

No. IV-24011/22/2020-Prov-I/270.
Government of India
Ministry of Home Affairs
Police Modernization Division
Prov-III Desk

26, Man Singh Road,
Jaisalmer House, New Delhi
Dated the 26 April, 2024.

Office Memorandum

Subject : Forwarding of MeitY's communications regarding CCTVs.

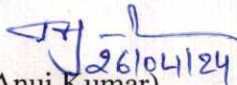
- (i) Notification dated 06 March, 2024 on the amendments to Public Procurement Order (PPO)-2017 for CCTV/Video Surveillance Systems,
(ii) Amendment notification dated 09 April, 2024 to the "Electronics and information Technology Goods (Requirement of Compulsory Registration) Order, 2021
(iii) Advisory dated 11 March, 2024 on the Threat of Information through CCTV/Video Surveillance system."

The undersigned is directed to say that Ministry of Electronics and Information Technology has notified amendment to Public Procurement (Preference to Make in India) Order 2017 for CCTV/Video Surveillance System for Security and furtherance of the order vide Gazette Notification dated 6th March, 2024 (copy enclosed). MeitY has also issued amendment notification dated 09 April, 2024 to the "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021" for the security of a CCTV system (copy enclosed).

2. All Government agencies are advised that henceforth they may procure their CCTVs and allied solutions and hardware on the basis of the Public Procurement Order-2017 and ensure the security of CCTV systems as mentioned in the above said notifications.

3. Further, MeitY has issued Advisory vide O.M. dated W-43/11/2021-IPHW dated 11 Mar, 2024 (copy enclosed) on the Threat of Information through CCTV/Video Surveillance System (VSS)/Digital Video Recorders/Network Video Recorders. All Government agencies are advised to adhere to the guidelines outlined within the ambit of the Public Procurement Orders to safeguard the overall security and integrity of CCTV Cameras and IoT Devices.

Encl:A/a


(Anuj Kumar)

2IC (Prov.)

Tel: 23386034

e-mail ID: anuj-kumar38@nic.in

To:

1. Chief Secretaries of all States.
2. Administrators of all UTs.
3. Commissioner of Police, Delhi.
4. Directors : CBI, IB, SVP NPA-Hyderabad, NEPA-Shillong, NCRB, NICFS.
5. DsG : AR, BSF, BPR&D, CISF, CRPF, ITBP, NDRF, NSG, SSB & NIA

Internal:

1. All Divisional Heads, MHA.
2. SO(IT) with the request to upload the OM on MHA's website.
3. Director (Procurement)/Director (PM-I & II).
4. US (Prov-I)/US(Prov-II).



भारत का राजपत्र The Gazette of India

सी.जी.-डी.एल.-अ.-08032024-252738
CG-DL-E-08032024-252738

असाधारण
EXTRAORDINARY

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

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 1062]

नई दिल्ली, ब्रह्मस्पतिवार, मार्च 7, 2024/फाल्गुन 17, 1945

No. 1062]

NEW DELHI, THURSDAY, MARCH 7, 2024/PHALGUNA 17, 1945

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

(आईपीएचडब्ल्यू प्रभाग)

अधिसूचना

नई दिल्ली, 6 मार्च, 2024

विषय: सार्वजनिक क्रय (मेक इन इंडिया को वरीयता) आदेश 2017 के अनुक्रम में सुरक्षा के लिए क्लोज्ड सर्किट टेलीविजन (सीसीटीवी)/वीडियो निगरानी प्रणाली को अधिसूचित करना

सन्दर्भ:

(i) उद्योग और आंतरिक व्यापार संवर्धन विभाग (डीपीआईआईटी) के दिनांक 28.05.2018, 29.05.2019 और 04.06.2020 के आदेशों के जरिए यथासंशोधित आदेश संख्या पी-45021/2/2017-बीई-II दिनांक 15.06.2017

(ii) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) की दिनांक 07.09.2020 की इलेक्ट्रॉनिक उत्पाद अधिसूचना सं. डब्ल्यू-43/4/2019-आईपीएचडब्ल्यू-एमईआईटीवाई

का.आ. 1119(अ).—सरकार ने 'मेक इन इंडिया' को प्रोत्साहित करने और आय और रोजगार बढ़ाने के उद्देश्य से भारत में वस्तुओं और सेवाओं के विनिर्माण और उत्पादन को बढ़ावा देने के लिए उद्योग और आंतरिक व्यापार संवर्धन विभाग (डीपीआईआईटी) के दिनांक 28.05.2018, 29.05.2019 और 04.06.2020 के आदेशों के जरिए यथासंशोधित आदेश संख्या पी-45021/2/2017-बीई-II दिनांक 15.06.2017 के तहत सार्वजनिक क्रय (मेक इन इंडिया वरीयता) आदेश, 2017 जारी किया है।

2. उपर्युक्त संदर्भ के जरिये अधिसूचित सार्वजनिक क्रय (मेक इन इंडिया को वरीयता) आदेश 2017 [पीपीपी-एमआईआई आदेश 2017] के अनुक्रम में इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमआईआईटीवाई) एतद्वारा अधिसूचित करता है कि समय-समय पर संशोधित पूर्वोक्त आदेश के अनुसार स्थानीय रूप से विनिर्मित इलेक्ट्रॉनिक उत्पादों को सभी क्रय संस्थाओं द्वारा वरीयता प्रदान की जाएगी।

3. इस अधिसूचना के उद्देश्य से :

3.1 श्रेणी- I स्थानीय आपूर्तिकर्ता, श्रेणी-II स्थानीय आपूर्तिकर्ता और गैर-स्थानीय आपूर्तिकर्ता की परिभाषा दिनांक 16.09.2020 के डीपीआईआईटी पीपीपी-एमआईआई आदेश 2017 संख्या समय-समय पर यथा संशोधित पी-45021/2/2017-पीपी(बीई-II) के पैराग्राफ 2 के अनुसार होगी।, इस अधिसूचना में प्रत्येक अधिसूचित इलेक्ट्रॉनिक उत्पाद के लिए स्थानीय सामग्री की गणना के लिए तंत्र निर्धारित किया गया है।

3.2 समय-समय पर यथासंशोधित दिनांक 16.09.2020 के डीपीआईआईटी पीपीपी-एमआईआई आदेश 2017 सं. पी-45021/2/2017-पीपी(बीई-II) के पैराग्राफ 3 क को खरीद के प्रतिशत के लिए संदर्भित किया जाएगा, जिसके लिए घरेलू रूप से निर्मित इलेक्ट्रॉनिक उत्पादों को वरीयता प्रदान की जानी है (मूल्य के संदर्भ में)।

4. वीडियो निगरानी प्रणाली के निम्नलिखित इलेक्ट्रॉनिक उत्पादों को सार्वजनिक खरीद (मेक इन इंडिया को वरीयता) आदेश 2017 के तहत अधिसूचित किया गया है:

4.1 वीडियो निगरानी प्रणाली

परिभाषा:

इस अधिसूचना के प्रयोजन के लिए, वीडियो निगरानी प्रणाली आमतौर पर एक प्रणाली है जिसमें अन्य बातों के साथ-साथ निम्नलिखित शामिल हैं: (i) क्लोज्ड सर्किट टेलीविजन (सीसीटीवी) कैमरा (एनालॉग/आईपी/एनालॉग स्पीड डोम/आईपी स्पीड डोम), (ii) डिजिटल वीडियो रिकॉर्डर (डीवीआर)/नेटवर्क वीडियो रिकॉर्डर (एनवीआर)। सुरक्षा और वीडियो निगरानी प्रणाली के कुछ अनुप्रयोग शहरों, स्कूलों, बैंकों, सरकारी कार्यालयों, सार्वजनिक स्थानों, यातायात निगरानी और गृह सुरक्षा आदि की निगरानी हैं।

4.2 सीसीटीवी कैमरा (एनालॉग) की स्थानीय सामग्री की गणना के लिए तंत्र:

सीसीटीवी कैमरा (एनालॉग) का घरेलू बीओएम निम्नलिखित तालिका के कॉलम 1 में यथा निर्दिष्ट मुख्य इनपुट की लागत का योग होगा, बशर्ते इनपुट व्यक्तिगत रूप से तालिका के कॉलम 2 में निर्दिष्ट मूल्य संवर्धन आवश्यकता को पूरा करते हैं:

क्रम सं.	बीओएम में मुख्य इनपुट / सीसीटीवी कैमरा (एनालॉग) के निर्माण के लिए चरण	इनपुट को घरेलू बीओएम के रूप में वर्गीकृत करने के लिए अपेक्षित मूल्य संवर्धन/स्थानीय सामग्री
	(1)	(2)
1.0	मुख्य पीसीबी*	सेमीकंडक्टर के मूल्य सहित ** और बेयर पीसीबी के मूल्य को छोड़कर घरेलू पीसीबी असेम्बली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से परीक्षण, हालांकि, वैकल्पिक बोर्डों के साथ/इसके बिना मुख्य पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एनालॉग) के कुल बीओएम के 10% से अधिक नहीं होगा
(i)	आई/ओ बोर्ड (वैकल्पिक)	
(ii)	इन्फ्रारेड (आईआर) बोर्ड (वैकल्पिक)	
(iii)	नियंत्रण बोर्ड (वैकल्पिक)	
2.0	बेयर पीसीबी	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। बेयर पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एनालॉग) के कुल बीओएम के 5% से अधिक नहीं होगा
3.0	ऑप्टिक्स	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। बेयर पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एनालॉग) के कुल बीओएम के 10% से अधिक नहीं होगा
4.0	इन-हाउस आर एंड डी #	घरेलू/इन हाउस आर एंड डी में स्वयं अपने संसाधन/विशेषज्ञता का उपयोग कर नये उत्पादों, प्रक्रियाओं, प्रौद्योगिकीयों या समाधानों के विकास के लिए वैज्ञानिक अनुसंधान, प्रयोग, प्रोटोटाइपिंग और परीक्षण अथवा भारत में वैज्ञानिक और औद्योगिक अनुसंधान विभाग (डीएसआईआर) के साथ पंजीकृत आर एंड डी इकाई के साथ कानूनी अनुबंध शामिल है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।

		2023-24 & 2024-25	2025-26	2026-27 के बाद
		7%	10%	12%
5.0	इन-हाउस डिजाइन/आईपीआर #	घरेलू/इन हाउस डिजाइनिंग में संगठन के अपने संसाधन/विशेषज्ञता का प्रयोग कर अपनी फैसिलिटी में ही डिजाइन पद्धतियों सेवाओं या समाधानों की प्रक्रिया अथवा भारत में तृतीय पक्षकार के साथ कानूनी अनुबंध शामिल हैं। भारत में बौद्धिक संपदा अधिकार (आईपीआर) के तहत कोई भी पेटेंट, ट्रेडमार्क, कॉपीराइट और व्यापार रहस्य उनकी रचनाओं या आविष्कारों के डिजाइन के पक्ष में कानूनी स्वामित्व स्थापित करता है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।		
		2023-24 & 2024-25	2025-26	2026-27 के बाद
		7%	10%	12%
6.0	हाउसिंग (प्लास्टिक/एल्यूमीनियम/एमएस) और कैमरा माउंट	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से विनिर्माण। हाउसिंग और कैमरा माउंट के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एनालॉग) के कुल बीओएम के 15% से अधिक नहीं होगा।		
7.0	कनेक्टिंग केबल्स और कनेक्टर्स	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। कनेक्टिंग केबल्स और कनेक्टर्स के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एनालॉग) के कुल बीओएम के 5% से अधिक नहीं होगा।		
8.0	अंतिम असेम्बली और परीक्षण	समय-समय पर अधिसूचित भारतीय मानकों को पूरा करने वाले घरेलू रूप से असेम्बल / परीक्षित. अंतिम संयोजन और परीक्षण के कुल मूल्य का वेटेज सीसीटीवी कैमरे के कुल बीओएम के 10% से अधिक नहीं होगा		

* यह आवश्यक है कि एसएमटी प्रक्रिया का उपयोग करके बेयर पीसीबी पर कलपुर्जों और संघटकों के मुद्रित सर्किट बोर्ड की असेंबली (पीसीबीए) अनिवार्य रूप से भारत में की जानी चाहिए।

** भारत में सेमीकंडक्टर एफएबी के चालू होने पर इसकी समीक्षा की जाएगी।

आवेदक संबंधित वित्तीय वर्ष के लिए नीचे दी गई तालिका में उल्लिखित न्यूनतम मूल्यवर्धन/स्थानीय सामग्री को पूरा करके मूल्य संवर्धन/स्थानीय सामग्री की गणना के लिए संबंधित वित्तीय वर्ष में क्रम संख्या 4.0 (इन-हाउस आर एंड डी) और क्रम संख्या 5.0 (इन-हाउस डिजाइन/आईपीआर) का लाभ उठाने के लिए पात्र होगा।

वित्तीय वर्ष	2023-24 & 2024-25	2025-26	2026-27 के बाद
आवश्यक के रूप में न्यूनतम मूल्य संवर्धन/स्थानीय सामग्री (क्रम सं. 1.0) मुख्य पीसीबी और (क्रम सं.8.0) अंतिम असेंबली और परीक्षण और अन्य वैकल्पिक के रूप में	25%	35%	45%

4.3 सीसीटीवी कैमरा (आईपी) की स्थानीय सामग्री की गणना के लिए तंत्र:

सीसीटीवी कैमरा (आईपी) का घरेलू बीओएम निम्नलिखित तालिका के कॉलम 1 में यथा निर्दिष्ट मुख्य इनपुट की लागत का योग होगा, बशर्ते इनपुट व्यक्तिगत रूप से तालिका के कॉलम 2 में निर्दिष्ट मूल्यवर्धन आवश्यकता को पूरा करते हों:

क्रम सं.	बीओएम में मुख्य इनपुट / सीसीटीवी कैमरा (आईपी) के निर्माण के लिए चरण	इनपुट को घरेलू बीओएम के रूप में वर्गीकृत करने के लिए आवश्यक मूल्य संवर्धन/स्थानीय सामग्री
	(1)	(2)
1.0	मुख्य पीसीबी* कैप्चर और/या प्रोसेसर कार्ड के साथ	सेमीकंडक्टर के मूल्य सहित ** और बेयर पीसीबी के मूल्य को छोड़कर घरेलू पीसीबी असेम्बली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से परीक्षण.

(i)	नेटवर्क इंटरफेस कार्ड (वैकल्पिक)	हालांकि, वैकल्पिक बोर्डों के साथ/इनके बिना मुख्य पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपी) के कुल बीओएम के 10% से अधिक नहीं होगा		
(ii)	इन्फ्रारेड (आईआर) बोर्ड (वैकल्पिक)			
(iii)	आई/ओ बोर्ड (वैकल्पिक)			
(iv)	पावर ओवर इथरनेट (पी ओ ई) कार्ड (वैकल्पिक)			
2.0	बेयर पीसीबी	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। बेयर पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपी) के कुल बीओएम के 5% से अधिक नहीं होगा		
3.0	ऑप्टिक्स	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। प्रकाशिकी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपी) के कुल बीओएम के 10% से अधिक नहीं होगा		
4.0	इन-हाउस आर एंड डी #	घरेलू/इन हाउस आर एंड डी में स्वयं अपने संसाधन/विशेषज्ञता का उपयोग कर नये उत्पादों, प्रक्रियाओं, प्रौद्योगिकियों या समाधानों के विकास के लिए वैज्ञानिक अनुसंधान, प्रयोग, प्रोटोटाइपिंग और परीक्षण अथवा भारत में वैज्ञानिक और औद्योगिक अनुसंधान विभाग (डीएसआईआर) के साथ पंजीकृत आर एंड डी इकाई के साथ कानूनी अनुबंध शामिल है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।		
		2023-24 & 2024-25	2025-26	2026-27 के बाद
		7%	10%	12%
5.0	इन-हाउस डिजाइन/आईपीआर #	घरेलू/इन हाउस डिजाइनिंग में संगठन के अपने संसाधन/विशेषज्ञता का प्रयोग कर अपनी फैसिलिटी में ही डिजाइन पद्धतियों सेवाओं या समाधानों की प्रक्रिया अथवा भारत में तृतीय पक्षकार के साथ कानूनी अनुबंध शामिल हैं। भारत में बौद्धिक संपदा अधिकार (आईपीआर) के तहत कोई भी पेटेंट, ट्रेडमार्क, कॉपीराइट और व्यापार रहस्य उनकी रचनाओं या आविष्कारों के डिजाइन के पक्ष में कानूनी स्वामित्व स्थापित करता है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।		
		2023-24 & 2024-25	2025-26	2026-27 के बाद
		7%	10%	12%
6.0	हाउसिंग (प्लास्टिक / एल्यूमीनियम / एमएस) और	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। हाउसिंग और कैमरा माउंट के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपी) के कुल बीओएम के 15% से अधिक नहीं होगा।		
7.0	कनेक्टिंग केबल्स और कनेक्टर्स	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। कनेक्टिंग केबल्स और कनेक्टर्स के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपी) के कुल बीओएम के 5% से अधिक नहीं होगा।		
8.0	अंतिम असेम्बली और परीक्षण	समय-समय पर यथा अधिसूचित भारतीय मानकों को पूरा करने वाले घरेलू रूप से असेम्बल / परीक्षित .फाइनल असेंबलिंग और टेस्टिंग के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपी) के कुल बीओएम के 10% से अधिक नहीं होगा।		

* यह आवश्यक है कि एसएमटी प्रक्रिया का उपयोग करके बेयर पीसीबी पर कलपुर्जों और संघटकों की मुद्रित सर्किट बोर्ड असेंबली (पीसीबीए) अनिवार्य रूप से भारत में की जानी चाहिए।

** भारत में सेमीकंडक्टर एफएबी के चालू होने पर इसकी समीक्षा की जाएगी।# आवेदक संबंधित वित्तीय वर्ष के लिए नीचे दी गई तालिका में उल्लिखित न्यूनतम मूल्यवर्धन/स्थानीय सामग्री को पूरा करके मूल्य संवर्धन/स्थानीय सामग्री की गणना के लिए संबंधित वित्तीय वर्ष में क्रम संख्या 4.0 (इन-हाउस आर एंड डी) और क्रम संख्या 5.0 (इन-हाउस डिजाइन/आईपीआर) का लाभ उठाने के लिए पात्र होगा।

वित्तीय वर्ष	2023-24 & 2024-25	2025-26	2026-27 के बाद
आवश्यक के रूप में न्यूनतम मूल्य संवर्धन/स्थानीय सामग्री (क्रम सं. 1.0) मुख्य पीसीबी और (क्रम सं.8.0) अंतिम असेंबली और परीक्षण और अन्य वैकल्पिक के रूप में	25%	35%	45%

4.4 सीसीटीवी कैमरा (एनालॉग स्पीड डोम) की स्थानीय सामग्री की गणना के लिए तंत्र:

सीसीटीवी कैमरा (एनालॉग स्पीड डोम) का घरेलू बीओएम निम्नलिखित तालिका के कॉलम 1 में यथा निर्दिष्ट मुख्य इनपुट की लागत का योग होगा, बशर्ते इनपुट व्यक्तिगत रूप से तालिका के कॉलम 2 में निर्दिष्ट मूल्य संवर्धन आवश्यकता को पूरा करते हों:

क्रम सं.	बीओएम में मुख्य इनपुट / सीसीटीवी कैमरा (एनालॉग स्पीड डोम) के निर्माण के लिए चरण	इनपुट को घरेलू बीओएम के रूप में वर्गीकृत करने के लिए आवश्यक मूल्य संवर्धन						
	(1)	(2)						
1.0	मुख्य नियंत्रक बोर्ड*	सेमीकंडक्टर के मूल्य सहित ** और बेयर पीसीबी के मूल्य को छोड़कर घरेलू पीसीबी असेंबली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से परीक्षण. हालांकि, वैकल्पिक बोर्डों के साथ/के बिना मुख्य नियंत्रक बोर्ड/मुख्य पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एएसडी) के कुल बीओएम के 10% से अधिक नहीं होगा						
(i)	आई/ओ बोर्ड (वैकल्पिक)							
(ii)	इन्फ्रारेड (आईआर) बोर्ड (वैकल्पिक)							
2.0	बेयर पीसीबी	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। बेयर पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा						
3.0	इनहाउस आर एंड डी#	घरेलू/इन हाउस आर एंड डी में स्वयं अपने संसाधन/विशेषज्ञता का उपयोग कर नये उत्पादों, प्रक्रियाओं, प्रौद्योगिकियों या समाधानों के विकास के लिए वैज्ञानिक अनुसंधान, प्रयोग, प्रोटोटाइपिंग और परीक्षण अथवा भारत में वैज्ञानिक और औद्योगिक अनुसंधान विभाग (डीएसआईआर) के साथ पंजीकृत आर एंड डी इकाई के साथ कानूनी अनुबंध शामिल है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।						
		<table border="1"> <thead> <tr> <th>2023-24 & 2024-25</th> <th>2025-26</th> <th>2026-27 के बाद</th> </tr> </thead> <tbody> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </tbody> </table>	2023-24 & 2024-25	2025-26	2026-27 के बाद	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 के बाद						
7%	10%	12%						
4.0	इन-हाउस डिजाइन/आईपीआर#	घरेलू/इन हाउस डिजाइनिंग में संगठन के अपने संसाधन/विशेषज्ञता का प्रयोग कर अपनी फैसिलिटी में ही डिजाइन पद्धतियों सेवाओं या समाधानों की प्रक्रिया अथवा भारत में तृतीय पक्षकार के साथ कानूनी अनुबंध शामिल हैं। भारत में बौद्धिक संपदा अधिकार (आईपीआर) के तहत कोई भी पेटेंट, ट्रेडमार्क, कॉपीराइट और व्यापार रहस्य उनकी रचनाओं या आविष्कारों के डिजाइन के पक्ष में कानूनी स्वामित्व स्थापित करता है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।						
		<table border="1"> <thead> <tr> <th>2023-24 & 2024-25</th> <th>2025-26</th> <th>2026-27 के बाद</th> </tr> </thead> <tbody> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </tbody> </table>	2023-24 & 2024-25	2025-26	2026-27 के बाद	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 के बाद						
7%	10%	12%						
5.0	हाउसिंग (प्लास्टिक/एल्यूमीनियम/एमएस) और	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। हाउसिंग और कैमरा माउंट के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एएसडी) के कुल बीओएम के						

	कैमरा माउंट	5% से अधिक नहीं होगा।
6.0	कनेक्टिंग केबल्स और कनेक्टर्स	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। कनेक्टिंग केबल्स और कनेक्टर्स के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा।
7.0	मोटर, हीटर और ब्लोअर, जूम मॉड्यूल, बेल्ट, प्लास्टिक तंत्र भागों, ग्लास आदि	घरेलू रूप से आयातित/घरेलू रूप से निर्मित इनपुट भागों और यांत्रिक घटकों से निर्मित। हालांकि, इन सभी भागों/घटकों के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा।
8.0	पावर एडाप्टर	घरेलू पीसीवी असेम्बली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से अंतिम असेम्बली और परीक्षण, बशर्ते कि "पावर एडाप्टर" की असेम्बली में इस्तेमाल घरेलू रूप से निर्मित कलपुर्जों और संघटकों का मूल्य न्यूनतम 40% होगा ("पावर एडाप्टर" के निर्माण में इस्तेमाल कलपुर्जों और संघटकों के कुल मूल्य का)। हालांकि, "पावर एडाप्टर" के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा।
9.0	अंतिम असेम्बली और परीक्षण	समय-समय पर अधिसूचित भारतीय मानकों को पूरा करने वाले घरेलू रूप से असेम्बल / परीक्षित. अंतिम संयोजन और परीक्षण के कुल मूल्य का वेटेज सीसीटीवी कैमरा (एएसडी) के कुल बीओएम के 10% से अधिक नहीं होगा।

* यह आवश्यक है कि एसएमटी प्रक्रिया का उपयोग करके बेयर पीसीबी पर कलपुर्जों और संघटकों के मुद्रित सर्किट बोर्ड की असेंबली (पीसीबीए) अनिवार्य रूप से भारत में की जानी चाहिए।

** भारत में सेमीकंडक्टर एफएबी के चालू होने पर इसकी समीक्षा की जाएगी।

आवेदक संबंधित वित्तीय वर्ष के लिए नीचे दी गई तालिका में उल्लिखित न्यूनतम मूल्यवर्धन/स्थानीय सामग्री को पूरा करके मूल्य संवर्धन/स्थानीय सामग्री की गणना के लिए संबंधित वित्तीय वर्ष में क्रम संख्या 3.0 (इन-हाउस आर एंड डी) और क्रम संख्या 4.0 (इन-हाउस डिजाइन/आईपीआर) का लाभ उठाने के लिए पात्र होगा।

वित्तीय वर्ष	2023-24 & 2024-25	2025-26	2026-27 के बाद
आवश्यक के रूप में न्यूनतम मूल्य संवर्धन/स्थानीय सामग्री (क्रम सं. 1.0) मुख्य पीसीबी और (क्रम सं.8.0) अंतिम असेंबली और परीक्षण और वैकल्पिक के रूप में अन्य	25%	35%	45%

4.5 सीसीटीवी कैमरा (आईपी स्पीड डोम) की स्थानीय सामग्री की गणना के लिए तंत्र:

सीसीटीवी कैमरा (आईपी स्पीड डोम) का घरेलू बीओएम निम्नलिखित तालिका के कॉलम 1 में निर्दिष्ट मुख्य इनपुट की लागत का योग होगा, बशर्ते इनपुट व्यक्तिगत रूप से तालिका के कॉलम 2 में निर्दिष्ट मूल्यवर्धन आवश्यकता को पूरा करते हों:

क्रम सं.	बीओएम में मुख्य इनपुट / सीसीटीवी कैमरा (आईपी स्पीड डोम) के निर्माण के लिए चरण	इनपुट को घरेलू बीओएम के रूप में वर्गीकृत करने के लिए आवश्यक मूल्य संवर्धन/स्थानीय सामग्री
	(1)	(2)
1.0	मुख्य नियंत्रक बोर्ड*	सेमीकंडक्टर के मूल्य सहित ** और बेयर पीसीबी के मूल्य को छोड़कर घरेलू पीसीबी असेम्बली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से परीक्षण. हालांकि, वैकल्पिक बोर्डों के साथ/के बिना मुख्य नियंत्रक बोर्ड के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपीएसडी) के कुल बीओएम के 10% से अधिक नहीं होगा।
(i)	आई /ओ बोर्ड (वैकल्पिक)	
(ii)	इन्फ्रारेड (आईआर) बोर्ड (वैकल्पिक)	

(iii)	प्रोसेसर कार्ड (वैकल्पिक)							
(iv)	नेटवर्क इंटरफेस कार्ड (वैकल्पिक)							
(v)	पावर ओवर इथरनेट (पी ओ ई) कार्ड (वैकल्पिक)							
2.0	बेयर पीसीबी	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। बेयर पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपीएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा						
3.0	इन-हाउस आर एंड डी #	घरेलू/इन हाउस आर एंड डी में स्वयं अपने संसाधन/विशेषज्ञता का उपयोग कर नये उत्पादों, प्रक्रियाओं, प्रौद्योगिकियों या समाधानों के विकास के लिए वैज्ञानिक अनुसंधान, प्रयोग, प्रोटोटाइपिंग और परीक्षण अथवा भारत में वैज्ञानिक और औद्योगिक अनुसंधान विभाग (डीएसआईआर) के साथ पंजीकृत आर एंड डी इकाई के साथ कानूनी अनुबंध शामिल है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।						
		<table border="1"> <tr> <td>2023-24 & 2024-25</td> <td>2025-26</td> <td>2026-27 के बाद</td> </tr> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </table>	2023-24 & 2024-25	2025-26	2026-27 के बाद	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 के बाद						
7%	10%	12%						
4.0	इन-हाउस डिजाइन/आईपीआर #	घरेलू/इन हाउस डिजाइनिंग में संगठन के अपने संसाधन/विशेषज्ञता का प्रयोग कर अपनी फैसिलिटी में ही डिजाइन पद्धतियों सेवाओं या समाधानों की प्रक्रिया अथवा भारत में तृतीय पक्षकार के साथ कानूनी अनुबंध शामिल हैं। भारत में बौद्धिक संपदा अधिकार (आईपीआर) के तहत कोई भी पेटेंट, ट्रेडमार्क, कॉपीराइट और व्यापार रहस्य उनकी रचनाओं या आविष्कारों के डिजाइन के पक्ष में कानूनी स्वामित्व स्थापित करता है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।						
		<table border="1"> <tr> <td>2023-24 & 2024-25</td> <td>2025-26</td> <td>2026-27 के बाद</td> </tr> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </table>	2023-24 & 2024-25	2025-26	2026-27 के बाद	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 के बाद						
7%	10%	12%						
5.0	हाउसिंग (प्लास्टिक / एल्यूमीनियम / एमएस) और कैमरा माउंट	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। हाउसिंग और कैमरा माउंट के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपीएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा।						
6.0	कनेक्टिंग केबल्स और कनेक्टर्स	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। कनेक्टिंग केबल्स और कनेक्टर्स के लिए इनपुट के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपीएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा।						
7.0	मोटर, हीटर और ब्लोअर, जूम मॉड्यूल, बेल्ट, प्लास्टिक तंत्र भागों, ग्लास आदि	घरेलू रूप से आयातित/घरेलू रूप से निर्मित इनपुट भागों और यांत्रिक घटकों से निर्मित। तथापि, इन सभी भागों/संघटकों के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपीएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा।						
8.0	पावर एडाप्टर	घरेलू पीसीबी असेम्बली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से अंतिम असेम्बली और परीक्षण, बशर्ते कि "पावर एडाप्टर" की असेम्बली में इस्तेमाल घरेलू रूप से निर्मित कलपुर्जों और संघटकों का मूल्य न्यूनतम 40% होगा ("पावर एडाप्टर" के निर्माण में इस्तेमाल कलपुर्जों और संघटकों के कुल मूल्य का). हालांकि, "पावर एडाप्टर" के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपीएसडी) के कुल बीओएम के 5% से अधिक नहीं होगा						
9.0	अंतिम असेम्बली और परीक्षण	समय-समय पर यथाअधिसूचित भारतीय मानकों को पूरा करने वाले घरेलू रूप से असेम्बल /परीक्षित . अंतिम संयोजन और परीक्षण के कुल मूल्य का वेटेज सीसीटीवी कैमरा (आईपीएसडी) के कुल बीओएम के 10% से अधिक नहीं होगा						

* यह आवश्यक है कि एसएमटी प्रक्रिया का उपयोग करके बेयर पीसीबी पर कलपुर्जों और संघटकों के मुद्रित सर्किट बोर्ड की असेंबली (पीसीबीए) अनिवार्य रूप से भारत में की जानी चाहिए।

**भारत में सेमीकंडक्टर एफएबी के चालू होने पर इसकी समीक्षा की जाएगी।

आवेदक संबंधित वित्तीय वर्ष के लिए नीचे दी गई तालिका में उल्लिखित न्यूनतम मूल्यवर्धन/स्थानीय सामग्री को पूरा करके मूल्य संवर्धन/स्थानीय सामग्री की गणना के लिए संबंधित वित्तीय वर्ष में क्रम संख्या 3.0 (इन-हाउस आर एंड डी) और क्रम संख्या 4.0 (इन-हाउस डिजाइन/आईपीआर) का लाभ उठाने के लिए पात्र होगा।

वित्तीय वर्ष	2023-24 & 2024-25	2025-26	2026-27 के बाद
आवश्यक के रूप में न्यूनतम मूल्य संवर्धन/स्थानीय सामग्री (क्रम सं. 1.0) मुख्य पीसीबी और (क्रम सं.9.0) अंतिम असेंबली और परीक्षण और अन्य वैकल्पिक के रूप में	25%	35%	45%

4.6 डीवीआर/एनवीआर की स्थानीय सामग्री की गणना के लिए तंत्र:

डीवीआर/एनवीआर का घरेलू बीओएम निम्नलिखित तालिका के कॉलम 1 में यथा निर्दिष्ट मुख्य इनपुट की लागत का योग होगा, बशर्ते इनपुट व्यक्तिगत रूप से तालिका के कॉलम 2 में निर्दिष्ट मूल्यवर्धन आवश्यकता को पूरा करते हों:

क्रम सं.	बीओएम में मुख्य इनपुट / डीवीआर/एनवीआर के निर्माण के लिए चरण	इनपुट को घरेलू बीओएम के रूप में वर्गीकृत करने के लिए आवश्यक मूल्य संवर्धन/स्थानीय सामग्री						
	(1)	(2)						
1.0	मुख्य पीसीबी*	सेमीकंडक्टर के मूल्य सहित ** और बेयर पीसीबी के मूल्य को छोड़कर घरेलू पीसीबी असेम्बली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से परीक्षण. तथापि, वैकल्पिक बोर्डों के साथ/के बिना मुख्य पीसीबी के कुल मूल्य का वेटेज डीवीआर/एनवीआर के कुल बीओएम के 10 % से अधिक नहीं होगा.						
(i)	फ्रंट पैनल और एलईडी बोर्ड (वैकल्पिक)							
(ii)	आई/ओ बोर्ड (वैकल्पिक)							
2.0	बेयर पीसीबी	घरेलू रूप से विनिर्मित इनपुट से घरेलू रूप से निर्मित। बेयर पीसीबी के कुल मूल्य का वेटेज सीसीटीवी कैमरा (डीवीआर / एनवीआर) के कुल बीओएम के 5% से अधिक नहीं होगा.						
3.0	इन-हाउस आर एंड डी #	घरेलू/इन हाउस आर एंड डी में स्वयं अपने संसाधन/विशेषज्ञता का उपयोग कर नये उत्पादों, प्रक्रियाओं, प्रौद्योगिकियों या समाधानों के विकास के लिए वैज्ञानिक अनुसंधान, प्रयोग, प्रोटोटाइपिंग और परीक्षण अथवा भारत में वैज्ञानिक और औद्योगिक अनुसंधान विभाग (डीएसआईआर) के साथ पंजीकृत आर एंड डी इकाई के साथ कानूनी अनुबंध शामिल है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।						
		<table border="1"> <thead> <tr> <th>2023-24 & 2024-25</th> <th>2025-26</th> <th>2026-27 के बाद</th> </tr> </thead> <tbody> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </tbody> </table>	2023-24 & 2024-25	2025-26	2026-27 के बाद	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 के बाद						
7%	10%	12%						
4.0	इन-हाउस डिजाइन/आईपीआर #	घरेलू/इन हाउस डिजाइनिंग में संगठन के अपने संसाधन/विशेषज्ञता का प्रयोग कर अपनी फैसिलिटी में ही डिजाइन पद्धतियों सेवाओं या समाधानों की प्रक्रिया अथवा भारत में तृतीय पक्षकार के साथ कानूनी अनुबंध शामिल हैं। भारत में बौद्धिक संपदा अधिकार (आईपीआर) के तहत कोई भी पेटेंट, ट्रेडमार्क, कॉपीराइट और व्यापार रहस्य उनकी रचनाओं या आविष्कारों के डिजाइन के पक्ष में कानूनी स्वामित्व स्थापित करता है। इसके वेटेज की गणना संबंधित वित्तीय वर्ष में घरेलू बीओएम के प्रतिशत के आधार पर की जाएगी जैसा कि नीचे दी गई तालिका में उल्लिखित है।						
		<table border="1"> <thead> <tr> <th>2023-24 & 2024-25</th> <th>2025-26</th> <th>2026-27 के बाद</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	2023-24 & 2024-25	2025-26	2026-27 के बाद			
2023-24 & 2024-25	2025-26	2026-27 के बाद						

		7%	10%	12%
5.0	हाउसिंग (प्लास्टिक / एल्यूमीनियम / एमएस) और कैमरा माउंट	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। आवास और कैमरा माउंट के लिए इनपुट के कुल मूल्य का वेटेज डीवीआर/एनवीआर के कुल बीओएम के 5% से अधिक नहीं होगा।		
6.0	कनेक्टिंग केबल, कनेक्टर्स और यूएसबी माउस	घरेलू रूप से निर्मित इनपुट से घरेलू रूप से निर्मित। कनेक्टिंग केबल, कनेक्टर्स और यूएसबी माउस के लिए इनपुट के कुल मूल्य का वेटेज डीवीआर/एनवीआर के कुल बीओएम के 5% से अधिक नहीं होगा।		
7.0	रिमोट कंट्रोल	घरेलू असेंबली * और आयातित/घरेलू रूप से निर्मित कलपुर्जों और संघटकों से परीक्षण इस शर्त के अधीन है कि "रिमोट कंट्रोल" की असेंबली में उपयोग किए जाने वाले घरेलू रूप से निर्मित कलपुर्जों और संघटकों का मूल्य वर्ष 2 में न्यूनतम 20% होगा ("रिमोट कंट्रोल" के निर्माण में उपयोग किए जाने वाले कलपुर्जों और संघटकों के कुल मूल्य का), जो वित्तीय वर्ष 2025-26, 2026-27 और 2027-28 से आगे क्रमशः न्यूनतम 30%, 40% और 50% तक बढ़ जाएगा।		
8.0	पावर एडाप्टर	घरेलू पीसीबी असेम्बली * और आयातित / घरेलू रूप से निर्मित कलपुर्जों और संघटकों से अंतिम असेम्बली और परीक्षण, बशर्ते कि "पावर एडाप्टर" की असेम्बली में इस्तेमाल घरेलू रूप से निर्मित कलपुर्जों और संघटकों का मूल्य न्यूनतम 40% होगा ("पावर एडाप्टर" के निर्माण में इस्तेमाल कलपुर्जों और संघटकों के कुल मूल्य का). हालांकि, "पावर एडाप्टर" के कुल मूल्य का वेटेज डीवीआर/एनवीआर के कुल बीओएम के 5% से अधिक नहीं होगा।		
9.0	अंतिम असेम्बली और परीक्षण	समय-समय पर अधिसूचित वेटेज भारतीय मानकों को पूरा करने वाले घरेलू रूप से असेम्बल / परीक्षित. अंतिम संयोजन और परीक्षण के कुल मूल्य का वेटेज डीवीआर/एनवीआर के कुल बीओएम के 10% से अधिक नहीं होगा।		

* यह आवश्यक है कि एसएमटी प्रक्रिया का उपयोग करके बेयर पीसीबी पर कलपुर्जों और संघटकों के मुद्रित सर्किट बोर्ड असेंबली (पीसीबीए) अनिवार्य रूप से भारत में किया जाना चाहिए।

** भारत में सेमीकंडक्टर एफएबी के चालू होने पर इसकी समीक्षा की जाएगी।

आवेदक संबंधित वित्तीय वर्ष के लिए नीचे दी गई तालिका में उल्लिखित न्यूनतम मूल्यवर्धन/स्थानीय सामग्री को पूरा करके मूल्य संवर्धन/स्थानीय सामग्री की गणना के लिए संबंधित वित्तीय वर्ष में क्रम संख्या 3.0 (इन-हाउस आर एंड डी) और क्रम संख्या 4.0 (इन-हाउस डिजाइन/आईपीआर) का लाभ उठाने के लिए पात्र होगा।

वित्तीय वर्ष	2023-24 & 2024-25	2025-26	2026-27 के बाद
आवश्यक के रूप में न्यूनतम मूल्य संवर्धन/स्थानीय सामग्री (क्रम सं. 1.0) मुख्य पीसीबी और (क्रम सं.9.0) अंतिम असेंबली और परीक्षण और अन्य वैकल्पिक के रूप में	25%	35%	45%

5. निगरानी उपकरणों यानी सीसीटीवी कैमरों (एनालॉग/आईपी/एनालॉग स्पीड डोम/आईपी स्पीड डोम/आईपी स्पीड डोम) को समय-समय पर यथा संशोधित परिशिष्ट 'क' के अनुसार वीएसएस/सीसीटीवी सिस्टम की सुरक्षा सुनिश्चित करने के लिए एमईआईटीवाई द्वारा निर्धारित सुरक्षा के लिए आवश्यक आवश्यकताओं (ईआर) का अनुपालन करना चाहिए। सीसीटीवी/वीएसएस के लिए सुरक्षा परीक्षण प्रतिवेदन मानकीकरण परीक्षण और गुणवत्ता प्रमाणन (एसटीक्यूसी) प्रयोगशाला या एमईआईटीवाई द्वारा समय-समय पर अधिसूचित किसी अन्य एजेंसी द्वारा जारी किया जाएगा। एसटीक्यूसी लैब द्वारा जारी परीक्षण रिपोर्ट की वैधता रिपोर्ट के जारी होने की तारीख से तीन वर्ष होगी। सीसीटीवी कैमरों/वीएसएस प्रणाली की सुरक्षा के लिए इन अनिवार्य आवश्यकताओं (ईआर) को इस अधिसूचना के जारी होने की तारीख से 3 महीने के बाद लागू किया जाएगा। डीवीआर और एनवीआर के लिए सुरक्षा मानदंडों को बाद में अधिसूचित किया जाएगा।

6. अधिसूचना इस अधिसूचना के जारी होने की तारीख से 3 महीने के बाद प्रभावी होगी। यह अधिसूचना संशोधित अधिसूचना जारी होने तक वैध रहेगी। इस अधिसूचना के प्रयोजन के लिए 1 वर्ष 31.03.2025 तक होगा।

7. सार्वजनिक खरीद (मेक इन इंडिया को वरीयता) आदेश 2017 के तहत किसी भी इलेक्ट्रॉनिक उत्पाद अधिसूचना का पूर्वव्यापी प्रभाव नहीं होगा।

8. पूर्वोक्त इलेक्ट्रॉनिक्स उत्पादों की खरीद के लिए समय-समय पर यथा संशोधित दिनांक 16.09.2020 के सार्वजनिक खरीद (मेक इन इंडिया को वरीयता) आदेश 2017 में उद्धृत प्रावधानों के अनुसार खरीद वरीयता प्रदान की जाएगी।

9. यदि भारत सरकार द्वारा परियोजना या योजना पूरी तरह से या आंशिक रूप से वित्त पोषित होती है, तो राज्यों और स्थानीय निकायों द्वारा बनाए गए इलेक्ट्रॉनिक उत्पादों की क्रय के लिए अधिसूचना सभी केंद्रीय योजनाओं (सीएस)/केंद्रीय क्षेत्र की योजनाओं (सीएसएस) पर भी लागू होगी।

10. स्थानीय सामग्री/घरेलू मूल्यवर्धन की गणना करने हेतु प्रक्रिया

10.1 घरेलू विनिर्माताओं (डीओएम-बीओएम) से प्राप्त सामग्री के बिल की गणना उपलब्ध आंकड़ों के आधार पर निम्नलिखित में से किसी एक के आधार पर की जा सकती है।

क. सभी इनपुटों की लागतों का योग जो उस उत्पाद को बनाने के लिए आवश्यक है (इनपुटों की क्रय पर लगाए गए शुल्क और करों सहित, सिवाय उनको छोड़कर जिनके लिए क्रेडिट/सेट-ऑफ का लाभ लिया जा सकता है) और जिनका आयात प्रत्यक्ष रूप से या घरेलू व्यापारी या माध्यस्थ के माध्यम से नहीं किया गया है।

ख. उत्पाद के फैक्ट्री बाह्य मूल्य से उत्पाद के उत्पादन में इनपुटों के रूप में उपयोग की गई सामग्री के आयातित बिल (प्रत्यक्ष या अप्रत्यक्ष रूप से) को घटाकर (इनपुटों की क्रय पर लगाए गए शुल्क और करों सहित, सिवाय उनको छोड़कर जिनके लिए क्रेडिट/सेट-ऑफ का लाभ लिया जा सकता है) और उसमें से वारंटी लागत को घटाकर।

ग. बाजार मूल्य से उत्पादन पश्चात मालभाडा, बीमा और अन्य हथालन लागतों को घटाकर, उसमें से कर पश्चात लाभ, वारंटी लागत को घटाया जाता है, उसमें से उत्पादों के उत्पादन (इनपुटों की क्रय पर लगाए गए शुल्क और करों सहित, सिवाय उनको छोड़कर जिनके लिए क्रेडिट/सेट-ऑफ लिया जा सकता है) में इनपुटों के रूप में उपयोग की गई सामग्री के आयातित बिल के योग को घटाया जाता है और बिक्री और विपणन खर्च को घटाया जाता है।

10.2 सामग्री के कुल बिल (कुल-बीओएम) की गणना उपलब्ध आंकड़ों पर आधारित निम्नलिखित में से किसी एक के आधार पर की जा सकती है।

क. सभी इनपुटों की लागतों का योग जो उस उत्पाद को बनाने के लिए आवश्यक है (इनपुटों की क्रय पर लगाए गए शुल्क और करों सहित, सिवाय उनको छोड़कर जिनके लिए क्रेडिट/सेट-ऑफ का लाभ लिया जा सकता है)।

ख. उत्पाद के फैक्ट्री बाह्य मूल्य से कर पश्चात लाभ और वारंटी लागतों को घटाया जाता है।

ग. बाजार मूल्य से उत्पादन पश्चात मालभाडा, बीमा और अन्य हथालन लागतों को घटाकर उसमें से कर पश्चात लाभ, वारंटी लागत, बिक्री और विपणन खर्च घटाया जाता है।

10.3 निम्नलिखित फॉर्मूला के अनुसार प्रस्तुत जानकारी के आधार पर घरेलू मूल्य-वृद्धि के प्रतिशत की गणना की जा सकती है:

$$\text{स्थानीय सामग्री/घरेलू मूल्य-वृद्धि का प्रतिशत} = \frac{\text{डीओएम-बीओएम}}{\text{कुल-बीओएम}} \times 100$$

11. स्थानीय सामग्री/घरेलू मूल्यवृद्धि का सत्यापन

11.1. निविदा, बोली प्रक्रिया या सिफ़ारिश के समय स्थानीय आपूर्तिकर्ता स्व-प्रमाणन प्रदान करेगा कि प्रस्तावित की गई वस्तुएं न्यूनतम स्थानीय सामग्री की आवश्यकताओं को पूरा करती हैं और उस स्थान (स्थानों) का विवरण देगा, जिस पर स्थानीय मूल्य वृद्धि की गई है।

11.2. 10 करोड़ रुपए से अधिक मूल्य की क्रय के मामलों में, स्थानीय आपूर्तिकर्ता स्थानीय सामग्री का प्रतिशत देते हुए कंपनी के सांविधिक लेखा परीक्षक (कंपनियों के मामले में) या लागत लेखापरीक्षक या किसी पेशेवर लागत लेखाकार या पेशेवर चार्टर्ड लेखाकार (कंपनियों के अलावा अन्य आपूर्तिकर्ताओं के संबंध में) से एक प्रमाणपत्र उपलब्ध कराएगा।

- 11.3.** यदि किसी इलेक्ट्रॉनिक उत्पाद के संबंध में स्थानीय सामग्री/घरेलू मूल्य वृद्धि के संबंध में बोलीकर्ता के दावे के खिलाफ क्रय एजेंसी या संबंधित मंत्रालय/विभाग द्वारा शिकायत प्राप्त की जाती है, तो उसे एसटीक्यूसी के पास भेजा जाएगा।
- 11.4.** एसटीक्यूसी को संदर्भित कोई भी शिकायत 4 सप्ताह के भीतर निपटा दी जाएगी। बोलीकर्ता को एसटीक्यूसी हेतु किसी इलेक्ट्रॉनिक उत्पाद में दावा की गई घरेलू मूल्य वृद्धि के समर्थन में आवश्यक दस्तावेज प्रस्तुत करने की आवश्यकता होगी। यदि बोलीकर्ता के द्वारा कोई जानकारी प्रस्तुत नहीं की जाती है, तो ऐसी प्रयोगशालाएं दावे के वास्तविकता को सिद्ध करने के लिए अगली आवश्यक कार्रवाई कर सकती हैं। **स्थानीय सामग्री की गणना में विसंगतियों के मामले में, स्थानीय सामग्री के प्रतिशत की गणना के लिए कंपनी के सांविधिक लेखा परीक्षक या लागत लेखा परीक्षक (कंपनियों के मामले में) या प्रैक्टिसिंग कौन्सिल एकाउंटेंट या प्रैक्टिसिंग चार्टर्ड एकाउंटेंट (कंपनियों के अलावा अन्य आपूर्तिकर्ताओं के संबंध में) से एक प्रमाण पत्र स्व-घोषणा प्रमाण पत्र पर अधिकृत होगा।**
- 11.5.** 2 लाख रुपए या खरीदे जा रहे घरेलू रूप से विनिर्मात इलेक्ट्रॉनिक उत्पादों की कीमत का 1% शिकायत शुल्क (5 लाख रुपए की अधिकतम सीमा के अध्यक्षीन), जो भी अधिक हो, का डिमांड ड्राफ्ट द्वारा भुगतान किया जाएगा, जो एसटीक्यूसी में जमा जमा होगा। यदि शिकायत गलत पाई जाती है, तो शिकायत शुल्क जब्त कर लिया जाएगा। यदि, शिकायत को बरकरार रखा जाता है और काफी हद तक सही पाया जाता है तो शिकायतकर्ता को जमा शुल्क बिना किसी ब्याज के वापस कर दिया जाएगा।
- 11.6.** सामान्य वित्तीय नियम (जीएफआर) के नियम 175(1)(i)(एच) के तहत झूठी घोषणाएं सत्यनिष्ठा संहिता का उल्लंघन होंगी, जिसके लिए बोली लगाने वाले या उसके उत्तराधिकारियों को नियम 151 (iii) के अनुसार प्रतिबंधित किया जा सकता है। सामान्य वित्तीय नियमों के साथ-साथ बोली लगाने के ऐसे अन्य प्रावधान, एकल मंत्रालय/विभाग द्वारा रोक लगाना और व्यय विभाग के कार्यालय ज्ञापन संख्या एफ.1/20/2018-पीपीडी दिनांक 2 नवंबर, 2021 के अनुसार आदेशों को रद्द करना समय-समय पर संशोधित कानून के तहत अनुमन्य हो सकता है।
- 12.** इलेक्ट्रॉनिक्स उत्पाद अधिसूचनाओं के कार्यान्वयन की निगरानी के लिए एमईआईटीवाई नोडल मंत्रालय होगा। एसटीक्यूसी द्वारा दिए गए निर्णय के विरुद्ध किसी विवाद/स्पष्टीकरण के मामले में, शिकायतों के सत्यापन/पुनरीक्षण, यादृच्छिक आधार पर स्व-घोषणाओं और लेखा परीक्षक/लेखाकार के प्रमाणपत्रों के स्वतंत्र सत्यापन, इलेक्ट्रॉनिकी उत्पादों के घरेलू विनिर्माताओं के विरुद्ध प्रतिबंधात्मक और भेदभावपूर्ण निबंधन और शर्तों के लिए निम्नलिखित घटकों वाली एक समिति गठित की जाती है: -
- | | | |
|------|--|-------------|
| i) | समूह समन्वयक/वैज्ञानिक- 'जी' (आईपीएचडब्ल्यू) | - अध्यक्ष |
| ii) | एसटीक्यूसी से वैज्ञानिक-'जी'/वैज्ञानिक-'एफ' | - सदस्य |
| iii) | वैज्ञानिक- 'ई'/सर्ट-इन/साइबर डिवीजन अथवा वरिष्ठ. | - सदस्य |
| vi) | अध्यक्ष द्वारा सहयोजित कोई अन्य सदस्य (सदस्यों) | -सदस्य |
| v) | आईपीएचडब्ल्यू प्रभाग से वैज्ञानिक-'ई'/प्रतिनिधि | -सदस्य सचिव |

13. यदि प्रश्न उठता है कि क्या खरीदी जा रही कोई वस्तु एक इलेक्ट्रॉनिक उत्पाद है, जिसे सार्वजनिक क्रय (मेक इन इंडिया को वरीयता) आदेश 2017 के तहत शामिल किया जाना है, तो इस मामले को स्पष्टीकरण के लिए इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय को संदर्भित किया जाएगा।

[फ़ा. सं. डब्ल्यू-43/11/2021-आईपीएचडब्ल्यू]

आशा नांगिया, समूह समन्वयक और वैज्ञानिक 'जी'

परिशिष्ट 'क'

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 एक्सपोस्ड 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:

		<p>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 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)।</p>	<p>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>	
		<p>4.4 आपूर्ति शृंखला जोखिम की पहचान, मूल्यांकन, प्राथमिकता और शमन आयोजित किया जाएगा।</p>		<p>आपूर्ति शृंखला जोखिम / व्यापार निरंतरता योजना नीति दस्तावेज, प्लेबुक जो दर्शाती है कि आपूर्ति शृंखला व्यवधान को कैसे संभालना है, घटना के बाद सारांश दस्तावेजों को प्रस्तुत करने और उसी को प्रदर्शित करने की आवश्यकता है।</p>

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

(IPHW DIVISION)

NOTIFICATION

New Delhi, the: 6th March, 2024

Subject: Public Procurement (Preference to Make in India) Order 2017-Notifying CCTV/ Video Surveillance System for Security in furtherance of the Order

Reference:

(i) Department for Promotion of Industry and Internal Trade (DPIIT) Order No. P-45021/2/2017-B.E.-II dated 15.06.2017, as amended by Orders dated 28.05.2018, 29.05.2019, 04.06.2020 and 16.09.2020

(ii) Ministry of Electronics and Information Technology (MeitY) Electronic Products Notification No. W-43/4/2019-IPHW-MeitY dated 07.09.2020

S.O. 1119(E).—The Government has issued Public Procurement (Preference to Make in India) Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P-45021/2/2017-B.E.-II dated 15.06.2017, as amended by Orders dated 28.05.2018, 29.05.2019, 04.06.2020 and 16.09.2020, to encourage 'Make in India' and promote manufacturing and production of goods and services in India with a view to enhancing income and employment.

2. In furtherance of the Public Procurement (Preference to Make in India) Order 2017 [PPP-MII Order 2017] notified vide reference cited above, the Ministry of Electronics and Information Technology (MeitY) hereby notifies

that preference shall be provided by all procuring entities to locally manufactured Video Surveillance System for Security as per the aforesaid Order, as amended from time to time.

3. For the purpose of this notification:

3.1 The definition of Class-I local supplier, Class-II local supplier and Non-local supplier shall be as per paragraph 2 of the DPIIT PPP-MII Order 2017 No. P-45021/2/2017-PP(BE-II) dated 16.09.2020, as amended from time to time. The mechanism for calculation of local content is prescribed for each notified Electronic Product in this notification.

3.2 Paragraph 3A of the DPIIT PPP-MII Order 2017 No. P-45021/2/2017-PP(BE-II) dated 16.09.2020, as amended from time to time, shall be referred for percentage of procurement for which preference to domestically manufactured Electronic Products is to be provided (in value terms).

4. Following electronic products of Video Surveillance System are notified under the Public Procurement (Preference to Make in India) Order 2017:

4.1 Video Surveillance System

Definition:

For the purpose of this Notification, Video Surveillance System is usually a system that *inter-alia* includes: (i) Closed Circuit Television (CCTV) Camera (Analog/ IP/ Analog Speed Dome/ IP Speed Dome), (ii) Digital Video Recorder (DVR) / Network Video Recorder (NVR). Some of the applications of Security and Video Surveillance System are surveillance of Cities, Schools, Banks, Government Offices, public places, traffic monitoring and home security, etc.

4.2 Mechanism for calculation of local content of CCTV Camera (Analog):

The domestic BOM of CCTV Camera (Analog) would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (Analog)	Value addition / local content required for the input to be classified as domestic BOM		
	(1)	(2)		
1.0	Main PCB*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main PCB with/without optional boards shall not exceed 10 % of the total BOM of the CCTV Camera (Analog)		
(i)	I/O Board (optional)			
(ii)	Infrared (IR) Board (optional)			
(iii)	Control Board (optional)			
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BOM of the CCTV Camera (Analog)		
3.0	Optics	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Optics shall not exceed 10 % of the total BOM of the CCTV Camera (Analog)		
4.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:		
		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
5.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property		

		Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:						
		<table border="1"> <tr> <td>2023-24 & 2024-25</td> <td>2025-26</td> <td>2026-27 onwards</td> </tr> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
6.0	Housing (Plastic /Aluminium/MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed to 15 % of the total BOM of the CCTV Camera (Analog).						
7.0	Connecting Cables & Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BOM of the CCTV Camera (Analog).						
8.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10% of the total BOM of the CCTV Camera.						

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 4.0 (In-house R&D) & Sr. No. 5.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1) Main PCB and (Sr. No.8) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.3 Mechanism for calculation of local content of CCTV Camera (IP):

The domestic BOM of CCTV Camera (IP) would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (IP)	Value addition / local content required for the input to be classified as domestic BOM
	1	2
1.0	Main PCB* with Capture and/or Processor Card	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main PCB with/without optional boards shall not exceed 10 % of the total BOM of the CCTV Camera (IP)
(i)	Network Interface Card (optional)	
(ii)	Infrared (IR) Board (optional)	
(iii)	I/O Board (optional)	
(iv)	Power over Ethernet (PoE) Card (optional)	
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BOM of the CCTV Camera (IP)
3.0	Optics	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Optics shall not exceed 10 % of the total BOM of the CCTV Camera (IP)
4.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation,

		prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:						
		<table border="1"> <tr> <td>2023-24 & 2024-25</td> <td>2025-26</td> <td>2026-27 onwards</td> </tr> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
5.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:						
		<table border="1"> <tr> <td>2023-24 & 2024-25</td> <td>2025-26</td> <td>2026-27 onwards</td> </tr> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
6.0	Housing (Plastic / Aluminium / MS) and	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 15 % of the total BOM of the CCTV Camera (IP).						
7.0	Connecting Cables and Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BOM of the CCTV Camera (IP).						
8.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of Final Assembling and Testing shall not exceed 10% of the total BOM of the CCTV Camera (IP)						

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 4.0 (In-house R&D) & Sr. No. 5.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 8.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.4 Mechanism for calculation of local content of CCTV Camera (Analog Speed Dome):

The domestic BOM of CCTV Camera (Analog Speed Dome) would be the sum of the costs of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (Analog Speed Dome)	Value addition required for the input to be classified as domestic BOM
	1	2
1	Main Controller Board*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main Controller Board/Main PCB with/without optional boards shall not exceed 10 % of the total BoM of the CCTV Camera (ASD)
(i)	I/O Board (optional)	
(ii)	Infrared (IR) Board (optional)	
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total

		BoM of the CCTV Camera (ASD)		
3.0	Inhouse R&D#	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.:		
		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
4.0	In-house Design/IPR#	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.:		
		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
5.0	Housing (Plastic/ Aluminium/ MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 5 % of the total BoM of the CCTV Camera (ASD).		
6.0	Connecting Cables and Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BoM of the CCTV Camera (ASD).		
7.0	Motor, Heater & Blower, Zoom Module, Belt, Plastic Mechanism Parts, Glass etc.	Domestically manufactured from imported / domestically manufactured input parts and mechanical components. However, the weightage of the total value of all these parts/components shall not exceed 5% of the total BoM of the CCTV Camera (ASD)		
8.0	Power Adapter	Domestic PCB assembly* and the final assembly and testing from imported / domestically manufactured parts and components, subject to the condition that the value of domestically manufactured parts and components used in the assembly of "Power Adapter" will be minimum 40% (of the total value of parts and components used in the manufacture of "Power Adapter"). However, the weightage of the total value of "Power Adapter" shall not exceed 5% of the total BoM of the CCTV Camera (ASD)		
9.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10 % of the total BoM of the CCTV Camera (ASD)		

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 3.0 (In-house R&D) & Sr. No. 4.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 9.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.5 Mechanism for calculation of local content of CCTV Camera (IP Speed Dome):

The domestic BOM of CCTV Camera (IP Speed Dome) would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr. No.	Main inputs in BOM / stages for manufacture of CCTV Camera (IP Speed Dome)	Value addition / local content required for the input to be classified as domestic BOM						
	1	2						
1.0	Main Controller Board*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main Controller Board with/without optional boards Shall not exceed 10 % of the total BoM of the CCTV Camera (IPSD)						
(i)	I/O Board (optional)							
(ii)	Infrared (IR) Board (optional)							
(iii)	Processor Card (optional)							
(iv)	Network Interface Card (Optional)							
(v)	Power over Ethernet (PoE) Card (optional)							
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BoM of the CCTV Camera (IPSD)						
3.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources /expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>2023-24 & 2024-25</th> <th>2025-26</th> <th>2026-27 onwards</th> </tr> </thead> <tbody> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </tbody> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
4.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BoM in respective Financial Year as mentioned in below table.: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>2023-24 & 2024-25</th> <th>2025-26</th> <th>2026-27 onwards</th> </tr> </thead> <tbody> <tr> <td>7%</td> <td>10%</td> <td>12%</td> </tr> </tbody> </table>	2023-24 & 2024-25	2025-26	2026-27 onwards	7%	10%	12%
2023-24 & 2024-25	2025-26	2026-27 onwards						
7%	10%	12%						
5.0	Housing (Plastic / Aluminium / MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 5 % of the total BoM of the CCTV Camera (IPSD).						
6.0	Connecting Cables and Connectors	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables and Connectors shall not exceed 5% of the total BoM of the CCTV Camera (IPSD).						
7.0	Motor, Heater & Blower, Zoom Module, Belt, Plastic Mechanism Parts, Glass etc.	Domestically manufactured from imported / domestically manufactured input parts and mechanical components. However, the weightage of the total value of all these parts/components shall not exceed 5% of the total BoM of the CCTV Camera (IPSD).						
8.0	Power Adapter	Domestic PCB assembly* and the final assembly and testing from imported / domestically manufactured parts and components, subject to the condition that the value of domestically manufactured parts and components used in the						

		assembly of "Power Adapter" will be minimum 40% (of the total value of parts and components used in the manufacture of "Power Adapter"). However, the weightage of the total value of "Power Adapter" shall not exceed 5% of the total BoM of the CCTV Camera (IPSD)
9.0	Final Assembly and Testing	Domestically assembled / tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10 % of the total BoM of the CCTV Camera (IPSD)

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 3.0 (In-house R&D) & Sr. No. 4.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 9.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

4.6 Mechanism for calculation of local content of DVR/ NVR:

The domestic BOM of DVR/ NVR would be the sum of the cost of main inputs as specified in Column 1 of the following table, provided the inputs individually satisfy the value addition requirement specified in Column 2 of the table:

Sr No.	Main inputs in BOM / stages for manufacture of DVR / NVR	Value addition / local content required for the input to be classified as domestic BOM		
	1	2		
1.0	Main PCB*	Domestic PCB Assembly* and testing from imported / domestically manufactured parts and components, including the value of Semiconductors** and excluding the value of bare PCB. However, the weightage of the total value of Main PCB with/without optional boards shall not exceed 10 % of the total BoM of the DVR/NVR.		
(i)	Front Panel & LED Board (optional)			
(ii)	I/O Board (optional)			
2.0	Bare PCB	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of Bare PCB shall not exceed 5 % of the total BoM of the CCTV Camera (DVR/NVR)		
3.0	In-house R&D #	Domestically/In-house R&D includes scientific research, experimentation, prototyping and testing for development of new products, process, technologies, or solutions using its own resources/expertise or legal contract with R&D unit registered with <i>Department of Scientific and Industrial Research (DSIR)</i> in India. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:		
		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
4.0	In-house Design/IPR #	Domestically/In-house Designing involves the process of design practices, services, or solutions within the organization's own facilities, using its own resources/expertise or legal contract with third party in India. Any patents, trademarks, copyrights, and trade secrets registered under Intellectual Property Rights (IPR) in India in favor of the design for their creations or inventions establishes legal ownership. The weightage of this will be calculated based on the percentage of the domestic BOM in respective Financial Year as mentioned in below table.:		

		2023-24 & 2024-25	2025-26	2026-27 onwards
		7%	10%	12%
5.0	Housing (Plastic / Aluminium / MS) and Camera Mount	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Housing and Camera Mount shall not exceed 5 % of the total BoM of the DVR/NVR.		
6.0	Connecting Cables, Connectors and USB Mouse	Domestically manufactured from domestically manufactured inputs. The weightage of the total value of inputs for Connecting Cables, Connectors and USB Mouse shall not exceed 5% of the total BoM of the DVR/NVR.		
7.0	Remote Control	Domestic assembly* and testing from imported / domestically manufactured parts and components subject to the condition that the value of domestically manufactured parts and components used in the assembly of "Remote Control" will be minimum 20% (of the total value of the parts and components used in the manufacture of "Remote Control") in Year 2, which will increase to minimum 30%, 40% and 50% in Financial Years 2025-26, 2026-27 and 2027-28 onwards respectively.		
8.0	Power Adapter	Domestic PCB assembly* and the final assembly and testing from imported / domestically manufactured parts and components, subject to the condition that the value of domestically manufactured parts and components used in the assembly of "Power Adapter" will be minimum 40% (of the total value of parts and components used in the manufacture of "Power Adapter"). However, the weightage of the total value of "Power Adapter" shall not exceed 5% of the total BoM of the DVR/NVR.		
9.0	Final Assembly and Testing	Domestically assembled/tested meeting Indian Standards as notified from time to time. The weightage of the total value of final assembling and testing shall not exceed 10 % of the total BOM of the DVR/NVR.		

* It is essential that the Printed Circuit Board Assembly (PCBA) of the parts and components on the bare PCB using the SMT process should mandatorily be done in India.

** This shall be reviewed when the Semiconductor FAB in India is operational.

The applicant will be eligible to avail the benefit of Sr. No. 4.0 (In-house R&D) & Sr. No. 5.0 (In-house Design/IPR) in respective financial year for calculation of Value Addition/Local Content by meeting the minimum Value Addition/Local Content mentioned in below table for respective financial year.

Financial Year	2023-24 & 2024-25	2025-26	2026-27 onwards
Minimum Value Addition/Local Content of (Sr. No. 1.0) Main PCB and (Sr. No. 9.0) Final Assembly and Testing as -Essential and others as optional	25%	35%	45%

5. The surveillance devices i.e., CCTV Cameras (Analog/ IP/ Analog Speed Dome/ IP Speed Dome) should comply with the Essential Requirements (ERs) for security prescribed by MeitY to ensure the security of the VSS / CCTV systems, as per the Appendix 'A', as amended from time to time. The security testing report for CCTV/VSS to be issued by Standardisation Testing and Quality Certification (STQC) Laboratory or any other agency notified by MeitY from time to time. The validity of the test report issued by STQC Lab will be three years from the date of issue of the report. These Essential Requirements (ERs) for security of CCTV Cameras/VSS system will be enforced after 3 months from the date of issuance of this Notification. The security norms for the DVR and NVR will be notified subsequently.

6. The notification will come into effect after 3 months from the date of issuance of this Notification. This Notification shall remain valid till the revised Notification is issued. The Year 1 for the purpose of this notification would be upto 31.03.2025.

7. No Electronic Product Notification under the Public Procurement (Preference to Make in India) Order 2017 shall have retrospective effect.

8. Purchase Preference shall be provided as per the provisions cited in the Public Procurement (Preference to Make in India) Order 2017 dated 16.09.2020 and, as amended from time to time, for the procurement of aforesaid electronics products.

9. The notification would also be applicable to all Central Schemes (CS)/ Central Sector Schemes (CSS) for the procurement of electronic products made by States and local bodies, if project or scheme is fully or partially funded by Government of India.

10. Procedure for calculating local content/ domestic value addition

10.1 Bill of Material sourced from domestic manufacturers (Dom-BOM) may be calculated based on one of the followings depending on data available:

- a) Sum of the costs of all inputs which go into the product (including duties and taxes levied on procurement of inputs except those for which credit/ set-off can be taken) and which have not been imported directly or through a domestic trader or an intermediary.
- b) Ex-Factory Price of product minus profit after tax minus sum of imported Bill of Material used (directly or indirectly) as inputs in producing the product (including duties and taxes levied on procurement of inputs except those for which credit/ set-off can be taken) minus warranty costs.
- c) Market price minus post-production freight, insurance and other handling costs minus profit after tax minus warranty costs minus sum of Imported Bill of Material used as inputs in producing the product (including duties and taxes levied on procurement of inputs except those for which credit / set-off can be taken) minus sales and marketing expenses.

10.2 Total Bill of Material (Total BOM) may be calculated based on one of the following depending on data available:

- a) Sum of the costs of all inputs which go into the product (including duties and taxes levied on procurement of inputs except those for which credit / set-off can be taken).
- b) Ex-Factory Price of product minus profit after tax, minus warranty costs.
- c) Market price minus post-production freight, insurance and other handling costs minus profit after tax, minus warranty costs minus sales and marketing expenses.

10.3 The percentage of domestic value-addition may be calculated based on information furnished as per the following formula:

Percentage of local content/ domestic value-addition = [(Dom-BOM) / (Total BOM)]*100

11. Verification of local content/ Domestic Value Addition

11.1. The local supplier at the time of tender, bidding or solicitation shall provide self-certification that the item offered meets the minimum local content and shall give details of the location(s) at which the local value addition is made.

11.2. In cases of procurement for a value in excess of Rs.10 crore, the local supplier shall provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.

11.3. In case a complaint is received by the procuring agency or the concerned Ministry/Department against the claim of a bidder regarding local content/ domestic value addition in an Electronic Product(s), the same shall be referred to STQC.

11.4. Any complaint referred to STQC shall be disposed of within 4 weeks. The bidder shall be required to furnish the necessary documentation in support of the domestic value addition claimed in an Electronic Product(s) to STQC. If no information is furnished by the bidder, such laboratories may take further necessary action, to establish the bonafides of the claim. In case of the discrepancies in computation of local content, a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) for calculating the percentage of local content will supersede over the self-declaration certificate.

11.5. A complaint fee of Rs.2 Lakh or 1% of the value of the domestically manufactured Electronic Products being procured (subject to a maximum of Rs. 5 Lakh), whichever is higher, to be paid by Demand Draft to be deposited with STQC. In case, the complaint is found to be incorrect, the complaint fee shall be forfeited. In case, the complaint is upheld and found to be substantially correct, deposited fee of the complainant would be refunded without any interest.

11.6. False declarations will be in breach of the Code of Integrity under Rule 175(1)(i)(h) of the General Financial Rules (GFR) for which a bidder or its successors can be debarred as per Rule 151 (iii) of the General Financial Rules along with such other provisions of bidding, debarment by a single Ministry/Department and revocation of orders as per the Department of Expenditure O.M-No. F.1/20/2018-PPD dated 2nd Nov, 2021 may be permissible under law amended from time to time.

12. MeitY shall be the Nodal Ministry to monitor the implementation of the Electronic Products notifications. In case of any dispute/clarifications against the decision given by STQC, a committee is constituted with the following

compositions for verification/vetting the complaints, independent verification of self-declarations and auditor's/accountant's certificates on random basis, restrictive and discriminating terms and conditions against the domestic manufactures of Electronics Products(s): -

- | | | |
|------|--|--------------------|
| i) | Group Coordinator/Scientist- 'G' (IPHW) | - Chairperson |
| ii) | Scientist-'G'/Scientist-'F' from STQC | - Member |
| iii) | Scientist- 'E' or above from Cert-In/Cyber Division | - Member |
| vi) | Any other member(s) as co-opted by the Chairperson - | Member |
| v) | Representative from IPHW Division | - Member Secretary |

13. In case of a question whether an item being procured is an Electronic Product(s) to be covered under the Public Procurement (Preference to Make in India) Order 2017, the matter would be referred to the Ministry of Electronics and Information Technology for clarification.

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

ASHA NANGIA, Group Coordinator & Scientist 'G'

Appendix 'A'

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.	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	1. Datasheet of the SoC being used in the device. 2. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. 3. Process flow of the Manufacturing/Provisioning of the device

		<p>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 audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning.</p> <p>[For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/peripherals.]</p>	
	1.2 Verify that cryptographic keys and certificates are unique to each individual device.	<p>Identifying all the keys and certificates being used in the device eco-system 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>1. List of all keys and certificates being used in the device ecosystem</p> <p>2. Key management life cycle (purpose, generation, storage, destruction/zeroization, validity, key changeover/rotation)</p>
	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.	<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</p>	<p>1. Datasheet of the SoC being used in the device.</p> <p>2. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same.</p> <p>3. Process flow of the Manufacturing/Provisioning of the device</p>

		<p>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 audit of the manufacturing facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning.</p> <p>[For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/peripherals.]</p>	
	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: No further assessment</p> <p>CASE 2: TEE/SE/TPM is available and enabled: 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: Termed as non-conformance to the requirement. OEM is required to enable and implement the TEE/SE/TPM.</p>	<p>1. Datasheet of the SoC being used in the device.</p> <p>2. User manual/ Technical specifications of the device</p> <p>3. Code snippets of the TEE API call, wherever applicable</p>
	1.5 Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM,	<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>	<p>1. List of all keys and certificates being used in the device ecosystem</p> <p>2. List of all the sensitive data with their intended usage and secure storage</p>

	TEE (Trusted Execution Environment), or protected using strong cryptography.	<ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	<p>mechanism(s) as implemented along with secure configurations to be enabled in the device.</p> <p>3. Key management life cycle (purpose, generation, storage, destruction/zeroization, validity, key changeover/rotation) private keys and certificates.</p>
	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>1. Measures available in the device to prevent software tampering.</p> <p>2. Measures available in the device to prevent hardware tampering.</p>
	1.7 Verify that any available Intellectual Property protection technologies provided by the chip manufacturer are enabled.	Testing, in presence of OEM team, to verify the enabling of the Intellectual Property protection technologies provided by the chip manufacturer, if available.	<p>1. Datasheet of the SoC</p> <p>2. Documentation regarding the Intellectual Property protection technologies provided by the chip manufacturer which have been enabled.</p> <p>3. In case, no Intellectual Property protection technologies are being provided by the chip manufacturer, then a declaration stating the same.</p>
	1.8 Verify the device validates the boot image signature before loading.	<p>Testing, in presence of OEM team, to verify the following:</p> <p>1. Device boots up successfully with the documented secure boot process when a valid boot image is provided.</p> <p>2. Device does not boot up when a tampered boot image (like with missing signature, invalid signature) is provided.</p>	<p>1. Datasheet of the SoC</p> <p>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.)</p>
	1.9 Verify usage of cryptographically secure pseudo-random number generator on embedded device (e.g., using chip-provided random number	<p>Verification of the documentation provided by the vendor regarding the random number generators being used in the device.</p> <p>Verification through code-review that random number generators or related</p>	<p>Documentation regarding the random generators (either hardware based or software based or both) being used in the device with their intended usage.</p> <p>In case, hardware based random number generators are being used, vendors</p>

		generators).	libraries as applicable are being used in the device.	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.	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 security.	1. Verifying that strong encryption algorithms and secure TLS version is supported by the device to establish secure 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 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.	Specifications and documentation related to the configurations available in the applications and 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: <ul style="list-style-type: none">• Security features, related to secure server connections and digital	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

			<p>signature validation as implemented like strong cipher suites, secure TLS version, SSL pinning etc. supported by code walkthrough.</p> <ul style="list-style-type: none"> • 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> <p>3. Using tools such as Nmap to identify open ports through which device can be accessed 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>	server connections.
		<p>2.4 Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.</p>	<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> <ol style="list-style-type: none"> 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. 	<ol style="list-style-type: none"> 1. Firmware binaries for code review. 2. Internal code review reports

		<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>2.5 Verify that each firmware maintains a software bill of materials cataloging third party components, versioning, and published vulnerabilities.</p>	<p>Verification of the submitted list of third-party components by running automated tools like FACT on the firmware.</p> <p>Identifying vulnerabilities in the third-party component(s) through publically available vulnerability databases</p> <p>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>	<p>1. Documentation for information on software bill of materials, including third-party components and versions.</p> <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>
	<p>2.6 Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).</p>	<p>Independent secure code review [both automated and manual] 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.</p>	<p>1. Firmware binaries for code review.</p> <p>2. Internal code review reports</p>

			<p>[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>	
	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. 	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.	
	2.8 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.	Documentation regarding the security controls in place to hinder firmware reverse engineering.	
	2.9 Verify that	Testing, in presence of	Measures implemented in	

	the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.	OEM team, to verify the measures implemented in the device to make it resistant to time-of-check vs.time-of-use attacks.	the device to make it resistant to time-of-check vs. time-of-use attacks.
	2.10 Verify the device uses code signing and validates firmware upgrade files before installing.	Testing, in presence of OEM team, to verify the following: i) Device gets successfully updated with the documented secure upgrade process when a valid update package is provided. ii) Device does not boot up when a tampered update package (like with missing signature, invalid signature) is provided.	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 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.	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.
	2.12 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. 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	1. Modes of updates available i.e. automatic, manual or both. 2. Organizational process and policies regarding the issuing of updates to the devices.

			evaluation agency as per C20, C21 and C22 security requirement.	
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.	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 channel.	Identifying all the security mechanisms being used in the communication process verification through: <ul style="list-style-type: none"> • Testing, in presence of OEM team • Code review • Process audit of the key-life cycle process 	Documentation regarding the security measures implemented in the device to prevent tampering of the data 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.		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,		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.

		post-incident summary documents need to be submitted and demonstrate the same.		
		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 product development stage	4.1 Design and architecture details till the PCBA and SoC level to be provided to aid in counterfeit mitigation and malware detection.		Design and architecture documents till the PCBA and SoC level.
		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	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.	

		malware detection tools).		
		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.



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]
No. 1569]

नई दिल्ली, मंगलवार, अप्रैल 9, 2024/चैत्र 20, 1946
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 एक्सपोस्ट 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 एन्क्लोजर 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 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 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 डिबगर्स और एक्सेस कंट्रोल तंत्र का उपयोग करके सभी पोर्ट और यूएसबी, यूएआरटी और अन्य सीरियल वेरिएंट जैसे डिबगिंग 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

		टीम की उपस्थिति में परीक्षण। 4. डिवर्गिंग 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 क्रिप्टोग्राफिक 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	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 एसडब्ल्यूडी जैसे ऑन-चिप डिवर्गिंग 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 डिवर्गिंग इंटरफ़ेस की उपलब्धता की पहचान करना 2. विक्रेता दस्तावेज़ में घोषित की गई सुरक्षा के लिए उत्पादन उपकरणों और संबंधित पट्टेच नियंत्रण तंत्र में सक्षम पोर्ट/इंटरफ़ेस का सत्यापन और वैधता 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 डिवर्गिंग इंटरफ़ेस को सक्षम/अक्षम करने को सत्यापित करने के लिए ओईएम टीम की उपस्थिति में परीक्षण। 4. डिवर्गिंग इंटरफ़ेस 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	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>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>	
1.4 सत्यापित करें कि विश्वसनीय निष्पादन लागू और सक्षम है, यदि डिवाइस एसओसी या सीपीयू पर उपलब्ध है।	<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: कोई और अग्रिम मूल्यांकन नहीं</p> <p>स्थिति 2: टीईई/एसई/टीपीएम उपलब्ध और सक्षम है: कोड-समीक्षा के माध्यम से सत्यापन कि क्रिप्टो फंक्शन 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: 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 मैन्युअल/तकनीकी विनिर्देश 3. टीईई एपीआई कॉल के कोड क्लिपेट, 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।	<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 सूची 2. 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 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 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 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 जनरेटर (या तो हार्डवेयर आधारित या सॉफ्टवेयर 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	<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>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>विक्रेता को डिवाइस में उपलब्ध और सक्षम मेमोरी सुरक्षा नियंत्रणों की घोषणा प्रस्तुत करनी होगी।</p>
		<p>2.2 सत्यापित करें कि फर्मवेयर ऐप्स ट्रांसपोर्ट लेयर सुरक्षा का उपयोग करके ट्रांजिट में डेटा की सुरक्षा करते हैं।</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 बर्पसुइट जैसे टूल का उपयोग करके मैन-इन-द-मिडिल हमलों का उपयोग करके नेटवर्क ट्रैफिक के अवरोधन और डिक्लिप्शन के प्रयासों के लिए प्रतिरोधी हैं।</p>	<p>विक्रेता ट्रांसपोर्ट लेयर सुरक्षा से संबंधित एप्लिकेशन और फर्मवेयर में उपलब्ध कॉन्फिगरेशन से संबंधित विनिर्देश और दस्तावेज प्रस्तुत करेगा।</p>
		<p>2.3 सत्यापित करें कि फर्मवेयर ऐप्स सर्वर कनेक्शन के डिजिटल हस्ताक्षर को मान्य करते हैं।</p>	<p>1. उन परिदृश्यों की पहचान करना जब डिवाइस बाह्य दुनिया के साथ सर्वर कनेक्शन स्थापित करता है और निम्नलिखित की पुष्टि करता है:</p>	<p>विक्रेता को उपयोग के मामलों का उल्लेख करते हुए एक दस्तावेज प्रस्तुत करना होगा जब डिवाइस बाहरी दुनिया के साथ सर्वर कनेक्शन स्थापित करता है, जिसमें सर्वर कनेक्शन के डिजिटल</p>

			<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 ऑरिकल 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 पहुँचा जा सकता है जिससे अनपेक्षित डेटा पुनर्प्राप्ति हो सकती है।</p> <p>4. यह सत्यापित करना कि टीएलएस सत्र बर्पसुइट जैसे उपकरणों का उपयोग करके मैन-इन-द-मिडिल हमलों का उपयोग करके नेटवर्क ट्रैफिक के अवरोधन और डिफ्रिप्शन के प्रयासों के लिए प्रतिरोधी हैं।</p>	<p>हस्ताक्षरों को मान्य करते समय सुरक्षा उपायों के बारे में विस्तृत जानकारी होगी।</p>
	<p>2.4 सत्यापित करें कि प्रतिबंधित सी फ़ंक्शंस के किसी भी उपयोग को उचित सुरक्षित समकक्ष फ़ंक्शंस के साथ बदल दिया गया है।</p>	<p>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]:</p> <p>1. फ़र्मवेयर कोड के साथ विक्रेता द्वारा मूल्यांकन एजेंसी का दौरा करना और मूल्यांकन एजेंसी के पास उपलब्ध लाइसेंस प्राप्त स्थैतिक विश्लेषण उपकरण को</p>	<p>विक्रेता द्वारा उपलब्ध करना होगा:</p> <p>1. कोड समीक्षा के लिए फ़र्मवेयर बायनेरिज़।</p> <p>2. आंतरिक कोड समीक्षा रिपोर्ट</p>	

		<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>श्रेमबर्क सहित सभी कोड की समीक्षा की जाती है।</p>	<p>कोड समीक्षा [स्वचालित और मैनुअल दोनों]:</p> <ol style="list-style-type: none"> 1. फ़र्मवियर 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 फ़र्मवियर 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 फ़र्मवियर कोड वाले मूल्यांकन एजेंसी को विक्रेता साइट पर सिस्टम की दूरस्थ पहुंच प्रदान करना। 	<p>2. आंतरिक कोड समीक्षा रिपोर्ट</p>
<p>2.7 सत्यापित करें कि फ़र्मवियर 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 बॉकश्रु द्वारा समर्थित हैं। • डिवाइस में उचित प्रमाणपत्र सत्यापन, प्रमाणपत्र श्रृंखला सत्यापन और प्रमाणपत्र निरस्तीकरण जांच लागू की जाती है। 	<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 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 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 है और विक्रेता मैन्युअल अपडेट प्रदान करता है:</p> <p>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।</p>		
3.	सुरक्षित अनुरूपता	प्रक्रिया	<p>3.1 सत्यापित करें कि वायरलेस संचार परस्पर प्रमाणित हैं।</p> <p>3.2 सत्यापित करें कि वायरलेस संचार एक एन्क्रिप्टेड चैनल पर भेजा जाता है।</p> <p>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।</p> <p>3.4 आपूर्ति श्रृंखला जोखिम की पहचान,</p>	<p>विक्रेता द्वारा दस्तावेज में निर्धारित आपसी प्रमाणीकरण की प्रक्रिया को सत्यापित करने के लिए, ओईएम टीम की उपस्थिति में परीक्षण करना।</p> <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 	<p>विक्रेताओं को वायरलेस संचार शुरू होने पर डिवाइस में लागू पारस्परिक प्रमाणीकरण की प्रक्रिया के संबंध में दस्तावेज प्रदान करना होगा।</p> <p>यदि डिवाइस वायरलेस संचार का समर्थन नहीं करता है, तो विक्रेता को इसके लिए एक घोषणा पत्र प्रदान करना होगा।</p> <p>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 बनाने होंगे।</p> <p>यदि डिवाइस वायरलेस संचार का समर्थन नहीं करता है, तो विक्रेता को इसके लिए एक घोषणा पत्र प्रदान करना होगा।</p> <p>विक्रेता को महत्वपूर्ण हार्डवेयर घटकों (एसओसी जैसे सुरक्षा कार्यों से संबंधित) के लिए सामग्री का बिल प्रस्तुत करना होगा।</p>
				विक्रेता निम्नलिखित प्रस्तुत करेंगे: 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 प्रप्राइवेटरी 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.	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: <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

	<p>1.4 Verify that trusted execution is implemented and enabled, if available on the device SoC or CPU.</p>	<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: No further assessment</p> <p>CASE 2: TEE/SE/TPM is available and enabled: 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: 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
	<p>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>	<p>Identifying all the keys and certificates being used in the device ecosystem, 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.
	<p>1.6 Verify the presence of tamper resistance and/or tamper detection features.</p>	<p>Testing, in presence of OEM team, to verify the measures implemented in the device to prevent software and hardware tampering.</p>	<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.
	<p>1.7 Verify that any available Intellectual</p>	<p>Testing, in presence of OEM team, to verify the enabling of the</p>	<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>	
	<p>2.4 Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.</p>	<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>
	<p>2.5 Verify that each firmware maintains a software bill of materials third party</p>	<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>

		<p>components, versioning, and published vulnerabilities.</p>	<p>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>	<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>
		<p>2.6 Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).</p>	<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"> 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. 	<p>Vendor shall provide:</p> <ol style="list-style-type: none"> 1. Firmware binaries for code review. 2. Internal code review reports

		<p>2.7 Verify that the firmware apps pin the digital signature to a trusted server(s).</p>	<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>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>
		<p>2.7 Verify security controls are in place to hinder firmware reverse engineering (e.g. removal of verbose debugging symbols).</p>	<p>Testing, in presence of OEM team, to verify the security controls as provided by the vendor to hinder firmware reverse engineering.</p>	<p>Vendor shall submit the documentation regarding the security controls in place to hinder firmware reverse engineering.</p>
		<p>2.8 Verify that the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.</p>	<p>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.</p>	<p>Vendor shall submit the measures implemented in the device to make it resistant to time-of-check vs. time-of-use attacks.</p>
		<p>2.9 Verify the device uses code signing and validates firmware upgrade files before installing.</p>	<p>Testing, in presence of OEM team, to verify the following:</p> <ol style="list-style-type: none"> 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. 	<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.</p>

		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.

W-43/11/2021-IPHW
Government of India
Ministry of Electronics and Information Technology
(IPHW Division)

Electronics Niketan,
6, CGO Complex,
Lodhi Road, New Delhi-110003.

Dated: 11 Mar, 2024

OFFICE MEMORANDUM

Subject: -Advisory on the Threat of Information Leakage through CCTV/ Video Surveillance system (VSS)/ Digital Video Recorders /Network Video Recorders-reg

The reference is made to the concerns raised by various Ministries/Departments regarding the security implications associated with the deployment of Closed-Circuit Television (CCTV) Cameras and the conduct of cyber auditing and testing of hardware pertaining to CCTV cameras and other Internet of Things (IoT) devices. The Ministry of Electronics and Information Technology (MeitY) has formulated comprehensive security guidelines for CCTV cameras as included in **Annexure 'A'**.

2. In light of these concerns, Government Ministries/Departments are strongly advised to adhere to the guidelines outlined within the ambit of the Public Procurement Orders to safeguard the overall security and integrity of CCTV Cameras and IoT Devices.
3. This issues with the approval of the Competent Authority.


(Asha Nangia)

Group Coordinator & Scientist-'G'
Ph. 011-24301965

To,

- i) Secretaries of All Ministries/Department of Government of India**
- ii) Chief Secretaries/Administrators of Union Territories/National Capital Territory of Delhi**

Annexure- 'A'

A video surveillance system, also known as Closed-Circuit Television (CCTV) system, is a collection of cameras and other related equipment used to monitor and record activities in a specific area commonly used for security and surveillance purposes.

2. Key components of a video surveillance system typically include cameras, (Analog, Digital, IP Cameras), Video Management System (VMS) Software, Storage (Network Video Recorders (NVRs) or Digital Video Recorders (DVRs)), Power Supply etc.

3. While these surveillance technologies undoubtedly offer a range of benefits and are valuable tools for monitoring and security, they also raise certain concerns and risks. Some of the growing risks associated with CCTV systems include data security, privacy breach, hacking and cyber-attack etc. Various incidents have also been reported due to security flaw in the surveillance cameras.

4. The cybersecurity is an ongoing process, so staying vigilant and keeping system up to date with the latest security practices can significantly enhance the security of CCTV system and protect it from potential threats and unauthorized access. In this regard, the following measures are advised to minimize the risk associated with CCTV surveillance system:

- i) The Rules and regulations as applicable, notified by the Government or procurement of goods and services must be followed e.g.
 - a) Public procurement Order (Make in India), 2017
 - b) Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021
- ii) BIS has formulated Blank Detail Specification (BDS) for IS 16910 for performance requirements of CCTVs. The procuring government agency can stipulate their own technical requirements for the parameters listed in the BDS and the testing can be done as per the test methods prescribed in the standard.
- iii) The procurement of Video Surveillance System from the brand having history of security breaches and data leakages should be avoided.

- iv) **Hardware Security:** For the Hardware Security testing of CCTV cameras, the government agencies should use the testing infrastructure available with Standardization Testing and Quality Certification (STQC) Laboratory or any other agency notified by MeitY from time to time for testing the CCTVs as per the Essential Requirement(s) notified under the PPO for CCTV.
- v) **Network Security:** The general cyber security practices for installation and monitoring should be also be adopted. Maintain the network isolation (Air-Gap) from the public network to minimize the risk of unauthorized access and potential cyberattacks. Wherever, air gap is not possible, Network segmentation, secure tunnel/Virtual Private Network (VPN) /Dedicated Lease Line etc. should be used for restricting access to CCTV systems and isolate them from critical infrastructure and sensitive data. Use MAC address binding to prevent the unauthorized access by unidentified devices.
- vi) **Secure Physical Access:** Restrict physical access to the CCTV control room and equipment. Only authorized personnel should have access to the system. Use locks, access control systems, and surveillance measures to protect the equipment.
- vii) **Strong Passwords:** Change default passwords immediately upon installation and use strong, unique passwords for all cameras, recorders, and access points. Avoid using easily guessable information or common words.
- viii) **Regular Firmware Updates:** Manufacturers often release updates that address security vulnerabilities. Regularly check for updates and apply them promptly keeps the firmware and software of your CCTV devices up to date.
- ix) **Encryption of Data:** Ensure all communication between cameras, recorders, and viewing devices is encrypted. This prevents unauthorized individuals from intercepting and accessing sensitive information.
- x) **Disable Unused Features:** Turn off or disable any features and services that are not necessary for the proper functioning of the CCTV system. Each enabled feature potentially introduces another security vulnerability.
- xi) **Secure Remote Access:** If remote access is required for maintenance or monitoring, implement a secure VPN (Virtual Private Network) for remote connections. Avoid exposing the system directly to the internet whenever possible. IPBEUs (IP-Based Encryption Unit) to safeguard data transmission between cameras and recording devices, Lease Line for dedicated and secure

network connectivity and Implementation of data diodes to ensure unidirectional flow of information, enhancing security.

- xii) **Regular Auditing and Monitoring:** Monitor the CCTV system logs for unusual activities and potential security breaches. Regularly audit the system to ensure that everything is functioning correctly and there are no unauthorized access attempts.
- xiii) **Physical Camera Security:** Position cameras in a way that prevents tampering and vandalism. Use vandal-resistant camera housings and install them in high and secure locations where they are less likely to be tampered with.
- xiv) **User Access Control:** Implement a strict access control policy to limit the number of individuals who can access the CCTV system and its data. Assign different levels of access based on roles and responsibilities.
- xv) **Data Storage and Retention:** Ensure proper data storage and retention policies are in place. Securely store recordings and define how long data should be retained before it gets automatically deleted. Data Storage should be in terms of storage duration (number of Days) based on operational requirements rather than storage capacity. The data storage of all CCTVs installed at Government Establishment/Public Places should be mandated to be within the India even if it is stored in cloud platforms.
- xvi) **Staff Training:** Provide comprehensive training to employees and system administrators on security best practices. Make sure they understand the potential risks and how to mitigate them effectively.
- xvii) **Regular Security Assessments:** Conduct periodic security assessments and penetration tests to identify vulnerabilities and weaknesses in the CCTV system. Address any issues discovered promptly.
- xviii) **Tender/RFP** should encompass both Hardware and Software parts of the Bill of Materials (BoM) combined presenting comprehensive specifications for these components to facilitate the interoperability of the HW/SW as a whole in the VSs system. Model Technical Specifications/Guidelines for CCTVs/VSS issued by MHA from time to time, should be adopted while formulating the technical specifications for procurement of CCTV/VSS.
- xix) **CCTV Device testing and certification:** CCTV Cameras (Analog/ IP/ Analog Speed Dome/ IP Speed Dome) should comply with the Essential Requirements (ERs) notified as part of the PPO for CCTV in Gazette of India (EXTRAORDINARY, PART II—Section 3—Sub-section (ii) dated 7th March,

2024, at Sr. No. No. 1062) to ensure the security of the VSS / CCTV systems, as amended from time to time. The security testing certificate for CCTV/VSS to be issued by Standardisation Testing and Quality Certification (STQC) Laboratory or any other agency notified by MeitY from time to time. The validity of the test report issued by STQC Lab will be three years from the date of issue of the report.

5. In this regard, the Government Ministries, Departments are advised to instruct the Chief Information Security Officers (CISOs) of their respective organizations and subordinate organizations for enforcing the above measures to address the security threats of the CCTV network vulnerability and to ensure the overall security and integrity of CCTV/Video Surveillance Systems.

=====*********=====