुओं में कुछ भी लागू नहीं होगा जिनके पास ''इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (आवश्यक पंजीकरण की आवश्यकता) आदेश, 2012'' के प्रावधानों के अनुसार वैध पंजीकरण संख्या मौजूद है। तथापि, ''इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (आवश्यक पंजीकरण की आवश्यकता) आदेश, 2021'' के प्रावधानों के अंतर्गत पंजीकरण का नवीकरण किया जाएगा।

5. प्रमाणन और प्रवर्तन : कथित अनुसूची के कॉलम (2) में विनिर्दिष्ट माल या वस्तुओं के संबंध में भारतीय मानक ब्यूरो इस आदेश के अंतर्गत मानक चिह्न के साथ समरूपता को प्रमाणित और प्रवृत्त करने के लिए प्राधिकृत होगा और साथ ही आवश्यक होने पर भारत सरकार के अवर सचिव से ऊपर के पद वाले या जिला उद्योग केंद्र, इस आदेश के प्रवर्तन में ब्यूरो को सहायता देंगे इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय के परामर्श से भारतीय मानक ब्यूरो द्वारा अधिसूचित एजेंसियों द्वारा निगरानी की जाएगी।

अनुसूची

क्रम संख्या	माल या लेख	भारतीय मानक	भारतीय मानक का शीर्षक
(1)	(2)	(3)	(4)
1.	इलेक्ट्रॉनिक गेम्स (वीडियो)	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण – सुरक्षा आवश्यकताएं
2.	लैपटॉप / नोटबुक / टैबलेट	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
3.	प्लाज्मा / एलसीडी / एलईडी / 32 इंच और इससे अधिक आकार के स्क्रीन की टीवी	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं
4.	200वाट और उससे अधिक के इनपुट पावर के एम्पलीफायरों निर्मित ऑप्टिकल डिस्क प्लेयर	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण - सुरक्षा आवश्यकताएँ
5.	माइक्रोवेव ओवेन	आईएस 302 : भाग -2: खंड 25: 2014	घरेलू और समान विद्युत उपकरणों की सुरक्षा: खंड 2 विशेष आवश्यकताएं: खंड 25 माइक्रोवेव ओवन
6.	विजुअल डिस्प्ले यूनिट, 32 इंच और इससे अधिक स्क्रीन आकार के वीडियो मॉनिटर	आईएस 13252 : भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
7.	प्रिंटर / मल्टी-फंक्शन डिवाइस (एमएफडी) / प्लॉटर्स	आईएस 13252: भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
8.	स्कैनर्स	आईएस 13252: भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
9.	वायरलेस कीबोर्ड	आईएस 13252 : भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
10.	टेलिफोन आंसरिंग मशीन	आईएस 13252 : भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
11.	इनपुट पावर 2000वाट और इससे अधिक इनपुट पावर वाले एम्पलीफायर	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण - सुरक्षा आवश्यकताएँ
12.	200वाट और इससे अधिक के इलेक्ट्रॉनिक इससे अधिक जिकल सिस्टम	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण - सुरक्षा आवश्यकताएँ
13.	मेन्स पॉवर्स के साथ इलेक्ट्रॉनिक क्लॉक्स	आईएस 302 भाग -2: खंड- 26: 2014	घरेलू और समान विद्युत उपकरणों की सुरक्षा: खंड 2 विशेष आवश्यकताएं: खंड 26 क्लॉक्स
14.	सेट टॉप बॉक्स	आईएस 13252 : भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण-सुरक्षा-सामान्य आवश्यकताएँ
15.	स्वचालित डाटा प्रोसेसिंग मशीन	आईएस 13252 : भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण-सुरक्षा-सामान्य आवश्यकताएँ
16.	आईटी उपकरणों के लिए पॉवर एडेप्टर	आईएस 13252 : भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण-सुरक्षा-सामान्य आवश्यकताएँ

17.	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण के लिए पावर एडेप्टर	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण - सुरक्षा आवश्यकताएँ
18.	यूपीएस / इनवर्टर रेटिंग 5 केवीए	आईएस 16242 :भाग 1: 2014	यूपीएस के लिए निर्बाध विद्युत प्रणाली (यूपीएस) खंड 1 सामान्य और सुरक्षा आवश्यकताएँ
19.	एलईडी मॉड्यूल के लिए डीसी या एसी आपूर्ति इलेक्ट्रॉनिक नियंत्रण गियर	आईएस 15885 :भाग 2 : खंड 13 : 2012	लैंप कंट्रोल गियर की सुरक्षा पार्ट 2 की विशेष रूप से आवश्यक खंड 13 डीसी या एसी। एलईडी मॉड्यूल के लिए सप्लीमेंट इलेक्ट्रॉनिक कंट्रोल गियर
20.	पोर्टेबल एप्लीकेशन में उपयोग के लिए अल्कलाइन या अन्य नॉन-एसिड इलेक्ट्रोलाइट्स वाले सील्ड सेकेंडरी सेल/ बैटरियां	आईएस 16046 : भाग 1 : 2018	अल्कलाइन या अन्य नॉन-एसिड इलेक्ट्रोलाइट्स युक्त माध्यमिक कोशिकाएं और बैटरियां - पोर्टेबल सील माध्यमिक कोशिकाओं के लिए सुरक्षा आवश्यकताएं और पोर्टेबल अनुप्रयोगों में उपयोग के लिए उनके द्वारा निर्मित बैटरियों के लिए भाग 1 निकल सिस्टम
		आईएस 16046 : भाग 2 : 2018	अल्कलाइन या अन्य नॉन-एसिड इलेक्ट्रोलाइट्स युक्त माध्यमिक कोशिकाएं और बैटरियां - पोर्टेबल सील माध्यमिक कोशिकाओं के लिए सुरक्षा आवश्यकताएं और पोर्टेबल अनुप्रयोगों में उपयोग के लिए उनके द्वारा निर्मित बैटरियों के लिए पार्ट 2 लिथियम सिस्टम
21.	जनरल लाइटिंग सेवाओं के लिए सेल्फ –बैलेस्टेड लईडी लैंप	आईएस 16102 :भाग 1: 2012	जनरल लाइटिंग सर्विसेज पार्ट 1 के लिए सुरक्षा आवश्यकता के लिए सेल्फ बैलेस्टेड लईडी लैंप
22.	फिक्स्ड जनरल पर्पज एलईडी ल्यूमिनरीज	आईएस 10322 : भाग 5 खंड 1: 2012	ल्यूमिनरीज खंड 5 विशेष आवश्यकताएं खंड 1 फिक्स्ड सामान्य उद्देश्य ल्यूमिनरीज
23.	मोबाइल फोन	आईएस 13252: भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा- सामान्य आवश्यकताएँ
24.	कैश रजिस्टर	आईएस 13252: भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा- सामान्य आवश्यकताएँ
25.	प्वाइंट ऑफ सेल टर्मिनल	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा- सामान्य आवश्यकताएँ
26.	कॉपी मशीनें / डुप्लिकेटर्स	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा- सामान्य आवश्यकताएँ
27.	स्मार्ट कार्ड पाठक	आईएस 13252 : भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा- सामान्य आवश्यकताएँ
28.	मेल प्रोसेसिंग मशीन / डाक मशीनें / फ्रैकिंग मशीन	आईएस 13252:भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा- सामान्य आवश्यकताएँ
29.	पासपोर्ट रीडर	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा- सामान्य आवश्यकताएँ
30.	पोर्टेबल एप्लीकेशन में उपयोग के लिए पावर बैंक	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी - उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
31.	मोबाइल फोन के लिए भारतीय भाषा समर्थन	आईएस 16333 :भाग 3: 2017	मोबाइल फोन हैंडसेट के लिए मोबाइल फोन हैंडसेट खंड 3 भारतीय भाषा समर्थन - विशिष्ट आवश्यकताएं
32.	रिसेस्ड एलईडी लाइट्स	आईएस 10322 :भाग 5: खंड 2): 2012	ल्यूमिनेयर भाग 5: विशेष आवश्यकताएं खंड 2 रिसेस्ड ल्यूमिनरीज

33.	रोड और स्ट्रीट लाइटिंग के लिए एलईडी ल्यूमिनेयर	आईएस 10322 :भाग 5 : खंड 3): 2012	ल्यूमिनेयर खंड 5: रोड और स्ट्रीट लाइटिंग के लिए विशेष आवश्यकताएं खंड 3 ल्यूमिनेरी
34.	एलईडी फ्लड लाइट्स	आईएस 10322 :भाग 5 : खंड 5): 2013	ल्यूमिनरीज खंड 5: विशेष आवश्यकताओं खंड 5 फ्लड लाईट
35.	एलईडी हाथ लैंप	आईएस 10322 : भाग 5 : खंड 6: 2013	ल्यूमिनरीज खंड 5: विशेष आवश्यकताएं खंड 6 हैण्ड लैंप
36.	एलईडी लाइटिंग चेन	आईएस 10322 :भाग 5: खंड 7 : 2017	ल्यूमिनरीज भाग 5: विशेष आवश्यकताएं धारा 7 प्रकाश चेन
37.	इमरजेंसी लाइटिंग के लिए एलईडी ल्यूमिनरीज	आईएस 10322 भाग 5 : खंड 8: 2013	ल्यूमिनरीज भाग 5: विशेष आवश्यकताएं खंड 8 इमरजेंसी लाइटिंग के लिए ल्यूमिनरीज
38.	यूपीएस / रेटिंग के इनवर्टर के 10केवीए	आईएस 16242 भाग 1: 2014	यूपीएस के लिए निर्बाध विद्युत प्रणाली (यूपीएस) खंड 1 सामान्य और सुरक्षा आवश्यकताएँ
39.	प्लाज्मा / एलसीडी / एलईडी / 32 इंच तक आकार के स्क्रीन की टीवी	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं
40.	विजुअल डिस्प्ले इकाइयाँ, 32 इंच तक स्क्रीन आकार के वीडियो मॉनिटर	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा - सामान्य आवश्यकताएँ
41.	सीसीटीवी कैमरे / सीसीटीवी रिकार्डर	आईएस 13252 : भाग 1 : 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा सामान्य आवश्यकताएँ
42.	घरेलू और इसी तरह के बिजली के उपकरणों के लिए एडेप्टर	आईएस 302 :भाग 1: 2008	सुरक्षा या घरेलू और समान विद्युत उपकरण भाग 1 सामान्य आवश्यकताएं
43.	यूएसबी संचालित बारकोड रीडर, बारकोड स्कैनर, आइरिस स्कैनर, ऑप्टिकल फिंगरप्रिंट स्कैनर	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा सामान्य आवश्यकताएँ
44.	स्मार्ट घड़ियाँ	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा सामान्य आवश्यकताएँ
45.	सामान्य प्रकाश व्यवस्था के लिए स्टैंडअलोन एलईडी मॉड्यूल	आईएस 16103: भाग 1: 2012	सामान्य प्रकाश व्यवस्था के लिए एलईडी मॉड्यूल: खंड 1 सुरक्षा आवश्यकतायें
46.	लाइटिंग चेन (रोप लाईट)	आईएस 10322: भाग 5 खंड 9: 2017	ल्यूमिनरीज: खंड 5 विशेष आवश्यकताएं धारा 9 रस्सी लाइट्स
47.	कीबोर्ड	आईएस 13252: भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा खंड 1 सामान्य आवश्यकताएं
48.	इंडक्शन चूल्हा	आईएस 302: भाग 2: खंड 6: 2009	घरेलू और समान विद्युत उपकरणों की सुरक्षा: खंड 2 विशेष आवश्यकताएं, खंड 6 खाना पकाने की रेंज, हॉब्स, ओवन और इसी तरह के उपकरण
49.	स्वचालित टेलर कैश डिस्पेंसिंग मशीन	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा खंड 1 सामान्य आवश्यकताएं
50.	यूएसबी प्रकार बाहरी हार्ड डिस्क ड्राइव	आईएस 13252: भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा खंड 1 सामान्य आवश्यकताएं
51.	वायरलेस हेडफोन और ईयरफोन	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण - सुरक्षा आवश्यकताओं
52.	यूएसबी टाइप एक्सटर्नल सॉलिड-स्टेट स्टोरेज डिवाइसेस (256 जीबी क्षमता से ऊपर)	आईएस 13252 भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा खंड 1 सामान्य आवश्यकताएं

53.	200 वाट से कम इनपुट पावर के साथ इलेक्ट्रॉनिक म्यूजिक सिस्टम	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण - सुरक्षा आवश्यकताएँ
54.	आउटपुट वोल्टेज 48 वी (अधिकतम) के साथ स्टैंडअलोन स्विच मोड पावर सप्लाई (एसएमपीएस)	आईएस 13252: भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा खंड 1 सामान्य आवश्यकताएं
55.	प्लाज्मा / एलसीडी / एलईडी टीवी के आलावा टेलीवीजन	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं
56.	चावल पकाने का बर्तन	आईएस 302 : भाग 2: खंड 15: 2009	घरेलू और इसी तरह के बिजली के उपकरणों की सुरक्षा: खंड 2 विशेष आवश्यकताएं: तरल पदार्थ हीटिंग के लिए खंड 15 उपकरण
57.	वायरलेस माइक्रोफोन	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं
58.	डिजिटल कैमरा	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा भाग 1 सामान्य आवश्यकताएं
59.	वीडियो कैमरा	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं
60.	वेब कैमरा (तैयार उत्पाद)	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं
61.	स्मार्ट स्पीकर (डिस्पले के साथ तथा डिस्पले के बिना)	आईएस 13252 :भाग 1: 2010	सूचना प्रौद्योगिकी उपकरण - सुरक्षा खंड 1 सामान्य आवश्यकताएं
62.	एलईडी उत्पादों के लिए डीमर्स	आईएस 60669: भाग 2: खंड 1: 2008	घरेलू और इसी तरह के बिजली के प्रतिष्ठानों के लिए स्विच के लिए इलेक्ट्रॉनिक स्विच मानकों की विशेष आवश्यकताएं ।
63.	ब्लूटूथ स्पीकर	आईएस 616: 2017	ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं

नोट : अनुसूची के प्रयोजन के लिए, भारतीय मानक का नवीनतम संस्करण, जिसमें संशोधन जारी किए गए हैं, जैसा कि समय-समय पर ब्यूरो द्वारा प्रकाशित और अधिसूचित किया जाता है, ब्यूरो द्वारा अधिसूचित तिथि से लागू होगा।

[फा. सं. डब्लू-47/4/2020-आइ.पी.एच.डब्ल्यू.–ई. एवं सू. प्रौ.मं.]

आशा नांगिया, वैज्ञानिक 'जी'

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

ORDER

New Delhi, the 18th March, 2021

S.O. 1248(E).—In exercise of the powers conferred by sub-section (1) and (2) of section 16 read with sub section (3) of section 25 of the Bureau of Indian Standards Act, 2016,(11 of 2016), the Central Government, after consulting the Bureau of Indian Standards, is of the opinion that it is necessary or expedient so to do in the public interest, hereby makes the following Order, namely:-

1. Short Title and commencement: - (1) This Order may be called the "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021".

2. Compulsory use of standard mark:-Goods or articles specified in the column (2) of the Schedule below shall conform to the corresponding Indian Standard given in the column (3) of the said Schedule and shall bear the 'Standard' Mark under a license from the Bureau of Indian Standards as per Scheme-lI of Schedule-II of Bureau of Indian Standards (Conformity Assessment) Regulations, 2018, provided that nothing in the Order shall apply in relation to goods or articles, as specified in the column (2) of the said

Schedule meant for export which conform to the specification required by the foreign buyer and to goods or articles, for which the Central Government has issued specific exemption letter based on reasons to be recorded in writing.

3. Timeline: The Order shall be applicable after expiry of six months of publication in official Gazette.

4. Concurrent Running with Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2012:- Nothing in the Order shall apply in relation to goods or articles, which are having valid registration number as per the provisions of ''Electronics and Information Technology Goods(Requirement of Compulsory Registration) Order, 2012". However the registration would be renewed under the provisions of "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021".

5. Certification and enforcement: In respect of the goods or articles specified in column (2) of the said Schedule, the Bureau of Indian Standards shall be the authority to certify and enforce conformity to the Standard Mark under this Order and in addition, whenever required, an officer not below the rank of an Under Secretary to the Government of India or District Industries Centre shall assist the Bureau in the enforcement of this Order. The surveillance would be conducted by agencies notified by Bureau of Indian Standards in consultation with Ministry of Electronics and Information Technology.

SCHEDULE

S. No.	Goods or articles	Indian Standard	Title of Indian Standard
(1)	(2)	(3)	(4)
1.	Electronic Games (Video)	IS 616:2017	Audio, Video and Similar Electronic Apparatus - Safety Requirements
2.	Laptops/Notebooks/Tablets	IS 13252 : Part 1 : 2010	Information Technology Equipment Safety -General Requirements
3.	Plasma/LCD/LED Televisions of screen size 32 inches & above	IS 616:2017	Audio, Video and Similar Electronic Apparatus -Safety Requirements
4.	Optical Disc Players with built in amplifiers of input power 200W and above	IS 616:2017	Audio, Video and Similar Electronic Apparatus - Safety Requirements
5.	Microwave Ovens	IS 302 : Part 2 : Sec 25 : 2014	Safety of household and similar electrical appliances: Part 2 Particular requirements: Section 25 Microwave ovens
6.	Visual Display Units, Video Monitors of screen size 32 inch & above	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety - General Requirements
7.	Printers/ Multi-Function Devices (MFD)/ Plotters	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety - General Requirements
8.	Scanners	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety - General Requirements
9.	Wireless Keyboards	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety - General Requirements
10.	Telephone Answering Machines	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety - General Requirements
11.	Amplifiers with input power 2000W and above	IS 616:2017	Audio, Video and Similar Electronic Apparatus - Safety Requirements
12.	Electronic Musical Systems 200 Watt & above	IS 616:2017	Audio, Video and Similar Electronic Apparatus – Safety Requirements
13.	Electronic Clocks with Mains Power	IS 302 : Part 2 : Sec 26 : 2014	Safety of household and similar electrical appliances: Part 2 Particular requirements: Section 26 Clocks
14.	Set Top Boxes	IS 13252 : Part 1 : 2010	Information Technology Equipment-Safety-General Requirements

15.	Automatic Data Processing Machines	IS 13252 : Part 1 : 2010	Information Technology Equipment-Safety-General Requirements
16.	Power Adaptors for IT Equipment	IS 13252 : Part 1 : 2010	Information Technology Equipment-Safety-General Requirements
17.	Power Adaptors for Audio, Video & Similar Electronic Apparatus	IS 616:2017	Audio, Video and Similar Electronic Apparatus - Safety Requirements
18.	UPS/Inverters of rating ≤ 5kVA	IS 16242 : Part 1 : 2014	Uninterruptible Power Systems (UPS) Part 1 General and Safety Requirements for UPS
19.	DC or AC Supplied Electronic Control gears for LED Modules	IS 15885 : Part 2 : Sec 13 : 2012	Safety of Lamp Control gear Part 2 Particular Requirements Section 13 d.c. or a.c. Supplied Electronic Control gear for LED Modules
20.	Sealed Secondary Cells/Batteries containing Alkaline or other non-acid Electrolytes for use in portable applications	IS 16046 : Part 1 : 2018	Secondary Cells and Batteries Containing Alkaline or Other Non-Acid Electrolytes — Safety Requirements for Portable Sealed Secondary Cells and for Batteries Made from Them for Use in Portable Applications Part 1 Nickel Systems
		IS 16046 : Part 2 : 2018	Secondary Cells and Batteries Containing Alkaline or Other Non-Acid Electrolytes — Safety Requirements for Portable Sealed Secondary Cells and for Batteries Made from Them for Use in Portable Applications Part 2 Lithium Systems
21.	Self-Ballasted LED Lamps for General Lighting Services	IS 16102 : Part 1 : 2012	Self-Ballasted LED Lamps for General Lighting Services Part 1 Safety Requirements
22.	Fixed General Purpose LED Luminaries	IS 10322 : Part 5 : Sec 1 : 2012	Luminaries Part 5 Particular Requirements Sec 1 General purpose luminaries
23.	Mobile Phones	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety- General Requirements
24.	Cash Registers	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety- General Requirements
25.	Point of Sale Terminals	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety- General Requirements
26.	Copying Machines/Duplicators	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety- General Requirements
27.	Smart Card Readers	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety- General Requirements
28.	Mail Processing Machines/Postage Machines/ Franking Machines	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety- General Requirements
29.	Passport Readers	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety- General Requirements
30.	Power Bank for use in portable applications	IS 13252 : Part 1 : 2010	Information Technology - Equipment – Safety - General Requirements
31.	Indian Language Support for Mobile Phones	IS 16333 : Part 3 : 2017	Mobile Phone Handsets Part 3 Indian Language Support for Mobile Phone Handsets – Specific Requirements
32.	Recessed LED Luminaries	IS 10322 : Part 5 : Sec 2 : 2012	Luminaries Part 5: Particular Requirements-Section 2: Recessed Luminaries

33.	LED Luminaries for Road and Street Lightings	IS 10322 : Part 5 : Sec 3 : 2012	Luminaries: Part 5: Particular Requirements, Section 3: Luminaries for Road and Street Lighting
34.	LED Flood Lights	IS 10322 : Part 5 : Sec 5 : 2013	Luminaries: Part 5: Particular Requirements, Section 5 Flood Lights
35.	LED Hand Lamps	IS 10322 : Part 5 : Sec 6 : 2013	Luminaries Part 5: Particular Requirements Section 6 Hand Lamps
36.	LED Lighting Chains	IS 10322 : Part 5 : Sec 7 : 2017	Luminaries Part 5: Particular Requirements Section 7 Lighting Chains
37.	LED Luminaries for Emergency Lighting	IS 10322 : Part 5 : Sec 8 : 2013	Luminaries Part 5: Particular Requirements Section 8 Emergency Lighting
38.	UPS/Inverters of rating ≤ 10kVA	IS 16242 : Part 1 : 2014	Uninterruptible Power Systems (UPS) Part 1 General and Safety Requirements for UPS
39.	Plasma/LCD/LED Televisions of screen size upto 32 inches	IS 616 : 2017	Audio, Video and Similar Electronic Apparatus -Safety Requirements
40.	Visual Display Units, Video Monitors of screen size upto 32 inch	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety - General Requirements
41.	CCTV Cameras/CCTV Recorders	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety General Requirements
42.	Adapters for household and similar electrical appliances	IS 302 : Part 1 : 2008	Safety or Household and similar electrical appliances Part 1 General requirements
43.	USB driven Barcode readers, barcode scanners, Iris scanners, Optical fingerprint scanner	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety General Requirements
44.	Smart Watches	IS 13252 : Part 1 : 2010	Information Technology Equipment - Safety General Requirements
45.	Standalone LED Modules for General Lighting	IS 16103 : Part 1 : 2012	LED modules for general lighting: Part 1 safety requirements
46.	Lighting Chains (Rope Lights)	IS 10322 : Part 5 : Sec 9 : 2017	Luminaries: Part 5 Particular Requirements Section 9 Rope Lights
47.	Keyboards	IS 13252 : Part 1 : 2010	Information technology equipment - safety part 1 general requirements
48.	Induction Stoves	IS 302 : Part 2 : Sec 6 : 2009	Safety of household and similar electrical appliances: part 2 particular requirements, section 6 cooking ranges, hobs, ovens and similar appliances
49.	Automatic Teller Cash dispensing machines	IS 13252 : Part 1 : 2010	Information technology equipment - safety part 1 general requirements
50.	USB Type External Hard Disk Drives	IS 13252 : Part 1 : 2010	Information technology equipment - safety part 1 general requirements
51.	Wireless Headphones and Earphones	IS 616 : 2017	Audio, video and similar electronic apparatus-safety requirements
52.	USB Type External Solid-State Storage Devices (above 256 GB capacity)	IS 13252 : Part 1 : 2010	Information technology equipment - safety part 1 general requirements
53.	Electronic Musical Systems with input power below 200 Watts	IS 616 : 2017	Audio, Video and Similar Electronic Apparatus – Safety Requirements

54.	Standalone Switch Mode Power Supplies (SMPS) with output voltage 48 V (max)	IS 13252 : Part 1 : 2010	Information technology equipment - safety part 1 general requirements
55.	Televisions other than Plasma/ LCD/LED TVs	IS 616 : 2017	Audio, video and similar electronic apparatus-safety requirements
56.	Rice Cookers	IS 302 : Part 2 : Sec 15 : 2009	safety of household and similar electrical appliances: part 2 particular requirements: section 15 appliances for heating liquids
57.	Wireless microphones	IS 616 : 2017	Audio, video and similar electronic apparatus-safety requirements
58.	Digital Cameras	IS 13252 : Part 1 : 2010	Information technology equipment - safety part 1 general requirements
59.	Video cameras	IS 616 : 2017	Audio, video and similar electronic apparatus-safety requirements
60.	Webcams (Finished Product)	IS 616 : 2017	Audio, video and similar electronic apparatus-safety requirements
61.	Smart Speakers (with and without Display)	IS 13252 : Part 1 : 2010	Information technology equipment - safety part 1 general requirements
62.	Dimmers for LED products	IS 60669 : Part 2 : Sec 1 : 2008	Switches for Household and Similar Fixed Electrical Installations Part 2 Particular Requirements Section 1 Electronic Switches
63.	Bluetooth speakers	IS 616 : 2017	Audio, video and similar electronic apparatus-safety requirements

Note : For the purpose of Schedule, the latest version of Indian standards including the amendments issued thereof, as published and notified by the Bureau from time to time, shall be applicable from the date as notified by the Bureau.

[F.No.W-47/4/2020-IPHW-MeitY]

ASHA NANGIA, Scientist 'G'

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. ALOK KUMAR Digitally signed by ALOK KUMAR Date: 2021.03.18 22:36:09 +05'30'

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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-26032021-226142
CG-DL-E-26032021-226142

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 1249] नई दिल्ली, बृहस्पतिवार, मार्च 25, 2021/चैत्र 4, 1943
No. 1249] NEW DELHI, THURSDAY, MARCH 25, 2021/CHAITRA 4, 1943

इलेक्ट्रॉनिक और सूचना प्रौद्योगिकी मंत्रालय

शुद्धिपत्र

नई दिल्ली, 25 मार्च, 2021

का. आ.1353(अ).—इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार की भारत के राजपत्र, असाधारण, भाग II, धारा 3, उप-धारा (ii) में दिनांक 18, मार्च, 2021 को प्रकाशित अधिसूचना क्रमांक 1248 (अ) में

(i) अनुसूची के क्रमांक संख्या 45 के कॉलम 2 में सामान्य प्रकाश व्यवस्था के लिए स्टैंडअलोन एलईडी मॉड्यूल' को सामान्य प्रकाश के लिए स्वतंत्र एलइडी मॉड्यूल ' पढ़ा जाए।

(ii) अनुसूची के क्रमांक संख्या 61 के कॉलम 3 में आईएस 13252 :भाग 1: 2010' को आईएस 616: 2017' पढ़ा जाए।

(iii) अनुसूची के क्रमांक संख्या 61 के कॉलम 4 में 'सूचना प्रौद्योगिकी उपकरण - सुरक्षा खंड 1 सामान्य आवश्यकताएं' को 'ऑडियो, वीडियो और समान इलेक्ट्रॉनिक उपकरण-सुरक्षा आवश्यकताएं' पढ़ा जाए।

[फा. नंबर डब्लू-47/4/2020-आइ० पी० एच० डब्लु० –ई० एवं सू० प्रौ० मं०]

आशा नांगिया, वैज्ञानिक 'जी'

टिपण्णी : प्रधान आदेश भारत के राजपत्र असाधारण में दिनांक 18 मार्च, 2021 के का० आ० संख्या 1248 (अ) के तहत प्रकाशित किया गया था।

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

CORRIGENDUM

New Delhi, the 25th March, 2021

S.O. 1353(E).—In the notification of the Government of India, Ministry of Electronics and Information Technology, published in the Gazette of India, Extraordinary, Part II, Section 3, Sub-section (ii), vide number G.S.R. 1248(E), dated the 18th March,2021:

(i) at column 2 of S. No 45 of the schedule; the entry 'Standalone LED Modules for General lighting' be read as 'Independent LED Modules for General Lighting'.

(ii) at column 3 of S. No. 61 of the schedule, the entry IS 13252 : Part 1 : 2010 be read as IS 616:2017.

(iii) at column 4 of S. No. 61 of the schedule, the entry 'Information technology equipment - safety part 1 general requirements' be read as 'Audio, video and similar electronic apparatus-safety requirements'.

[F.No.W-47/4/2020-IPHW-MeitY]

ASHA NANGIA, Scientist 'G'

Note : The Principal Order was published in the Gazette of India, Extraordinary vide S.O. number 1248(E), dated the 18th March, 2021.

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.

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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-15072021-228311
CG-DL-E-15072021-228311

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 2638] नई दिल्ली, बृहस्पतिवार, जुलाई 15, 2021/आषाढ़ 24, 1943
No. 2638] NEW DELHI, THURSDAY, JULY 15, 2021/ASHADHA 24, 1943

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय

आदेश

नई दिल्ली, 1 जुलाई 2021

का.आ. 2844(अ).—भारतीय मानक ब्यूरो अधिनियम, 2016 (2016 का 11) की धारा 25 की उप धारा (3) के साथ पठित धारा 16 की उप-धारा (1) और (2) द्वारा प्रदत्त शक्तियों के अनुसरण में केंद्र सरकार का यह मत है कि जनहित में ऐसा करना आवश्यक या समीचीन है, एतद्वारा इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (आवश्यक पंजीकरण की आवश्यकता) आदेश, 2021 में निम्नलिखित संशोधन करती है |

पैराग्राफ 5 के बाद, निम्नलिखित पैराग्राफ डाला जाएगा, अर्थात्:

6. आदेश के आस्थगित अनुप्रयोग" : ऐसे विनिर्माताओं, जो इस आदेश के अंतर्गत पहले से ही पंजीकृत है, के लिए भारत के संघीय सीमा के भीतर किसी नए स्थल पर विनिर्मित मॉल (वस्तुओ) के लिए आदेश का अनुप्रयोग को छः माह तक आस्थगित रखा जायेगा बशर्ते कि:

क) नया विनिर्माण स्थल उसी विनिर्माता की जिम्मेदारी के तहत आता हो ;

ख) इस नए स्थल पर विनिर्मित माल का विशिष्ठ प्रकार / मॉडल नंबर किसी अन्य स्थल पर उसकी विनिर्माण यूनिट के लिए उसी विनिर्माता के पंजीकरण के कार्य क्षेत्र (परिधि) में पहले से ही शामिल हो |

अनंतिम अवधी के दौरान ऐसे उत्पाद/ उत्पादों के लिए इस विनिर्माता को किस अन्य स्थल हेतु स्वीकृत की गयी पंजीकरण संख्या का समर्थन जारी रहेगा |

7. बंदरगाह पर मानक चिन्ह लगाना : "इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी माल (अनिवार्य पंजीकरण की आवश्यकता) आदेश, 2021" के तहत अधिसूचित सभी उत्पाद श्रेणियों के लिए, विदेशी विनिर्माण इकाई के भारत में स्थित सम्बद्ध कार्यालय या शाखा कार्यालय के प्रतिनिधि को ब्यूरो से पंजीकरण संख्या रखने वाले माल पर बंदरगाह पर मानक चिन्ह लगाने का प्रावधान उस विशेष उत्पाद श्रेणी के लिए आदेश के प्रभाव में आने की तारीख से तीन महीने (अधिकतम) का संक्रमण अवधि सीमा शुल्क से माल की निकासी के लिए उपलब्ध होगा ।

8. अति विशिष्ट उपकरणों के लिए छूट: नीचे दिए गए मानदंडों के अनुसार अति विशिष्ट उपकरण (एचएसई) को इस आदेश के लागू होने से छूट दी जाएगी, बशर्ते कि वे प्रति वर्ष प्रति मॉडल 100 इकाइयों से कम में निर्मित/आयातित हों-

क) तीन फेज बिजली आपूर्ति द्वारा संचालित उपकरण या

ख) एक फेज बिजली आपूर्ति द्वारा संचालित उपकरण जिनकी करंट रेटिंग 16 एम्पीयर या उससे अधिक हो, या

ग) 1.5 मीटर x 0.8 मीटर से अधिक आयाम वाले उपकरण, या

घ) 80 किलोग्राम से अधिक वजन वाले उपकरण

[फा. सं. डब्लू-47/4/2020-आइ.पी.एच.डब्ल्यू.–ई. एवं सू. प्रौ. मं.]

आशा नांगिया, वैज्ञानिक 'जी'

टिपण्णी : प्रधान आदेश भारत के राजपत्र असाधारण में दिनांक 18 मार्च, 2021 के का० आ० संख्या 1248 (अ) के तहत प्रकाशित किया गया था, तत्पश्चात एस.ओ. संख्या 1353 (अ) दिनांक 25.03.2021 के द्वारा संशोधित किया गया था |

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

ORDER

New Delhi, the 1st July, 2021

S.O. 2844(E).—n exercise of the powers conferred by sub-section (1) and (2) of section 16 read with sub section (3) of section 25 of the Bureau of Indian Standards Act, 2016, (11 of 2016), the Central Government is of the opinion that it is necessary or expedient so to do in the public interest, hereby makes the following amendments to the "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021",

After Paragraph 5, the following paragraph shall be inserted, namely:-

"6 . Deferred Application of Order"- For manufacturers that are already registered under this Order, the application of the Order shall be deferred by six months for goods manufactured at any new location within the territory of India provided:

(a) That the new manufacturing location is within the responsibility of the same manufacturer

(b) That the specific type/model number of the goods manufactured at this new location are already covered in the scope of registration of the same manufacturer for its manufacturing unit, at any other location.

During the interim period such product/products will continue to support the registration number granted to this manufacturer earlier for any other manufacturing location.

"7. Labeling at Custom ports:" For all the product categories notified under the "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021", a transition period of three months (max), from the date of coming into effect of the Order for the particular product category, would be available to the representative of the foreign manufacturing unit having liaison office or branch office located in India for affixing Standard Mark at the ports which are already having registration number from the Bureau for clearance of goods from customs.

"8. Exemption for Highly Specialized Equipment (HSE) : HSE as per the criteria given below shall stand exempted from the application of this Order provided they are manufactured/ imported in less than 100 units per model per year-

a. Equipment Powered by three phase power supply or

b. Equipment Powered by single phase power supply with current rating exceeding 16 Ampere or

c. Equipment with dimensions exceeding 1.5 m x 0.8 m or

d. Equipment with weight exceeding 80 Kg

[F. No. W-47/4/2020-IPHW-MeitY]

ASHA NANGIA, Scientist 'G'

Note : The Principal Order was published in the Gazette of India, Extraordinary vide S.O. number 1248(E), dated the 18th March, 2021 and subsequently amended vide S.O. No 1353(E) dated 25.03.2021

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.

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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-27042023-245471
CG-DL-E-27042023-245471

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 1841] नई दिल्ली, बुधवार, अप्रैल 26, 2023/वैशाख 6, 1945
No. 1841] NEW DELHI, WEDNESDAY, APRIL 26, 2023/VAISAKHA 6, 1945

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

(आईo पीo एचo डब्ल्यूo डिवीजन)

अधिसूचना

नई दिल्ली, 26 अप्रैल, 2023

विषय: "इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (अनिवार्य पंजीकरण की आवश्यकता) आदेश, 2021" में संशोधन

का.आ. 1929(अ).—भारतीय मानक ब्यूरो अधिनियम, 2016, (2016 का 11) की धारा 25 की उप-धारा (3) के साथ पठित धारा 16 की उप-धारा (1) और (2) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए केंद्र सरकार का यह मत है कि जनहित में ऐसा करना आवश्यक या समीचीन है, "इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी सामान (अनिवार्य पंजीकरण के लिए आवश्यकताएं) आदेश, 2021" में निम्नलिखित संशोधन करती है:

(i) उपरोक्त आदेश के पैरा 2 को इस प्रकार पढ़ा जाएगा:

मानक चिह्न का अनिवार्य उपयोग: - निम्नलिखित अनुसूची के कॉलम (2) में विनिर्दिष्ट माल या सामान,कथित अनुसूची के कॉलम (3) में दिए गए तदनुरूपी भारतीय मानक के अनुरूप होंगे और भारतीय मानक (अनुरूपता मूल्यांकन) ब्यूरो विनियमावली,2018 की अनुसूची-II की योजना- II के अनुसार भारतीय मानक ब्यूरो से एक लाइसेंस के तहत 'मानक' चिह्न रखेंगे बशर्ते कि इस आदेश में निर्यात के लिए निर्धारित कथित अनुसूची के कॉलम

(2) में यथा-विनिर्दिष्ट ऐसे माल या वस्तुओं के विनिर्माण के संबंध में लागू नहीं होगा जो विदेशी खरीदकर्ताओं द्वारा आवश्यक विनिर्देशों के अनुरूप होंगे। इलेक्ट्रॉनिक्स एवं सूचना प्रोधोगिकी मंत्रालय, उसके द्वारा समय-समय पर लेखबद्ध किए जाने और उसके द्वारा यथापरिलक्षित वाले कारणों से अनुसूची में वर्णित विनिर्दिष्ट वस्तुओं अथवा उत्पादों के प्रकार या श्रेणी को इस आदेश को लागू करने से छूट दे सकेगा।

(ii) निम्नलिखित प्रविष्टि "इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी माल (आवश्यक पंजीकरण की आवश्यकताएं) आदेश, 2021 की अनुसूची में क्रम संख्या 64 पर की जाए।

क्रम संख्या (1)	उत्पाद श्रेणी (2)	भारतीय मानक संख्या (3)	भारतीय मानक का शीर्षक (4)
64.	टेलीविजन सेट	आईएस 18112:2022	सैटेलाइट ब्रॉडकास्ट ट्रांसमिशन के लिए डिजिटल टेलीविजन रिसीवर - स्पेसिफिकेशन

2. "इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी सामान (अनिवार्य पंजीकरण के लिए आवश्यकताएं) आदेश, 2021" के प्रावधान इस अधिसूचना के द्वारा उक्त आदेश की अनुसूची में जोड़े गए कॉलम (2) में निर्दिष्ट माल या वस्तुओं पर कॉलम (3) में निर्दिष्ट अनुसार भारतीय मानक के अनुपालन के लिए आधिकारिक राजपत्र में इस अधिसूचना के प्रकाशन की तारीख से दो साल की समाप्ति पर लागू होंगे।

[फा. सं. : डब्ल्यु-47/7/2023-आईपीएचडब्ल्यु-एमईआईटीवाई]

आशा नांगिया, वैज्ञानिक ' जी '

नोट : प्रधान आदेश 18 मार्च, 2021 को एसओ संख्या 1248 (ई) के माध्यम से भारत के राजपत्र,अतिविशिष्ट में प्रकाशित किया गया था और बाद में दिनांक 25.03.2021 की एस.ओ. सं 1353 (ई) और दिनांक 01.07.2021 की एस.ओ. 2844 (ई) के जरिये इसे संशोधित किया गया।

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

(IPHW Division)

NOTIFICATION

New Delhi, the 26th April, 2023

Subject: Amendment to the "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021"

S.O. 1929(E).—In exercise of the powers conferred by sub-section (1) and (2) of section 16 read with sub section (3) of section 25 of the Bureau of Indian Standards Act, 2016, (11 of 2016), the Central Government is of the opinion that it is necessary or expedient so to do in the public interest, hereby makes the following amendments to the "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021":

(i) The Para 2 of the aforesaid Order shall be read as:

Compulsory use of standard mark:-Goods or articles specified in the column (2) of the Schedule below shall conform to the corresponding Indian Standard given in the column (3) of the said Schedule and shall bear the 'Standard' Mark under a license from the Bureau of Indian Standards as per Scheme-II of Schedule-II of Bureau of Indian Standards (Conformity Assessment) Regulations, 2018, provided that nothing in the Order shall apply in relation to manufacture of goods or articles, as specified in the column (2) of the said Schedule for export which

conform to the specification required by the foreign buyer. Further, the Ministry of Electronics and Information Technology may exempt, the application of this order to specific article or type or range of products mentioned in the Schedule for reasons to be recorded in writing and as identified by it from time to time.

(ii) The following entry be added at S. No. 64 in the Schedule of the "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021.

S. No (1)	Goods or Articles (2)	Indian Standard (3)	Title of Indian Standard (4)
64.	Television Sets	IS 18112:2022	Digital Television Receiver for Satellite Broadcast Transmission —Specification

2. The provisions of "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021" shall apply on the Goods or articles as specified in the column (2) added to the schedule of the said Order by virtue of this notification for conforming the corresponding Indian standard as specified in the column (3), on the expiry of two years from the date of publication of this notification in the Official Gazette.

[F. No. : W-47/7/2023-IPHW-MeitY]

ASHA NANGIA, Scientist 'G'

Note: The Principal Order was published in the Gazette of India, Extraordinary vide S.O. number 1248(E), dated the 18th March, 2021 and subsequently amended vide S.O. No 1353(E) dated 25.03.2021 and S.O. 2844(E). dated 01.07.2021.

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.

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

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-09042024-253632
CG-DL-E-09042024-253632

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 1569] नई दिल्ली, मंगलवार, अप्रैल 9, 2024/चैत्र 20, 1946
No. 1569] NEW DELHI, TUESDAY, APRIL 9, 2024/CHAITRA 20, 1946

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

(आईपीएचडब्ल्यू प्रभाग)

आदेश

नई दिल्ली, 9 अप्रैल, 2024

विषय: "इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल में संशोधन" (अनिवार्य पंजीकरण की आवश्यकता) आदेश, 2021"

का.आ. 1652(अ).—भारतीय मानक ब्यूरो अधिनियम, 2016, (2016 का 11) की धारा 25 की उपधारा (3) के साथ पठित धारा 16 की उप-धारा (1) और (2) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, केंद्र सरकार का यह मत है कि सार्वजनिक हित में ऐसा करना आवश्यक या समीचीन है, इसके द्वारा "इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (अनिवार्य पंजीकरण के लिए आवश्यकताएं) आदेश, 2021" में निम्नलिखित संशोधन किए जाते हैं:

2. सी.सी.टी.वी. कैमरे हेतु, कॉलम (5) की निम्नलिखित प्रविष्टि को "इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (अनिवार्य पंजीकरण के लिए आवश्यकताएं) आदेश, 2021 की अनुसूची में क्रम संख्या 41 पर जोड़ा जाएगा।

क्रमांक (1)	माल या सामान (2)	भारतीय मानक (3)	भारतीय मानक का शीर्षक (4)	अपेक्षित आवश्यकता (आवश्यकताएँ) (5)
41	सीसीटीवी कैमरा	आईएस 13252 : भाग 1 : 2010	सूचना तकनीकी उपकरण - सुरक्षा सामान्य आवश्यकताएं--	अनुलग्नक के अनुसार सीसीटीवी हेतु अनिवार्य आवश्यकता (आवश्यकताएँ)

3. "इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी माल (अनिवार्य पंजीकरण के लिए आवश्यकताएं) आदेश, 2021" के प्रावधान इस अधिसूचना के आधार पर उक्त आदेश की अनुसूची में जोड़े गए कॉलम (2) में निर्दिष्ट माल या सामान पर आधिकारिक राजपत्र में इस अधिसूचना के प्रकाशन की तारीख से छह महीने की समाप्ति पर, कॉलम (5) में निर्दिष्ट किए गए संबंधित अपेक्षित आवश्यकताओं के अनुरूप लागू होंगे। बीआईएस अनुरूपता मूल्यांकन विनियम, 2018 की योजना II के अनुसार बीआईएस मान्यता प्राप्त प्रयोगशालाओं से परीक्षण रिपोर्ट जमा करना मानक चिन्ह का उपयोग करने के लिए लाइसेंस प्राप्त करने हेतु एक पूर्व-आवश्यकता होगी।

[फा.सं. डब्ल्यू-43/11/2021-आईपीएचडब्ल्यू]
आशा नांगिया, समूह समन्वयक और वैज्ञानिक 'जी'

अनुलग्नक

सीसीटीवी की सुरक्षा के लिए अनिवार्य आवश्यकता

संवेदनशील जानकारी की सुरक्षा और सिस्टम को प्रभावी ढंग से संचालित करने के लिए सीसीटीवी (क्लोज-सर्किट टेलीविजन) प्रणाली को सुरक्षित करना महत्वपूर्ण है। परीक्षण के प्रमुख क्षेत्रों में एक्स्पोस्ड नेटवर्क सेवाएं, डिवाइस संचार प्रोटोकॉल, डिवाइस के यूएआरटी,जेटीएजी,एसडब्ल्युडी आदि तक भौतिक पहुंच, मेमोरी और फर्मवेयर निकालने की क्षमता, फर्मवेयर अपडेट प्रक्रिया सुरक्षा और डेटा का भंडारण और एन्क्रिप्शन शामिल हैं। सीसीटीवी सिस्टम की सुरक्षा के लिए यहां संक्षिप्त आवश्यकताएं दी गई हैं:

1. भौतिक सुरक्षा - भौतिक छेड़छाड़ को रोकने के लिए छेड़छाड़-प्रतिरोधी कैमरा एन्क्लोज़र और लॉकिंग तंत्र का उपयोग करें।
2. प्रमाणीकरण द्वारा अभिगम नियंत्रण, भूमिका-आधारित अभिगम नियंत्रण (आरबीएसी) और कर्मियों के परिवर्तनों को प्रतिबिंबित करने के लिए अभिगम अनुमतियों की नियमित रूप से समीक्षा और अद्यतनीकरण ।
3. डेटा ट्रांसमिशन के एन्क्रिप्शन को नियोजित करके नेटवर्क सुरक्षा
4. नियमित अपडेट द्वारा सॉफ़्टवेयर सुरक्षा, अप्रयुक्त सुविधाओं को अक्षम करना और सुदृढ़ पासवर्ड नीतियाँ
5. पेनीट्रेशन परीक्षण: साइबर हमलों के लिए सिस्टम के प्रतिरोध का आकलन करने और कमजोरियों को दूर करने के लिए पेनीट्रेशन परीक्षण को नियोजित करें।

अनिवार्य सुरक्षा आवश्यकताएँ

क्रमांक	वर्ग	परीक्षण पैरामीटर	क्या परीक्षण किया जाए	अपेक्षित दस्तावेज़
	हार्डवेयर स्तर सुरक्षा पैरामीटर (सॉफ़्टवेयर द्वारा समर्थित)	1.1 एक जटिल पासवर्ड द्वारा यह सत्यापित करें कि एप्लिकेशन लेयर डिबगिंग इंटरफ़ेस जैसे यूएसबी, यूएआरटी और अन्य सीरियल वेरिएंट अक्षम या संरक्षित हैं।	1. परीक्षण के तहत डिवाइस में उपयोग किए जा रहे एसओसी की डेटाशीट के माध्यम से यूएसबी, यूएआरटी और अन्य सीरियल वेरिएंट जैसे डिबगिंग इंटरफेस की उपलब्धता की पहचान करना 2. विक्रेता दस्तावेज़ीकरण में घोषित की गई सुरक्षा के लिए उत्पादन उपकरणों और संबंधित पहुंच नियंत्रण तंत्र में सक्षम पोर्ट/इंटरफ़ेस का सत्यापन और वेधता हार्डवेयर आधारित डिबगर्स और एक्सेस कंट्रोल तंत्र का उपयोग करके सभी पोर्ट और यूएसबी, यूएआरटी और अन्य सीरियल वेरिएंट जैसे डिबगिंग इंटरफेस को सक्षम/अक्षम करने को सत्यापित करने के लिए ओईएम	विक्रेता द्वारा निम्नलिखित को उपलब्ध करना होगा: 1. डिवाइस में उपयोग किए जा रहे एसओसी की डेटाशीट। 2. उत्पादन उपकरणों में सक्षम पोर्ट/इंटरफ़ेस से संबंधित दस्तावेज़ीकरण और उसकी सुरक्षा के लिए संबंधित एक्सेस नियंत्रण तंत्र। 3. डिवाइस के विनिर्माण/प्रावधान की प्रक्रिया प्रवाह

			टीम की उपस्थिति में परीक्षण। 4. डिबगिंग इंटरफेस के बारे में विक्रेता के दावे को मान्य करने के लिए विनिर्माण सुविधा की प्रक्रिया लेखा परीक्षा जो प्रावधान के दौरान बंद/अक्षम हैं। [उदाहरण के लिए, ब्लॉक कनेक्शन आरेख के माध्यम से होस्ट माइक्रोकंट्रोलर के बीच पिन कनेक्शन और विभिन्न उप घटकों/परिधीय के साथ इसकी बातचीत को दर्शाया गया है।]	
		1.2 सत्यापित करें कि क्रिप्टोग्राफ़िक कुंजी और प्रमाणपत्र प्रत्येक व्यक्तिगत डिवाइस के लिए अद्वितीय हैं।	डिवाइस इको-सिस्टम में उपयोग की जा रही सभी कुंजियों और प्रमाणपत्रों की पहचान करना और इनके माध्यम से सत्यापन करना: ओईएम टीम की उपस्थिति में परीक्षण कोड समीक्षा कुंजी-जीवन चक्र प्रक्रिया संबंधी प्रक्रिया लेखा परीक्षा	विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा: 1. डिवाइस इकोसिस्टम में उपयोग की जा रही सभी कुंजियों और प्रमाणपत्रों की सूची 2. मुख्य प्रबंधन जीवन चक्र (उद्देश्य, उत्पादन, भंडारण, विनाश/शून्यीकरण, वैधता, कुंजी परिवर्तन/रोटेशन)
		1.3 सत्यापित करें कि जेटीएजी या एसडबल्यूडी जैसे ऑन-चिप डिबगिंग इंटरफ़ेस अक्षम हैं या उपलब्ध सुरक्षा तंत्र सक्षम और उचित रूप से कॉन्फ़िगर किया गया है।	1. परीक्षण के तहत डिवाइस में उपयोग किए जा रहे एसओसी की डेटाशीट के माध्यम से यूएसबी, यूएआरटी और अन्य सीरियल वेरिएंट जैसे डिबगिंग इंटरफेस की उपलब्धता की पहचान करना 2. विक्रेता दस्तावेज़ में घोषित की गई सुरक्षा के लिए उत्पादन उपकरणों और संबंधित पहुंच नियंत्रण तंत्र में सक्षम पोर्ट/इंटरफ़ेस का सत्यापन और वेधता 3. इंटरफ़ेस सक्षम होने की स्थिति में उनके प्रासंगिक हार्डवेयर आधारित डिबगर्स और एक्सेस कंट्रोल तंत्र का उपयोग करके सभी पोर्ट और यूएसबी, यूएआरटी और अन्य सीरियल वेरिएंट जैसे डिबगिंग इंटरफेस को सक्षम/अक्षम करने को सत्यापित करने के लिए ओईएम टीम की उपस्थिति में परीक्षण। 4. डिबगिंग इंटरफेस के बारे में विक्रेता के दावे को मान्य करने के लिए विनिर्माण सुविधा की प्रक्रिया लेखा परीक्षा जो प्रावधान	विक्रेता द्वारा निम्नलिखित को उपलब्ध करना होगा: 1. डिवाइस में उपयोग किए जा रहे एसओसी की डेटाशीट। 2. उत्पादन उपकरणों में सक्षम पोर्ट/इंटरफ़ेस से संबंधित दस्तावेज़ीकरण और उसकी सुरक्षा के लिए संबंधित एक्सेस नियंत्रण तंत्र। 3. डिवाइस के विनिर्माण/प्रावधान की प्रक्रिया प्रवाह

			के दौरान बंद/अक्षम हैं। [उदाहरण के लिए, ब्लॉक कनेक्शन आरेख के माध्यम से होस्ट माइक्रोकंट्रोलर के बीच पिन कनेक्शन और विभिन्न उप घटकों/परिधीय के साथ इसकी बातचीत को दर्शाया गया है।]	
		1.4 सत्यापित करें कि विश्वसनीय निष्पादन लागू और सक्षम है, यदि डिवाइस एसओसी या सीपीयू पर उपलब्ध है।	विक्रेता द्वारा प्रस्तुत एसओसी डेटाशीट और तकनीकी दस्तावेज के माध्यम से डिवाइस में टीईई/एसई/टीपीएम उपलब्ध है या नहीं, इसकी पहचान करना। आगे का मूल्यांकन डिवाइस पर लागू परिदृश्यों के आधार पर किया जाता है जैसा कि नीचे परिभाषित किया गया है: **स्थिति 1: टीईई/एसई/टीपीएम उपलब्ध नहीं है:** कोई और अग्रिम मूल्यांकन नहीं **स्थिति 2: टीईई/एसई/टीपीएम उपलब्ध और सक्षम है:** कोड-समीक्षा के माध्यम से सत्यापन कि क्रिप्टो फ़ंक्शन को टीईई/एसई/टीपीएम एपीआई के माध्यम से बुलाया जाता है। **स्थिति 3: टीईई/एसई/टीपीएम उपलब्ध है लेकिन विक्रेता द्वारा सक्षम नहीं किया गया है:** आवश्यकता के अनुरूप न होने के रूप में करार दिया गया। टीईई/एसई/टीपीएम को सक्षम और कार्यान्वित करने के लिए ओईएम की आवश्यकता होती है।	विक्रेता द्वारा निम्नलिखित को उपलब्ध कराना होगा: 1. डिवाइस में उपयोग किए जा रहे एसओसी की डेटाशीट। 2. डिवाइस का उपयोगकर्ता मैनुअल/तकनीकी विनिर्देश 3. टीईई एपीआई कॉल के कोड स्निपेट, जहां भी लागू हो
		1.5 सत्यापित करें कि संवेदनशील डेटा, निजी कुंजियाँ और प्रमाणपत्र एक सुरक्षित तत्व, टीपीएम, टीईई (विश्वसनीय निष्पादन पर्यावरण) में सुरक्षित रूप से संग्रहीत हैं, या सुदृढ़ क्रिप्टोग्राफी का उपयोग करके संरक्षित हैं।	डिवाइस इको-सिस्टम, संवेदनशील डेटा और उनके भंडारण तंत्र में उपयोग की जा रही सभी कुंजियों और प्रमाणपत्रों की पहचान करना; और इसके माध्यम से सत्यापन करना : • ओईएम टीम की उपस्थिति में परीक्षण • कोड समीक्षा • कुंजी-जीवन चक्र प्रक्रिया संबंधी प्रक्रिया लेखा परीक्षा	विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा: 1. डिवाइस इकोसिस्टम में उपयोग की जा रही सभी कुंजियों और प्रमाणपत्रों की सूची 2. डिवाइस में सक्षम किए जाने वाले सुरक्षित कॉन्फ़िगरेशन के साथ कार्यान्वित सभी संवेदनशील डेटा की उनके इच्छित उपयोग और सुरक्षित भंडारण तंत्र (ओं) के साथ सूची। 3. मुख्य प्रबंधन जीवन चक्र (उद्देश्य, उत्पादन, भंडारण, विनाश/शून्यीकरण, वैधता, कुंजी परिवर्तन/रोटेशन) निजी कुंजी

				और प्रमाणपत्र।
		1.6 टैम्पर रेसिस्टेंस और/या टैम्पर का पता लगाने वाली सुविधाओं की उपस्थिति सत्यापित करें।	सॉफ़्टवेयर और हार्डवेयर से टैंपरिंग को रोकने के लिए डिवाइस में लागू किए गए उपायों को सत्यापित करने के लिए ओईएम टीम की उपस्थिति में परीक्षण।	विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा: 1. सॉफ्टवेयर से टैंपरिंग रोकने के लिए डिवाइस संबंधी उपलब्ध उपाय। 2. हार्डवेयर से टैंपरिंग रोकने के लिए डिवाइस संबंधी उपलब्ध उपाय।
		1.7 चिप निर्माता द्वारा प्रदान की गई कोई भी उपलब्ध बौद्धिक संपदा सुरक्षा तकनीक सक्षम है।	यदि उपलब्ध हो तो चिप निर्माता द्वारा प्रदान की गई बौद्धिक संपदा सुरक्षा तकनीकों को सक्षम करने के लिए ओईएम टीम की उपस्थिति में परीक्षण।	विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा: 1. एसओसी की डेटाशीट 2. चिप निर्माता द्वारा प्रदान की गई बौद्धिक संपदा संरक्षण प्रौद्योगिकियों के संबंध में दस्तावेज़ीकरण, जिन्हें सक्षम किया गया है। 3. यदि चिप निर्माता द्वारा कोई बौद्धिक संपदा संरक्षण तकनीक प्रदान नहीं की जा रही है, तो एक घोषणा जिसमें समरूप बात हो।
		1.8 सत्यापित करें कि डिवाइस लोड करने से पहले बूट छवि हस्ताक्षर को सत्यापित करता है।	निम्नलिखित को सत्यापित करने के लिए ओईएम टीम की उपस्थिति में परीक्षण करना : 1. वैध बूट छवि प्रदान किए जाने पर डिवाइस दस्तावेज़ीकृत सुरक्षित बूट प्रक्रिया के साथ सफलतापूर्वक बूट हो जाता है। 2. छेड़छाड़ की गई बूट छवि (जैसे मिसिंग हस्ताक्षर, अमान्य हस्ताक्षर) प्रदान किए जाने पर डिवाइस बूट नहीं होता है।	विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा: 1. एसओसी की डेटाशीट 2. सुरक्षित बूट के संबंध में डिवाइस के तकनीकी विनिर्देश (इसमें शामिल कुंजियाँ और उनका प्रबंधन जीवन चक्र * , हस्ताक्षर सत्यापन प्रक्रिया और लागू होने पर कोई अन्य सुरक्षित तंत्र शामिल होना चाहिए।)
		1.9 एम्बेडेड डिवाइस पर क्रिप्टोग्राफ़िक रूप से सुरक्षित छद्म-यादृच्छिक संख्या जनरेटर के उपयोग को सत्यापित करें (उदाहरण के लिए, चिप-प्रदत्त यादृच्छिक संख्या जनरेटर का उपयोग करके)।	डिवाइस में उपयोग किए जा रहे यादृच्छिक संख्या जनरेटर के संबंध में विक्रेता द्वारा प्रदान किए गए दस्तावेज़ का सत्यापन करना । कोड-समीक्षा के माध्यम से सत्यापन कि डिवाइस में यादृच्छिक संख्या जनरेटर या संबंधित लाइब्रेरी का उपयोग किया जा रहा है।	विक्रेता को अपने इच्छित उपयोग के साथ डिवाइस में उपयोग किए जा रहे यादृच्छिक जेनरेटर (या तो हार्डवेयर आधारित या सॉफ़्टवेयर आधारित या दोनों) के संबंध में दस्तावेज़ प्रस्तुत करना होगा। यदि हार्डवेयर आधारित यादृच्छिक संख्या जनरेटर का उपयोग किया जा रहा है, तो विक्रेताओं को निम्नलिखित प्रस्तुत करना होगा: 1. एसओसी की डेटाशीट 2. यादृच्छिक जनरेटर के संबंध में डिवाइस की तकनीकी विशिष्टताएँ यदि सॉफ्टवेयर आधारित

				यादृच्छिक संख्या जनरेटर का उपयोग किया जा रहा है, तो विक्रेताओं को इसके लिए उपयोग की जाने वाली लाइब्रेरी प्रदान करनी होगी।
2.	सॉफ्टवेयर/फर्मवेयर	2.1 सत्यापित करें कि एएसएलआर और डीईपी जैसे मेमोरी सुरक्षा नियंत्रण एम्बेडेड/आईओटी ऑपरेटिंग सिस्टम द्वारा सक्षम हैं, यदि लागू हो।	कमांड लाइन-आधारित टूल/कमांड या डीईपी, ईएमईटी टूल जैसे किसी अन्य ओपन-सोर्स टूल का उपयोग करके डिवाइस में उपलब्ध और सक्षम घोषित मेमोरी सुरक्षा नियंत्रणों को सत्यापित करने के लिए ओईएम टीम की उपस्थिति में परीक्षण करना।	विक्रेता को डिवाइस में उपलब्ध और सक्षम मेमोरी सुरक्षा नियंत्रणों की घोषणा प्रस्तुत करनी होगी।
		2.2 सत्यापित करें कि फ़र्मवेयर ऐप्स ट्रांसपोर्ट लेयर सुरक्षा का उपयोग करके ट्रांज़िट में डेटा की सुरक्षा करते हैं।	1. यह सत्यापित करना कि सुरक्षित संचार स्थापित करने के लिए सुदृढ़ एन्क्रिप्शन एल्गोरिदम और सुरक्षित टीएलएस संस्करण डिवाइस द्वारा समर्थित है। 2. यह सत्यापित करना कि डिवाइस सर्वर के टीएलएस प्रमाणपत्र को ठीक से मान्य करता है ताकि यह सुनिश्चित हो सके कि यह विश्वसनीय है और इसके साथ छेड़छाड़ नहीं की गई है। 3. सुभेद्धताओं का परीक्षण जो टीएलएस कनेक्शन की सुरक्षा को प्रभावित कर सकता है जैसे पैडिंग ऑरेकल हमले, या सुभेद्ध सिफर सुइट्स। 4. खुले पॉर्ट्स की पहचान करने के लिए एनएमएपी जैसे टूल का उपयोग करना जिसके माध्यम से डिवाइस तक पहुंचा जा सकता है जिससे अनपेक्षित डेटा पुनर्प्राप्ति हो सकती है। 5. यह सत्यापित करना कि टीएलएस सत्र बर्पसुइट जैसे टूल का उपयोग करके मैन-इन-द-मिडिल हमलों का उपयोग करके नेटवर्क ट्रैफ़िक के अवरोधन और डिक्रिप्शन के प्रयासों के लिए प्रतिरोधी हैं।	विक्रेता ट्रांसपोर्ट लेयर सुरक्षा से संबंधित एप्लिकेशन और फर्मवेयर में उपलब्ध कॉन्फ़िगरेशन से संबंधित विनिर्देश और दस्तावेज प्रस्तुत करेगा।
		2.3 सत्यापित करें कि फ़र्मवेयर ऐप्स सर्वर कनेक्शन के डिजिटल हस्ताक्षर को मान्य करते हैं।	1. उन परिदृश्यों की पहचान करना जब डिवाइस बाह्य दुनिया के साथ सर्वर कनेक्शन स्थापित करता है और निम्नलिखित की पुष्टि करता है:	विक्रेता को उपयोग के मामलों का उल्लेख करते हुए एक दस्तावेज़ प्रस्तुत करना होगा जब डिवाइस बाहरी दुनिया के साथ सर्वर कनेक्शन स्थापित करता है, जिसमें सर्वर कनेक्शन के डिजिटल

			• सुरक्षित सर्वर कनेक्शन और डिजिटल हस्ताक्षर सत्यापन से संबंधित सुरक्षा सुविधाएँ, जैसे सुदृढ़ साईफर सुइट्स, सुरक्षित टीएलएस संस्करण, एसएसएल पिनिंग आदि कोड वॉकथ्रू द्वारा समर्थित हैं। • डिवाइस में उचित प्रमाणपत्र सत्यापन, प्रमाणपत्र श्रृंखला सत्यापन और प्रमाणपत्र निरस्तीकरण जांच लागू की जाती हैं। 2. सुभेद्धताओं का परीक्षण जो टीएलएस कनेक्शन की सुरक्षा को प्रभावित कर सकता है जैसे पैडिंग ऑरेकल हमले, या सुभेद्ध सिफर सुइट्स। 3. खुले पोर्ट की पहचान करने के लिए एनएमएपी जैसे टूल का उपयोग करना जिसके माध्यम से डिवाइस तक पहुंचा जा सकता है जिससे अनपेक्षित डेटा पुनर्प्राप्ति हो सकती है। 4. यह सत्यापित करना कि टीएलएस सत्र बर्पसुइट जैसे उपकरणों का उपयोग करके मैन-इन-द-मिडिल हमलों का उपयोग करके नेटवर्क ट्रैफ़िक के अवरोधन और डिक्रिप्शन के प्रयासों के लिए प्रतिरोधी हैं।	हस्ताक्षरों को मान्य करते समय सुरक्षा उपायों के बारे में विस्तृत जानकारी होगी।
		2.4 सत्यापित करें कि प्रतिबंधित सी फ़ंक्शंस के किसी भी उपयोग को उचित सुरक्षित समकक्ष फ़ंक्शंस के साथ बदल दिया गया है।	निम्नलिखित में से किसी भी दृष्टिकोण के माध्यम से लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण का उपयोग करके ओईएम टीम की उपस्थिति में सुरक्षित कोड समीक्षा [स्वचालित और मैन्युअल दोनों]: 1. फ़र्मवेयर कोड के साथ विक्रेता द्वारा मूल्यांकन एजेंसी का दौरा करना और मूल्यांकन एजेंसी के पास उपलब्ध लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण को	विक्रेता द्वारा उपलब्ध करना होगा: 1. कोड समीक्षा के लिए फ़र्मवेयर बायनेरिज़। 2. आंतरिक कोड समीक्षा रिपोर्ट

			अपने सिस्टम में स्थापित करना। [अनुशंसित] 2. विक्रेता द्वारा फर्मवेयर कोड और उनके पास उपलब्ध किसी भी लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण के साथ मूल्यांकन एजेंसी का दौरा करना और मूल्यांकन एजेंसी के प्रतिनिधियों की उपस्थिति में कोड समीक्षा गतिविधि का प्रदर्शन करना। 3. मूल्यांकन एजेंसी को उनके पास उपलब्ध लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण स्थापित करने के लिए विक्रेता साइट पर सिस्टम की रिमोट एक्सेस प्रदान करना। 4. विक्रेताओं के पास उपलब्ध लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण के साथ फर्मवेयर कोड वाले मूल्यांकन एजेंसी को विक्रेता साइट पर सिस्टम की दूरस्थ अभिगम प्रदान करना।	
		2.5 सत्यापित करें कि प्रत्येक फर्मवेयर तृतीय पक्ष के घटकों, संस्करण और प्रकाशित सुभेद्धताओं को सूचीबद्ध करने वाली सामग्री का एक सॉफ्टवेयर बिल रखता है।	फ़र्मवेयर पर एफ़एसीटी जैसे स्वचालित उपकरण चलाकर तृतीय-पक्ष घटकों की प्रस्तुत सूची का सत्यापन करना । सार्वजनिक रूप से उपलब्ध सुभेद्यता डेटाबेस के माध्यम से तीसरे पक्ष के घटकों में सुभेद्धताओं की पहचान करना तृतीय पक्ष के घटकों में किसी भी ज्ञात सुभेद्धता को दूर करने के लिए फर्मवेयर के लिए नियमित सुरक्षा अपडेट और पैच प्रदान करने के लिए विक्रेता द्वारा परिभाषित प्रक्रिया का सत्यापन और वैधता।	विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा: 1. तृतीय पक्ष के घटकों और संस्करणों सहित सामग्री के सॉफ़्टवेयर बिल की जानकारी के लिए दस्तावेज़ीकरण करना । 2. निम्नलिखित के लिए संगठन प्रक्रिया और नीतियां: • तृतीय पक्ष के घटकों में पहचानी गई किसी भी सुभेद्धता को संबोधित करना और ठीक करना। • ग्राहकों को सुरक्षा मुद्दों या सुभेद्धताओं के बारे में सूचित करना और उसके लिए सुरक्षा अद्यतन और पैच प्रदान करना। 3. उपकरणों के लिए जारी किए गए पैच/फिक्स के साथ फर्मवेयर और तृतीय-पक्ष बाइनरी, लाइब्रेरी और फ्रेमवर्क को बनाए रखने के लिए कॉन्फ़िगरेशन प्रबंधन प्रणाली और संबंधित नीतियां।
		2.6 हार्डकोडेड क्रेडेंशियल्स (बैकडोर) के लिए तृतीय-पक्ष बायनेरिज़, लाइब्रेरीज़,	निम्नलिखित में से किसी भी दृष्टिकोण के माध्यम से लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण का उपयोग करके स्वतंत्र सुरक्षित	विक्रेता द्वारा उपलब्ध करना होगा: 1. कोड समीक्षा के लिए फ़र्मवेयर बायनेरिज़।

		फ्रेमवर्क सहित सभी कोड की समीक्षा की जाती है।	कोड समीक्षा [स्वचालित और मैन्युअल दोनों]: 1. फ़र्मवेयर कोड के साथ विक्रेता द्वारा मूल्यांकन एजेंसी का दौरा करना और मूल्यांकन एजेंसी के पास उपलब्ध लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण को अपने सिस्टम में स्थापित करना। [अनुशंसित] 2. विक्रेता द्वारा फर्मवेयर कोड और उनके पास उपलब्ध किसी भी लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण के साथ मूल्यांकन एजेंसी का दौरा करना और मूल्यांकन एजेंसी के प्रतिनिधियों की उपस्थिति में कोड समीक्षा गतिविधि का प्रदर्शन करना। 3. मूल्यांकन एजेंसी को उनके पास उपलब्ध लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण स्थापित करने के लिए विक्रेता साइट पर सिस्टम की दूरस्थ पहुंच प्रदान करना। 4. विक्रेताओं के पास उपलब्ध लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण के साथ फर्मवेयर कोड वाले मूल्यांकन एजेंसी को विक्रेता साइट पर सिस्टम की दूरस्थ पहुंच प्रदान करना ।	2. आंतरिक कोड समीक्षा रिपोर्ट
		2.7 सत्यापित करें कि फ़र्मवेयर ऐप्स डिजिटल हस्ताक्षर को किसी विश्वसनीय सर्वर पर पिन करते हैं।	1. उन परिदृश्यों की पहचान करना जब डिवाइस बाहरी दुनिया के साथ सर्वर कनेक्शन स्थापित करता है और निम्नलिखित की पुष्टि करता है: • सुरक्षित सर्वर कनेक्शन और डिजिटल हस्ताक्षर सत्यापन से संबंधित सुरक्षा सुविधाएँ, जैसे सुदृढ़ सिफर सुइट्स, सुरक्षित टीएलएस संस्करण, एसएसएल पिनिंग आदि कोड वॉकथ्रू द्वारा समर्थित हैं। • डिवाइस में उचित प्रमाणपत्र सत्यापन, प्रमाणपत्र श्रृंखला सत्यापन और प्रमाणपत्र निरस्तीकरण जांच लागू की जाती हैं	विक्रेता को उपयोग के मामलों का उल्लेख करते हुए एक दस्तावेज़ प्रस्तुत करना होगा जब डिवाइस बाहरी दुनिया के साथ सर्वर कनेक्शन स्थापित करता है, जिसमें सर्वर कनेक्शन के डिजिटल हस्ताक्षरों को मान्य करते समय सुरक्षा उपायों के बारे में विस्तृत जानकारी होगी।

		2.8 (वर्बोज़ डिबगिंग प्रतीकों को हटाने) में बाधा डालने के लिए सुरक्षा नियंत्रण मौजूद हैं ।	फ़र्मवेयर रिवर्स इंजीनियरिंग में बाधा डालने के लिए विक्रेता द्वारा प्रदान किए गए सुरक्षा नियंत्रणों को सत्यापित करने के लिए, ओईएम टीम की उपस्थिति में परीक्षण करना ।	फ़र्मवेयर रिवर्स इंजीनियरिंग में बाधा डालने के लिए विक्रेता को सुरक्षा नियंत्रण के संबंध में दस्तावेज़ प्रस्तुत करना होगा।
		2.9 सत्यापित करें कि फ़र्मवेयर अपडेट प्रक्रिया समय जांच बनाम उपयोग के समय के हमलों के प्रति संवेदनशील नहीं है।	डिवाइस में लागू किए गए उपायों को सत्यापित करने के लिए ओईएम टीम की उपस्थिति में परीक्षण किया गया, ताकि इसे समय- समय पर उपयोग किए जाने वाले हमलों के प्रति प्रतिरोधी बनाया जा सके।	विक्रेता को डिवाइस में लागू किए गए उपायों को प्रस्तुत करना होगा ताकि इसे समय-जांच बनाम उपयोग के समय के हमलों के प्रति प्रतिरोधी बनाया जा सके।
		2.10 सत्यापित करें कि डिवाइस इंस्टॉल करने से पहले कोड साइनिंग का उपयोग करता है और फ़र्मवेयर अपग्रेड फ़ाइलों को मान्य करता है।	निम्नलिखित को सत्यापित करने के लिए ओईएम टीम की उपस्थिति में परीक्षण करना : क. वैध अपडेट पैकेज उपलब्ध कराए जाने पर डिवाइस दस्तावेज़ीकृत सुरक्षित अपग्रेड प्रक्रिया के साथ सफलतापूर्वक अपडेट हो जाता है। ख. छेड़छाड़ किए गए अपडेट पैकेज (जैसे मिसिंग हस्ताक्षर, अमान्य हस्ताक्षर) प्रदान किए जाने पर डिवाइस बूट नहीं होता है।	विक्रेता को सुरक्षित फ़र्मवेयर अपग्रेड प्राप्त करने की प्रक्रिया प्रस्तुत करनी होगी जिसमें शामिल कुंजियाँ और उनका प्रबंधन जीवन चक्र * , हस्ताक्षर सत्यापन प्रक्रिया और लागू होने पर कोई अन्य सुरक्षित तंत्र शामिल होना चाहिए।
		2.11 सत्यापित करें कि डिवाइस को वैध फर्मवेयर के पुराने संस्करण (एंटी-रोलबैक) में डाउनग्रेड नहीं किया जा सकता है।	यह सत्यापित करने के लिए कि डिवाइस को वैध फर्मवेयर के पुराने संस्करणों (एंटी-रोलबैक) में डाउनग्रेड नहीं किया जा सकता है, ओईएम टीम की उपस्थिति में परीक्षण किया जा रहा है।	विक्रेता को सुरक्षित फ़र्मवेयर अपग्रेड प्राप्त करने की प्रक्रिया प्रस्तुत करनी होगी जिसमें शामिल कुंजियाँ और उनका प्रबंधन जीवन चक्र * , हस्ताक्षर सत्यापन प्रक्रिया और लागू होने पर कोई अन्य सुरक्षित तंत्र शामिल होना चाहिए।
		2.12 सत्यापित करें कि फ़र्मवेयर पूर्वनिर्धारित शेड्यूल पर स्वचालित फ़र्मवेयर अपडेट कर सकता है।	सत्यापन लागू परिदृश्य के अनुसार किया जाएगा: **स्थिति 1: स्वचालित ओटीए अपडेट उपलब्ध हैं:** इन-फील्ड उपकरणों को स्वचालित अपडेट/अपग्रेड जारी करने के लिए एक मानक संचालन प्रक्रिया विक्रेता द्वारा प्रस्तुत की जानी आवश्यक है जिसका मूल्यांकन, मूल्यांकन एजेंसी द्वारा सी20, सी21 और सी22 सुरक्षा आवश्यकता के अनुसार किया जा सकता है।	विक्रेता निम्नलिखित प्रदान करेगा: विक्रेता द्वारा निम्नलिखित को प्रस्तुत कराना होगा: 1. उपलब्ध अपडेट के तरीके यानी स्वचालित, मैन्युअल या दोनों। 2. उपकरणों को अपडेट जारी करने के संबंध में संगठनात्मक प्रक्रिया और नीतियां।

			स्थिति 2: स्वचालित ओटीए अपडेट उपलब्ध नहीं हैं और विक्रेता मैन्युअल अपडेट प्रदान करता है: इन-फील्ड डिवाइसों में मैन्युअल अपडेट/अपग्रेड जारी करने के लिए विक्रेता द्वारा एक मानक संचालन प्रक्रिया प्रस्तुत की जानी आवश्यक है जिसका मूल्यांकन, मूल्यांकन एजेंसी द्वारा सी20, सी21 और सी22 सुरक्षा आवश्यकता के अनुसार किया जा सकता है।	
3.	सुरक्षित प्रक्रिया अनुरूपता	3.1 सत्यापित करें कि वायरलेस संचार परस्पर प्रमाणित हैं।	विक्रेता द्वारा दस्तावेज़ में निर्धारित आपसी प्रमाणीकरण की प्रक्रिया को सत्यापित करने के लिए, ओईएम टीम की उपस्थिति में परीक्षण करना ।	विक्रेताओं को वायरलेस संचार शुरू होने पर डिवाइस में लागू पारस्परिक प्रमाणीकरण की प्रक्रिया के संबंध में दस्तावेज़ प्रदान करना होगा। यदि डिवाइस वायरलेस संचार का समर्थन नहीं करता है, तो विक्रेता को इसके लिए एक घोषणा पत्र प्रदान करना होगा।
		3.2 सत्यापित करें कि वायरलेस संचार एक एन्क्रिप्टेड चैनल पर भेजा जाता है।	संचार प्रक्रिया सत्यापन में उपयोग किए जा रहे सभी सुरक्षा तंत्रों की पहचान करना: • ओईएम टीम की उपस्थिति में परीक्षण करना • कोड समीक्षा • कुंजी-जीवन चक्र प्रक्रिया संबंधी प्रक्रिया लेखा परीक्षा लेखा परीक्षा	संचार के वायरलेस मोड के माध्यम से भेजे जाने वाले डेटा से छेड़छाड़ को रोकने के लिए विक्रेताओं को डिवाइस में लागू सुरक्षा उपायों के संबंध में दस्तावेज उपलब्ध कराने होंगे। यदि डिवाइस वायरलेस संचार का समर्थन नहीं करता है, तो विक्रेता को इसके लिए एक घोषणा पत्र प्रदान करना होगा।
		3.3 सत्यापित करें कि क्या डिवाइस के घटकों की सोर्सिंग के लिए विश्वसनीय स्रोतों का उपयोग किया जा रहा है यानी महत्वपूर्ण हार्डवेयर घटकों (एसओसी जैसे सुरक्षा कार्यों से संबंधित) के लिए सामग्रियों के प्रबंधित बिल के माध्यम से विश्वसनीय आपूर्ति श्रृंखला का उपयोग किया जा रहा है।		विक्रेता को महत्वपूर्ण हार्डवेयर घटकों (एसओसी जैसे सुरक्षा कार्यों से संबंधित) के लिए सामग्री का बिल प्रस्तुत करना होगा।
		3.4 आपूर्ति श्रृंखला जोखिम की पहचान,		विक्रेता निम्नलिखित प्रस्तुत करेगा: आपूर्ति श्रृंखला जोखिम की

		मूल्यांकन, प्राथमिकता और शमन आयोजित किया जाएगा। आपूर्ति शृंखला जोखिम/व्यवसाय निरंतरता योजना नीति दस्तावेज़, आपूर्ति शृंखला व्यवधान को संभालने के तरीके को दर्शाने वाली प्लेबुक, घटना के बाद के सारांश दस्तावेज़ प्रस्तुत करने और उन्हें प्रदर्शित करने की आवश्यकता है।		पहचान, मूल्यांकन, प्राथमिकता और शमन दस्तावेज़। आपूर्ति श्रृंखला जोखिम / व्यापार निरंतरता योजना नीति दस्तावेज, प्लेबुक जो दर्शाती है कि आपूर्ति श्रृंखला व्यवधान को कैसे संभालना है, घटना के बाद सारांश दस्तावेजों को प्रस्तुत करना।
		3.5 सत्यापित करें कि डिवाइस में कोई प्रप्राइइटेरी नेटवर्क प्रोटोकॉल का उपयोग नहीं किया जा रहा है। यदि हाँ, तो संपूर्ण कार्यान्वयन विवरण और उसके लिए स्रोत कोड प्रदान किया जाएगा।		डिवाइस में प्रयुक्त नेटवर्क प्रोटोकॉल के लिए दस्तावेज़।
4.	उत्पाद विकास चरण में सुरक्षा अनुरूपता	4.1 नकली शमन और मैलवेयर का पता लगाने में सहायता के लिए पीसीबीए और एसओसी स्तर तक डिजाइन और आर्किटेक्चर विवरण प्रदान किया जाएगा।		पीसीबीए और एसओसी स्तर तक डिज़ाइन और आर्किटेक्चर दस्तावेज़।
		4.2 उत्पाद विकास के हिस्से के रूप में खराब और नकली उत्पादों के लिए खतरा कम करने की रणनीतियों को लागू किया जाएगा।	प्रक्रिया और विधि के विरूपण साक्ष्य प्रस्तुत करने और उन्हें प्रदर्शित करने की आवश्यकता है।	
		4.3 कोड स्वीकृति और विकास प्रक्रियाओं के हिस्से के रूप में एक या अधिक अद्यतन मैलवेयर पहचान उपकरण नियोजित किए जाएंगे। अंतिम पैकेजिंग और प्रदायगी से पहले मैलवेयर पहचान	उन घटकों की सूची जिनकी पहचान टैनिंग/जालसाजी, सीएम टूल के ट्रैकिंग लक्ष्यों की आवश्यकता के रूप में की गई है। गुणवत्ता आश्वासन प्रक्रिया को प्रस्तुत करने और उसे प्रदर्शित करने की आवश्यकता है।	

		तकनीकों का उपयोग किया जाएगा (उदाहरण के लिए, एक या अधिक अद्यतन मैलवेयर पहचान उपकरणों का उपयोग करके मैलवेयर के लिए तैयार उत्पादों और घटकों को स्कैन करना)।		
		4.4 आपूर्ति श्रृंखला जोखिम की पहचान, मूल्यांकन, प्राथमिकता और शमन आयोजित किया जाएगा।		आपूर्ति श्रृंखला जोखिम / व्यापार निरंतरता योजना नीति दस्तावेज, प्लेबुक जो दर्शाती है कि आपूर्ति श्रृंखला व्यवधान को कैसे संभालना है, घटना के बाद सारांश दस्तावेजों को प्रस्तुत करने और उसी को प्रदर्शित करने की आवश्यकता है।

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

(IPHW Division)

ORDER

New Delhi, the 9th April, 2024

Subject: Amendment to the "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021"

S.O. 1652(E).—In exercise of the powers conferred by sub-section (1) and (2) of section 16 read with sub section (3) of section 25 of the Bureau of Indian Standards Act, 2016, (11 of 2016), the Central Government is of the opinion that it is necessary or expedient so to do in the public interest, hereby makes the following amendments to the "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021":

2. For CCTV Camera, the following entry of Column (5) be added at S. No. 41 in the Schedule of the "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021.

Sr. No. (1)	Goods or Articles (2)	Indian Standard (3)	Title of Indian Standard (4)	Essential Requirement(s) (5)
41	CCTV Camera	IS 13252: Part 1: 2010	Information Technology Equipment - Safety General Requirements--	Essential Requirement(s) for CCTV as per Annexure

3. The provisions of "Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021" shall apply on the Goods or articles as specified in the column (2) added to the schedule of the said Order by virtue of this notification, for conforming to the corresponding Essential Requirement(s) as specified in the column (5), on the expiry of six months from the date of publication of this notification in the Official Gazette. As per Scheme II of BIS Conformity Assessment Regulations, 2018, submission of test reports from BIS recognized labs, shall form a pre -requisite for obtaining license to use Standard Mark.

[F.No. W-43/11/2021-IPHW]

ASHA NANGIA, Group Coordinator & Scientist 'G'

Annexure

Essential Requirement(s) for Security of CCTV

Securing a CCTV (Closed-Circuit Television) system is crucial to protect sensitive information and ensure the system operates effectively. Key areas of testing include exposed network services, device communication protocols, physical access to the device's UART, JTAG, SWD, etc., the ability to extract memory and firmware, firmware update process security and storage and encryption of data. Here are brief requirements for the security of a CCTV system:

1. Physical Security - Use tamper-resistant camera enclosures and locking mechanisms to deter physical tampering.
2. Access Control by Authentication, Role-Based Access Control (RBAC) and regularly review and update access permissions to reflect personnel changes.
3. Network Security by employing encryption of data transmission
4. Software Security by Regular Updates, Disable Unused Features and Strong Password Policies
5. Penetration Testing: Employ penetration testing to assess the system's resistance to cyberattacks and address vulnerabilities.

Essential Security Requirements

Sr. No.	Category	Testing Parameter	What to be tested	Documents Required
1.	Hardware Level Security Parameter (supported by software)	1.1 Verify that application layer debugging interfaces such USB, UART, and other serial variants are disabled or protected by a complex password.	1. Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being used in the device under test 2. Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation 3. Testing, in presence of OEM team, to verify the enabling/disabling of all the ports and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware-based debuggers and access control mechanisms in case the interface is enabled. 4. Process verification of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning. [For instance, through Block connection diagram depicting pin connections between the host	The vendor shall provide the following: a. Datasheet of the SoC being used in the device. b. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. c. Process flow of the Manufacturing/Provisioning of the device

			microcontroller and its interactions with various sub components/peripherals.]	
		1.2 Verify that cryptographic keys and certificates are unique to each individual device.	Identifying all the keys and certificates being used in the device eco-system and verification through: • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process	Vendor shall submit the following: 1. List of all keys and certificates being used in the device ecosystem 2. Key management life cycle (purpose, generation, storage, destruction/zeroization, validity, key changeover/rotation)
		1.3 Verify that on-chip debugging interfaces such as JTAG or SWD are disabled or that available protection mechanism is enabled and configured appropriately.	1. Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being used in the device under test 2. Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation 3. Testing, in presence of OEM team, to verify the enabling/disabling of all the ports and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware based debuggers and access control mechanisms in case the interface is enabled. 4. Process audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning. [For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/peripherals.]	The vendor shall provide the following: a. Datasheet of the SoC being used in the device. b. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. c. Process flow of the Manufacturing/Provisioning of the device

		1.4 Verify that trusted execution is implemented and enabled, if available on the device SoC or CPU.	Identifying whether TEE/SE/TPM is available or not in the device through the SoC datasheet and technical documentation submitted by the vendor. Further assessment is done on the basis of scenarios as applicable to device as defined below: **CASE 1: TEE/SE/TPM is not available:** No further assessment **CASE 2: TEE/SE/TPM is available and enabled:** Verification through code-review that crypto functions are called through TEE/SE/TPM APIs. **CASE 3: TEE/SE/TPM is available but not enabled by the vendor:** Termed as non-conformance to the requirement. OEM is required to enable and implement the TEE/SE/TPM.	The vendor shall provide the following: 1. Datasheet of the SoC being used in the device. 2. User manual/ Technical specifications of the device 3. Code snippets of the TEE API call, wherever applicable
		1.5 Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM, TEE (Trusted Execution Environment), or protected using strong cryptography.	Identifying all the keys and certificates being used in the device eco-system, sensitive data and their storage mechanism(s); and verification through: • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process	Vendor shall submit the following: 1. List of all keys and certificates being used in the device ecosystem 2. List of all the sensitive data with their intended usage and secure storage mechanism(s) as implemented along with secure configurations to be enabled in the device. 3. Key management life cycle (purpose, generation, storage, destruction/zeroization, validity, key changeover/rotation) private keys and certificates.
		1.6Verify the presence of tamper resistance and/or tamper detection features.	Testing, in presence of OEM team, to verify the measures implemented in the device to prevent software and hardware tampering.	Vendor shall submit the following: 1. Measures available in the device to prevent software tampering. 2. Measures available in the device to prevent hardware tampering.
		1.7 Verify that any available Intellectual	Testing, in presence of OEM team, to verify the enabling of the	Vendor shall submit the following: 1. Datasheet of the SoC

		Property protection technologies provided by the chip manufacturer are enabled.	Intellectual Property protection technologies provided by the chip manufacturer, if available.	2. Documentation regarding the Intellectual Property protection technologies provided by the chip manufacturer which have been enabled. 3. In case, no Intellectual Property protection technologies are being provided by the chip manufacturer, then a declaration stating the same.
		1.8 Verify the device validates the boot image signature before loading.	Testing, in presence of OEM team, to verify the following: 1. Device boots up successfully with the documented secure boot process when a valid boot image is provided. 2. Device does not boot up when a tampered boot image (like with missing signature, invalid signature) is provided.	Vendor shall submit the following: 1. Datasheet of the SoC 2. Technical specifications of the device regarding secure boot (should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.)
		1.9 Verify usage of cryptographically secure pseudo-random number generator on embedded device (e.g., using chip-provided random number generators).	Verification of the documentation provided by the vendor regarding the random number generators being used in the device. Verification through code-review that random number generators or related libraries as applicable are being used in the device.	Vendor shall submit the documentation regarding the random generators (either hardware based or software based or both) being used in the device with their intended usage. In case, hardware based random number generators are being used, vendors shall submit the following: 1. Datasheet of the SoC 2. Technical specifications of the device regarding random generators In case, software based random number generators are being used, vendors shall provide the libraries being used for the same.
2.	Software/Firmware	2.1 Verify that memory protection controls such as ASLR and DEP are enabled by the embedded/IoT operating system, if applicable.	Testing, in presence of OEM team, to verify the declared memory protection controls available and enabled in the device using command line-based tools/commands or any other open-source tool like DEP, EMET tool.	Vendor shall submit the declaration of the memory protection controls available and enabled in the device.
		2.2 Verify that the firmware apps protect data-in-transit using transport layer	1. Verifying that strong encryption algorithms and secure TLS version is supported by the device to establish secure	The vendor shall submit the specifications and documentation related to the configurations available in the applications and

		security.	communication. 2. Verifying that device properly validates the server's TLS certificate to ensure that it is trusted and has not been tampered with. 3. Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites. 4. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval. 5. Verifying that theTLS session(s) are resistant to attemptsof interception and decryption of network traffic using man-in-the-middle attacks using tools like Burpsuite.	firmware related to transport layer security.
		2.3 Verify that the firmware apps validate the digital signature of server connections.	1. Identifying the scenarios when the device establishes the server connections with the external world and verifying the following: • Security features, related to secure server connections and digital signature validation as implemented like strong cipher suites, secure TLS version, SSL pinning etc. supported by code walkthrough. • Proper certificate validation, certificate chain validation and certificate revocation checks are implemented in the device. 2. Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites.	Vendor shall submit a document mentioning the use-cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the server connections.

			3. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval. 4. Verifying that TLS session(s) are resistant to attemptsof interception and decryption of network traffic using man-in-the-middle attacks using tools like Burpsuite.	
		2.4 Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.	Secure code review [both automated and manual], in presence of OEM team, using a licensed static analysis tool through any of the following approaches: 1. Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended] 2. Visit to the evaluation agency by the vendor with the firmware code and any licensed static analysis tool available with them and demonstrating the code review activity in the presence of representatives of evaluation agency. 3. Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them. 4. Giving a remote access of the systems at vendor site to the evaluation agency containing the firmware code along with the licensed static analysis tool available with the vendors.	Vendor shall provide : 1. Firmware binaries for code review. 2. Internal code review reports
		2.5 Verify that each firmware maintains a software bill of materials cataloging third party	Verification of the submitted list of third-party components by running automated tools like FACT on the firmware. Identifying vulnerabilities	Vendor shall submit the following: 1. Documentation for information on software bill of materials, including third-party components and versions.

		components, versioning, and published vulnerabilities.	in the third-party component(s) through publically available vulnerability databases Verification and validation of the process defined by the vendor for providing regular security updates and patches for the firmware to address any known vulnerabilities in third-party components.	2. Organization process and policies for the following: • Addressing and patching any identified vulnerabilities in third-party components. • Informing the customers about the security issues or vulnerabilities and providing security updates and patches for the same. 3. Configuration management system and related policies for maintaining firmware and third-party binaries, libraries and frameworks along with the patches/fixes issued to the devices.
		2.6 Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).	Independent secure code review [both automated and manual] using a licensed static analysis tool through any of the following approaches: 1. Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended] 2. Visit to the evaluation agency by the vendor with the firmware code and any licensed static analysis tool available with them and demonstrating the code review activity in the presence of representatives of evaluation agency. 3. Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them. 4. Giving a remote access of the systems at vendor site to the evaluation agency containing the firmware code along with the licensed static analysis tool available with the vendors.	Vendor shall provide: 1. Firmware binaries for code review. 2. Internal code review reports

		2.7 Verify that the firmware apps pin the digital signature to a trusted server(s).	1. Identifying the scenarios when the device establishes the server connections with the external world and verifying the following: • Security features, related to secure server connections and digital signature validation as implemented like strong cipher suites, secure TLS version, SSL pinning etc. supported by code walkthrough. • Proper certificate validation, certificate chain validation and certificate revocation checks are implemented in the device.	Vendor shall submit a document mentioning the use-cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the server connections.
		2.7 Verify security controls are in place to hinder firmware reverse engineering (e.g.removal of verbose debugging symbols).	Testing, in presence of OEM team, to verify the security controls as provided by the vendor to hinder firmware reverse engineering.	Vendor shall submit the documentation regarding the security controls in place to hinder firmware reverse engineering.
		2.8 Verify that the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.	Testing, in presence of OEM team, to verify the measures implemented in the device to make it resistant to time-of-check vs.time-of-use attacks.	Vendor shall submit the measures implemented in the device to make it resistant to time-of-check vs. time-of-use attacks.
		2.9 Verify the device uses code signing and validates firmware upgrade files before installing.	Testing, in presence of OEM team, to verify the following: 1. Device gets successfully updated with the documented secure upgrade process when a valid update package is provided. 2. Device does not boot up when a tampered update package (like with missing signature, invalid signature) is provided.	Vendor shall submit the process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.

		2.10 Verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Testing, in presence of OEM team, to verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Vendor shall submit the process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.
		2.11 Verify that firmware can perform automatic firmware updates upon a predefined schedule.	Verification shall be done as per the applicable scenario: **Case 1: Automatic OTA updates are available:** A standard operating procedure for issuing automatic updates/upgrades to the in-field devices is required to be submitted by the vendor which can then be evaluated by the evaluation agency as per C20, C21 and C22 security requirement of OWASP open standard. **Case 2: Automatic OTA updates are not available and vendor provides manual updates:** A standard operating procedure for issuing manual updates/upgrades to the in-field devices is required to be submitted by the vendor which can then be evaluated by the evaluation agency as per C20, C21 and C22 security requirement of OWASP open standard.	Vendor shall provide the following: 1. Modes of updates available i.e. automatic, manual or both. 2. Organizational process and policies regarding the issuing of updates to the devices.
3.	Secure Process Conformance	3.1 Verify that wireless communications are mutually authenticated.	Testing, in presence of OEM team, to verify the process of mutual authentication as laid down in the documentation by the vendor.	Vendors shall provide the documentation regarding the process of mutual authentication as implemented in the device when wireless communications are initiated. In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.
		3.2 Verify that wireless communications are sent over an encrypted	Identifying all the security mechanisms being used in the communication process verification through:	Vendors shall provide the documentation regarding the security measures implemented in the device to prevent tampering of the data

		channel.	• Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process	being sent through wireless mode of communication. In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.
		3.3 Verify that whether trusted sources are being used for sourcing the components of the device i.e. trusted supply chain through a managed Bill of materials for critical hardware components (related to security functions like SoC) is in use.		Vendor shall submit Bill of materials for critical hardware components (related to security functions like SoC).
		3.4 Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted. Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents need to be submitted and demonstrate the same.		Vendor shall submit the following: Supply chain risk identification, assessment, prioritization, and mitigation documents. Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents.
		3.5 Verify the no proprietary network protocols are being used in the device. If yes, then complete implementation details and the source code for the same shall be provided.		Document for Network protocols used in the device.
4.	Security Conformance at	4.1 Design and architecture details till the PCBA and SoC		Design and architecture documents till the PCBA and SoC level.

	product development stage	level to be provided to aid in counterfeit mitigation and malware detection.		
		4.2 Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.	Process and method artifacts need to be submitted and demonstrate the same.	
		4.3 One or more up-to-date malware detection tools shall be deployed as part of the code acceptance and development processes. Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date malware detection tools).	List of components that have been identified as requiring tracking targets of tainting/counterfeiting, CM tool. Quality assurance process need to be submitted and demonstrate the same.	
		4.4 Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.		Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents need to be submitted and demonstrate the same.

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.