



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 आवश्यकताएँ--	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 एक्स्पोज्ड नेटवर्क सेवाएं, डिवाइस संचार प्रोटोकॉल, डिवाइस के यूएआरटी, जेटीएजी, एसडब्ल्यूडी 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 सॉफ्टवेयर 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 (सॉफ्टवेयर द्वारा समर्थित)	1.1 एक जटिल पासवर्ड द्वारा यह सत्यापित करें कि एप्लिकेशन लेयर डिबर्गिंग 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 डिबर्गिंग इंटरफ़ेस 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 डिबर्गर्स और एक्सेस कंट्रोल तंत्र का उपयोग करके सभी पोर्ट और यूएसबी, यूएआरटी और अन्य सीरियल वेरिएंट जैसे डिबर्गिंग इंटरफ़ेस 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

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

	<p>के दौरान बंद/अक्षम हैं।</p> <p>[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।]</p>	
<p>1.4 सत्यापित करें कि विश्वसनीय निष्पादन लागू और सक्षम है, यदि डिवाइस एसओसी या सीपीयू पर उपलब्ध है।</p>	<p>विक्रेता द्वारा प्रस्तुत एसओसी डेटाशीट और तकनीकी दस्तावेज के माध्यम से डिवाइस में टीईई/एसई/टीपीएम उपलब्ध है या नहीं, इसकी पहचान करना।</p> <p>आगे का मूल्यांकन डिवाइस पर लागू परिदृश्यों के आधार पर किया जाता है जैसा कि नीचे परिभाषित किया गया है:</p> <p>स्थिति 1: टीईई/एसई/टीपीएम उपलब्ध नहीं है:</p> <p>कोई और अग्रिम मूल्यांकन नहीं</p> <p>स्थिति 2: टीईई/एसई/टीपीएम उपलब्ध और सक्षम है:</p> <p>कोड-समीक्षा के माध्यम से सत्यापन कि क्रिप्टो फ़ंक्शन को टीईई/एसई/टीपीएम एपीआई के माध्यम से बुलाया जाता है।</p> <p>स्थिति 3: टीईई/एसई/टीपीएम उपलब्ध है लेकिन विक्रेता द्वारा सक्षम नहीं किया गया है:</p> <p>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।</p>	<p>विक्रेता द्वारा निम्नलिखित को उपलब्ध कराना होगा:</p> <ol style="list-style-type: none">1. डिवाइस में उपयोग किए जा रहे एसओसी की डेटाशीट।2. डिवाइस का उपयोगकर्ता मैनुअल/तकनीकी विनिर्देश3. टीईई एपीआई कॉल के कोड स्निपेट, जहां भी लागू हो
<p>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।</p>	<p>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 :</p> <ul style="list-style-type: none">• ओईएम टीम की उपस्थिति में परीक्षण• कोड समीक्षा• कुंजी-जीवन चक्र प्रक्रिया संबंधी प्रक्रिया लेखा परीक्षा	<p>विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा:</p> <ol style="list-style-type: none">1. डिवाइस इकोसिस्टम में उपयोग की जा रही सभी कुंजियों और प्रमाणपत्रों की सूची2. डिवाइस में सक्षम किए जाने वाले सुरक्षित कॉन्फिगरेशन 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।	सॉफ्टवेयर और हार्डवेयर से टैपरिंग 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 टैपरिंग रोकने के लिए डिवाइस संबंधी उपलब्ध उपाय। 2. हार्डवेयर से टैपरिंग 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 दस्तावेजीकरण, 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 दस्तावेजीकृत 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 क्रिप्टोग्राफिक 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 दस्तावेज 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 जनरेटर (या तो हार्डवेयर आधारित या सॉफ्टवेयर आधारित या दोनों) के संबंध में दस्तावेज 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	<p>2.1 सत्यापित करें कि एएसएलआर और डीईपी जैसे मेमोरी सुरक्षा नियंत्रण एम्बेडेड/आईओटी ऑपरेटिंग सिस्टम द्वारा सक्षम हैं, यदि लागू हो।</p> <p>2.2 सत्यापित करें कि फर्मवेयर ऐप्स ट्रांसपोर्ट लेयर सुरक्षा का उपयोग करके ट्रांज़िट में डेटा की सुरक्षा करते हैं।</p>	<p>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।</p> <p>1. यह सत्यापित करना कि सुरक्षित संचार स्थापित करने के लिए सुदृढ़ एन्क्रिप्शन एल्गोरिदम और सुरक्षित टीएलएस संस्करण डिवाइस द्वारा समर्थित है।</p> <p>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।</p> <p>3. सुभेद्धताओं का परीक्षण जो टीएलएस कनेक्शन की सुरक्षा को प्रभावित कर सकता है जैसे पैडिंग ऑरकल हमले, या सुभेद्ध सिफर सुइट्स।</p> <p>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।</p> <p>5. यह सत्यापित करना कि टीएलएस सत्र बर्षसुइट 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।</p>	<p>विक्रेता को डिवाइस में उपलब्ध और सक्षम मेमोरी सुरक्षा नियंत्रणों की घोषणा प्रस्तुत करनी होगी।</p> <p>विक्रेता ट्रांसपोर्ट लेयर सुरक्षा से संबंधित एप्लिकेशन और फर्मवेयर में उपलब्ध कॉन्फ़िगरेशन से संबंधित विनिर्देश और दस्तावेज प्रस्तुत करेगा।</p>
		2.3 सत्यापित करें कि फर्मवेयर 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

		<ul style="list-style-type: none">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। <p>2. सुभेद्धताओं का परीक्षण जो टीएलएस कनेक्शन की सुरक्षा को प्रभावित कर सकता है जैसे पैडिंग ऑरकल हमले, या सुभेद्ध सिफर सुइट्स।</p> <p>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।</p> <p>4. यह सत्यापित करना कि टीएलएस सत्र बर्षसुइट जैसे उपकरणों का उपयोग करके मैन-इन-द-मिडिल हमलों का उपयोग करके नेटवर्क ट्रैफिक के अवरोधन और डिक्रिप्शन के प्रयासों के लिए प्रतिरोधी हैं।</p>	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 मैनुअल 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

	<p>अपने सिस्टम में स्थापित करना। [अनुशंसित]</p> <p>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।</p> <p>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।</p> <p>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।</p>	
<p>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।</p>	<p>फर्मवेयर पर एफ़एसीटी जैसे स्वचालित उपकरण चलाकर तृतीय-पक्ष घटकों की प्रस्तुत सूची का सत्यापन करना।</p> <p>सार्वजनिक रूप से उपलब्ध सुभेद्धता डेटाबेस के माध्यम से तीसरे पक्ष के घटकों में सुभेद्धताओं की पहचान करना</p> <p>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।</p>	<p>विक्रेता द्वारा निम्नलिखित को प्रस्तुत करना होगा:</p> <p>1. तृतीय पक्ष के घटकों और संस्करणों सहित सामग्री के सॉफ्टवेयर बिल की जानकारी के लिए दस्तावेज़ीकरण करना।</p> <p>2. निम्नलिखित के लिए संगठन प्रक्रिया और नीतियां:</p> <ul style="list-style-type: none">• 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। <p>3. उपकरणों के लिए जारी किए गए पैच/फिक्स के साथ फर्मवेयर और तृतीय-पक्ष बाइनरी, लाइब्रेरी और फ्रेमवर्क को बनाए रखने के लिए कॉन्फिगरेशन प्रबंधन प्रणाली और संबंधित नीतियां।</p>
<p>2.6 हार्डकोडेड क्रेडेंशियल्स (बैकडोर) के लिए तृतीय-पक्ष बायनेरिज़, लाइब्रेरीज़,</p>	<p>निम्नलिखित में से किसी भी दृष्टिकोण के माध्यम से लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण का उपयोग करके स्वतंत्र सुरक्षित</p>	<p>विक्रेता द्वारा उपलब्ध करना होगा:</p> <p>1. कोड समीक्षा के लिए फर्मवेयर बायनेरिज़।</p>

		<p>फ्रेमवर्क सहित सभी कोड की समीक्षा की जाती है।</p> <p>कोड समीक्षा [स्वचालित और मैनुअल दोनों]:</p> <ol style="list-style-type: none"> 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 फ़र्मवेयर 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 फ़र्मवेयर कोड वाले मूल्यांकन एजेंसी को विक्रेता साइट पर सिस्टम की दूरस्थ पहुंच प्रदान करना। 	2. आंतरिक कोड समीक्षा रिपोर्ट
	<p>2.7 सत्यापित करें कि फ़र्मवेयर ऐप्स डिजिटल हस्ताक्षर को किसी विश्वसनीय सर्वर पर पिन करते हैं।</p>	<p>1. उन परिदृश्यों की पहचान करना जब डिवाइस बाहरी दुनिया के साथ सर्वर कनेक्शन स्थापित करता है और निम्नलिखित की पुष्टि करता है:</p> <ul style="list-style-type: none"> • 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 	<p>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।</p>

	2.8 (वर्बोज़ डिबर्गिंग 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 फ़र्मवेयर के पुराने संस्करण (एंटी-रोलबैक) में डाउनग्रेड नहीं किया जा सकता है।	यह सत्यापित करने के लिए कि डिवाइस को वैध फ़र्मवेयर 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।

			<p>स्थिति 2: स्वचालित ओटीए अपडेट उपलब्ध नहीं हैं और विक्रेता मैनुअल अपडेट प्रदान करता है:</p> <p>इन-फील्ड डिवाइसों में मैनुअल 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।</p>	
3.	सुरक्षित अनुरूपता प्रक्रिया	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।	<p>संचार प्रक्रिया सत्यापन में उपयोग किए जा रहे सभी सुरक्षा तंत्रों की पहचान करना:</p> <ul style="list-style-type: none"> • 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 दस्तावेज़ 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

		<p>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।</p>		<p>पहचान, मूल्यांकन, प्राथमिकता और शमन दस्तावेज़।</p> <p>आपूर्ति शृंखला जोखिम / व्यापार निरंतरता योजना नीति दस्तावेज़, प्लेबुक जो दर्शाती है कि आपूर्ति शृंखला व्यवधान को कैसे संभालना है, घटना के बाद सारांश दस्तावेज़ों को प्रस्तुत करना।</p>
		<p>3.5 सत्यापित करें कि डिवाइस में कोई प्रप्राइटेरी नेटवर्क प्रोटोकॉल का उपयोग नहीं किया जा रहा है। यदि हाँ, तो संपूर्ण कार्यान्वयन विवरण और उसके लिए स्रोत कोड प्रदान किया जाएगा।</p>		<p>डिवाइस में प्रयुक्त नेटवर्क प्रोटोकॉल के लिए दस्तावेज़।</p>
4.	उत्पाद विकास चरण में सुरक्षा अनुरूपता	<p>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।</p>		<p>पीसीबीए और एसओसी स्तर तक डिजाइन और आर्किटेक्चर दस्तावेज़।</p>
		<p>4.2 उत्पाद विकास के हिस्से के रूप में खराब और नकली उत्पादों के लिए खतरा कम करने की रणनीतियों को लागू किया जाएगा।</p>	<p>प्रक्रिया और विधि के विरूपण साक्ष्य प्रस्तुत करने और उन्हें प्रदर्शित करने की आवश्यकता है।</p>	
		<p>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</p>	<p>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।</p>	

		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 as USB, UART, and other serial variants are disabled or protected by a complex password.	<p>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</p> <p>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</p> <p>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.</p> <p>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</p>	<p>The vendor shall provide the following:</p> <p>a. Datasheet of the SoC being used in the device.</p> <p>b. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same.</p> <p>c. Process flow of the Manufacturing/Provisioning of the device</p>

			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 ecosystem and verification through: <ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	Vendor shall submit the following: <ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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.] 	<p>The vendor shall provide the following:</p> <ol style="list-style-type: none"> 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.	<p>Identifying whether TEE/SE/TPM is available or not in the device through the SoC datasheet and technical documentation submitted by the vendor.</p> <p>Further assessment is done on the basis of scenarios as applicable to device as defined below:</p> <p>CASE 1: TEE/SE/TPM is not available:</p> <p>No further assessment</p> <p>CASE 2: TEE/SE/TPM is available and enabled:</p> <p>Verification through code-review that crypto functions are called through TEE/SE/TPM APIs.</p> <p>CASE 3: TEE/SE/TPM is available but not enabled by the vendor:</p> <p>Termed as non-conformance to the requirement. OEM is required to enable and implement the TEE/SE/TPM.</p>	<p>The vendor shall provide the following:</p> <ol style="list-style-type: none"> 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.	<p>Identifying all the keys and certificates being used in the device eco-system, sensitive data and their storage mechanism(s); and verification through:</p> <ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	<p>Vendor shall submit the following:</p> <ol style="list-style-type: none"> 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.
		1.6 Verify 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.	<p>Vendor shall submit the following:</p> <ol style="list-style-type: none"> 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	<p>Vendor shall submit the following:</p> <ol style="list-style-type: none"> 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.	<p>communication.</p> <p>2. Verifying that device properly validates the server's TLS certificate to ensure that it is trusted and has not been tampered with.</p> <p>3. Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites.</p> <p>4. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval.</p> <p>5. Verifying that the TLS session(s) are resistant to attempts of interception and decryption of network traffic using man-in-the-middle attacks using tools like Burpsuite.</p>	firmware related to transport layer security.
		2.3 Verify that the firmware apps validate the digital signature of server connections.	<p>1. Identifying the scenarios when the device establishes the server connections with the external world and verifying the following:</p> <ul style="list-style-type: none"> • 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. <p>2. Testing for vulnerabilities which can affect the security of TLS connection such as padding oracle attacks, or weak cipher suites.</p>	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.

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

		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.	<p>2. Organization process and policies for the following:</p> <ul style="list-style-type: none"> 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. <p>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.</p>
		2.6 Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).	<p>Independent secure code review [both automated and manual] using a licensed static analysis tool through any of the following approaches:</p> <ol style="list-style-type: none"> 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] 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. Giving a remote access of the systems at vendor site to the evaluation agency for installing their licensed static analysis tool available with them. 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. 	<p>Vendor shall provide:</p> <ol style="list-style-type: none"> Firmware binaries for code review. Internal code review reports

		2.7 Verify that the firmware apps pin the digital signature to a trusted server(s).	<p>1. Identifying the scenarios when the device establishes the server connections with the external world and verifying the following:</p> <ul style="list-style-type: none"> • 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.	<p>Testing, in presence of OEM team, to verify the following:</p> <p>1. Device gets successfully updated with the documented secure upgrade process when a valid update package is provided.</p> <p>2. Device does not boot up when a tampered update package (like with missing signature, invalid signature) is provided.</p>	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.	<p>Verification shall be done as per the applicable scenario:</p> <p>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.</p> <p>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.</p>	<p>Vendor shall provide the following:</p> <ol style="list-style-type: none"> 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.	<p>Vendors shall provide the documentation regarding the process of mutual authentication as implemented in the device when wireless communications are initiated.</p> <p>In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.</p>
		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.	<ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	<p>being sent through wireless mode of communication.</p> <p>In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.</p>
		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.		<p>Vendor shall submit the following:</p> <p>Supply chain risk identification, assessment, prioritization, and mitigation documents.</p> <p>Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents.</p>
		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.