भारत सरकार
(गृह मंत्रालय)
संचार एवं आईटी निदेशालय
केन्द्रीय रिज़र्व पुलिस बल
पूर्व ब्लॉक -7, सेक्टर -1, आर.के. पुरम, नई दिल्ली -110066
(टेली / फैक्स नं -011-26107493, ईमेल आईडी: comncell@crpf.gov.in)

संख्या.ख.पाँच-7/2024-25-सी (*एनएसी*)-क्यू दिनांक, *11 दिसम्बर*2024

विषय:- "नेटवर्क एक्सेस कंट्रोल" के ड्राफ्ट क्यूआर (गुणात्मकआवश्यकता) / टीडीस (परीक्षणनिर्देशों) पर हितधारकों / निर्माताओं/ विक्रेताओंकीटिप्पणी के लिए अनुरोध।

1. "नेटवर्क एक्सेस कंट्रोल" के प्रस्तावित गुणात्मक आवश्यकता और परीक्षण निर्देशों को परिशिष्टए के रूप में संलग्न किया गया है। हितधारकों /निर्माताओं / विक्रेताओं से अनुरोध किया जाता है कि वे उस उत्पाद की विस्तृत एवम् सटीक जानकारी दें।साथ ही प्रत्येक पैरामीटर के अनुरूप अपने उत्पाद के सही विवरणों को प्रस्तुत करें। सिर्फ 'अनुपालना' या 'अनुपालना नहीं' वाली टिप्पणी स्वीकार नहीं की जाएगी। फर्म से निम्नलिखित विवरण प्रस्तुत करने का भी अनुरोध किया जाता है:-
   - आप ओईएम हैं या विक्रेता हैं ?
   - यदि विक्रेता हैं तो ओईएम का विवरण दें।
   - ओईएम का प्राधिकरण प्रमाण पत्र दें।

2. आवश्यक जानकारी / विवरण 26 दिसम्बर2024 तक निम्नलिखित पते पर भेजे जा सकते हैं।

   संचार निदेशालय सीआरपीएफ
   लेवल -4, ईस्ट ब्लॉक -7, सेक्टर -1, आर.के. पुरम
   नई दिल्ली -110066
   ईमेल: comncell@crpf.gov.in

3. शीघ्र प्रतिक्रिया का अनुरोध किया जाता है।

11/12/24

{उज्जवल कुमार सिंह, सहा०कमांडेंट(क्यू०आर०)}
कृते पुलिसउपमहानिरीक्षक (उपकरण)
महानिदेशालय, के.रि.पु.बल

नेटवर्क एक्सेस कंट्रोल सॉल्यूशन के लिए परीक्षण निर्देश

एसएल नं.	विनिर्देशन	परीक्षण निर्देश
प्रस्तावित सॉल्यूशन नीचे दिए गए विनिर्देशों को पूरा करेगा। कार्यक्षमता को सक्षम करने के लिए आवश्यक कोई भी हार्डवेयर / सॉफ़्टवेयर / लाइसेंस पहले दिन से ही प्रदान किया जाएगा		
ए	**डिवाइस प्रोफाइलिंग और विजिबलिटी**	
1	डिवाइस के प्रकार की परवाह किए बिना सुरक्षा और ऑडिट मांगों के लिए इंडपॉइंट्स का स्वचालित पता लगाना और वर्गीकरण करना।	ओईएमटेकब्रोशरऔरकंसोलसॉफ्टवेयरके साथसत्यापन
2	संग्रहीत प्रोफाइलिंग डेटा को डिवाइस प्रोफ़ाइल परिवर्तनों की पहचान करनी चाहिए और प्राधिकरण विशेषाधिकारों को गतिशील रूप से संशोधित करना चाहिए। *उदाहरण के लिए, यदि कोई प्रिंटर विंडोज लैपटॉप के रूप में दिखाई देता है, तो सिस्टम स्वचालित रूप से एसेस से इनकार कर सकता है। प्रोफ़ाइल स्कैन और शेड्यूल्ड सबनेट स्कैन के लिए लोड बैलेंसिंग का समर्थन करना चाहिए।*	
3	पैसिव डिवाइस प्रोफाइलिंग विधियों जैसे कि डीएचसीपी, स्पैन पोर्ट्स, एचटीटीपीउपयोगकर्ता-एजेंट, एमएसी ओयूआईऔर टीसीपी एसवाईएन-एसीकेहैंडशेक का समर्थन करना चाहिए।	
4	सक्रिय डिवाइस प्रोफाइलिंग विधियों जैसे कि एसएनएमपी, सबनेट स्कैन, एसएसएच, एसफ्लो, डब्ल्यूएमआईऔर एनएमएपीस्कैन का समर्थन करना चाहिए।	
5	आंतरिक डिवाइस फ़िंगरप्रिंट डिक्शनरी समय-समय पर स्वचालित रूप से या मैन्युअलीअपडेट करने का तरीका प्रदान करते हैं। वायर्ड और वायरलेस डिवाइस के लिए कस्टम फ़िंगरप्रिंट डिफाइन करने में सक्षम।	
6	कुल इंडप्वाइंट की संख्या, तथा श्रेणी के अनुसार संख्या, फेमली और डिवाइस प्रकार के अनुसार देखने के लिए एक व्यापक डैशबोर्ड प्रदान करना।	

बी	**प्रमाणीकरण, प्राधिकरण और लेखांकन (एएए)**	
1	एकीकृत स्केलेवल एएएसेवाएं (प्रमाणीकरण, प्राधिकरण और लेखांकन) जिसमें कान्टेक्स्ट की पूरी समझ के साथ एसेस पॉलिसी प्रबंधन शामिल है, जैसे उपयोगकर्ता की भूमिका, डिवाइस का प्रकार, स्थान, दिन का समय आदि।	ओईएमटेकब्रोशरऔरकंसोलसॉफ्टवेयरकेसाथसत्यापन
2	802.1X पर आधारित उपयोगकर्ता और डिवाइस प्रमाणीकरण, और बहु-विक्रेता वायर्ड नेटवर्क, वायरलेस नेटवर्क और वीपीएनपर वेब पोर्टल एक्सेस विधियाँ।	
3	एक साथ कई प्रमाणीकरण प्रोटोकॉलजैसे पीईएपी, ईएपी-एफएएसटी, ईएपी-टीएलएस, ईएपी-टीटीएलएस, और ईएपी-पीईएपी-पब्लिक का उपयोग।	
4	टीसीपीऔर टीएसएसपर रेडियसडेटाग्राम का सपोर्ट करने के लिए आरएडीएसईसीप्रोटोकॉल का सपोर्ट करना आवश्यक है।	
5	पहले दिन से ही सिंगल पॉलिसी के अंतर्गत मल्टीपलआईडेन्टीटी स्टोर, जैसे कि माइक्रोसॉफ्ट एक्टिव डायरेक्ट्री, केर्बेरोस, एलडीएपी-अनुरूप निर्देशिका, ओपन डाटाबेस कनेक्टिविटी (ओडीबीसी)-अनुरूप एसक्यूएल डाटाबेस, टोकन सर्वर, तथा डोमेन में आंतरिक डाटाबेस विशेषताओं का उपयोग करते हुए फाईन गेन कंट्रोल प्रदान किया जाना चाहिए।	
6	नॉन-802.1X डिवाइस (जैसे प्रिंटर, आईपी फोन, आईपी कैमरा और आईओटी डिवाइस) को डेटाबेस में उनके एमएसी एड्रेस की उपस्थिति के आधार पर ज्ञात के रूप में पहचाना जा सकता है, या नेटवर्क से कनेक्ट होने पर अज्ञात के रूप में पहचाना जा सकता है।	
7	विभिन्न विशेषाधिकार स्तरों वाले डिवाइस एडमिनिसट्रेटरऑपरेटरों आदि के सुरक्षित प्रमाणीकरण के लिए एकीकृत टीएसीएसीएस+ सर्वर इसे लॉग-इन यूजर द्वारा किए गए परिवर्तनों का ट्रैक रखना चाहिए।	
8	पीडीएफ/सीएसवी प्रारूपों में मैनुअल या शेड्युल्ड रिपोर्ट के साथ अनुकूलन योग्य रिपोर्टिंग, सीखे गए उपकरणों का विवरण दिखाने वाला इन्वेंटरी डैशबोर्ड, एक्सेस अनुरोधों और घटनाओं की वास्तविक समय की निगरानी, ईमेल के माध्यम से सक्रिय अलर्ट।	

9	एचटीटीपी/आरईएसटीएफयूएल एपीआई, एसवाईएसएलओजीमैसेजिंग और फ़ायरवॉल, एसआईईएम, इंडपॉइंट अनुपालन सुइट्स और उन्नतपॉलिसी प्रबंधन के लिए अन्य सॉल्यूशन के साथ इंडपॉइंट विशेषताओं का आदान-प्रदान करने की एक्सटेंशन क्षमता।	ओईएमटेकब्रोशरऔरकंसोलसॉफ्टवेयरकेसाथसत्यापन
10	मोबाइल डिवाइस प्रबंधन एकीकरण, डिवाइस निर्माता, मॉडल, ओएस वर्जन, जेल-ब्रोकन, किसी भी ब्लैक-लिस्टेड एप्लिकेशन की उपस्थिति, एमडीएम एजेंट की स्थापना की स्थिति आदि जैसी जानकारी प्राप्त करने और एक्सेस नीतियों में इस जानकारी का उपयोग करने के लिए।	
11	हेल्पडेस्क सॉफ्टवेयर सहित एपीआई इंटीग्रेशन, किसी भी नेटवर्क ट्रिगर्डपॉलिसी उल्लंघन के समस्या टिकटों के गतिशील निर्माण की अनुमति देता है।	
12	उत्पादन नेटवर्क पर लागू करने से पहले नीतियों का आकलन करने के लिए इंटरैक्टिव नीति सिमुलेशन और मॉनिटर मोड के लिए इनबिल्ट उपयोगिताएँ।	
13	प्रोसेस इनबाउंड थ्रीट से संबंधित इंवेट(जो किसी भी तृतीय-पक्ष विक्रेता डिवाइस, जैसे फ़ायरवॉल, एसआईईएम) एवं और डिफाईन प्रवर्तन पॉलिसी और सर्विस के आधार पर प्रवर्तन और कार्रवाई करना।	
14	उपयोगकर्ता जानकारी के लिए मल्टी डोमेन और मल्टीपल एडीऔर उपयोगकर्ता डेटाबेस सपोर्ट होना चाहिए।	
15	नेटवर्क पर अनुमति देने से पहले सभी यूजर मशीनों का मूल्यांकन किया जाना चाहिए और इस प्रकार उन्हें केवल सुरक्षित ।EEE 802.1X आर्किटेक्चर के साथ ही चालू किया जाना चाहिए।	
सी	**गेस्ट-एसेस प्रबंधन**	
1	किसी भी प्रकार के डिवाइस का उपयोग करके वायरलेस और वायर्ड नेटवर्क पर आगंतुकों, ठेकेदारों, भागीदारों, लेखा परीक्षकों आदि के लिए उपयोग में ईजी-टू-यूज गेस्ट प्रबंधन सॉल्यूशन करना।	ओईएमटेकब्रोशरऔरकंसोलसॉफ्टवेयरकेसाथसत्यापन
2	कंपनी के लोगो, विजुअल इमेजरी और संगठन के संदेश का विस्तार करने के लिए मल्टीमीडिया सामग्री के साथ वैकल्पिक विज्ञापनों सहित व्यापक ब्रांडिंग और कस्टोमाईजेशन के साथ	

	कैप्टिव पोर्टल के माध्यम से गेस्ट एसेस।	
3	कैप्टिव पोर्टल(विभिन्न स्क्रीन आकार का समर्थन करने के लिए उत्तरदायी डिजाइन) में मोबाइल डिवाइस जागरूकता होनी चाहिए ताकि वह स्मार्ट फोन, टैबलेट और लैपटॉप के लिए स्वचालित रूप से आकार ले सके।	
4	वेब पोर्टल के माध्यम से गेस्ट स्व-पंजीकरण, यूजर नाम और पासवर्ड सीधे आगंतुक के वेब ब्राउज़र पर पहुंचाना, या ईमेल या एसएमएस के माध्यम से भेजना।	
5	स्पांसर-आधारित अनुमोदन वर्कफ्लो, जिससे आंतरिक कर्मचारी गेस्ट को नेटवर्क तक पहुंचने की अनुमति देने से पहले गेस्ट खाते को अनुमोदित कर सके।	
6	बैंडविड्थ सीमा लागू करने, विशिष्ट संसाधनों तक एसेस, कनेक्शन की लंबाई और निर्दिष्ट घंटों या दिनों के बाद स्वचालित खाता समाप्ति सेट करने के लिए गेस्ट एसेस विशेषाधिकारों को अनुकूलित करना।	
7	गेस्ट पोर्टल में फेसबुक, ट्विटर, स्लैक और अन्य सोशल मीडिया क्रेडेंशियल्स का उपयोग करके सोशल लॉगिन स्वीकार करने का विकल्प होगा।	
8	तृतीय-पक्ष एकीकरण, सुव्यवस्थित पंजीकरण और भुगतान प्रणाली एकीकरण प्रदान करने के लिए रेस्ट-आधारित एपीआई का उपयोग करके अनुकूलन योग्य वर्कफ़्लो प्रदान करता है।	
डी	**पर्सनल डिवाईस प्रबंधन(BYOD)**	
1	मैकओएस , आईओएस, एंड्रॉइड, क्रोमबुक और उबंटू जैसे मोबाइल डिवाइस को स्वचालित रूप से कॉन्फ़िगर और प्रोविजन करना, जिससे सुरक्षित रूप से एंटरप्राइज़ नेटवर्क से कनेक्ट हो सकें । पहले दिन से कम से कम (यूजर विभाग द्वारा निर्धारित यूजरों की संख्या) यूजरके लिए सपोर्ट। प्रत्येक यूजर के पास अधिकतम दो डिवाइस हो सकते हैं और ऑनबोर्डिंग के लिए प्रायोजक अनुमोदन आवश्यक विकल्प का सपोर्ट कर सकते हैं।	ओईएमटेकब्रोशरऔरकंसोलसॉफ्टवेयरके साथसत्यापन

2	इक्सटर्नलसीएके कार्यान्वयन की आवश्यकता के बिना या आंतरिक सार्वजनिक कुंजी अवसंरचना (पीकेआई) में परिवर्तन किए बिना डिवाइस ऑनबोर्डिंग को सुरक्षित करने के लिए अंतर्निहित प्रमाणपत्र प्राधिकरण (सीए) प्रदान करना । यदि किसी कारण से कोई ओईएमअंतर्निहित सीएप्रदान करने में असमर्थ है, तो पहले दिन से हीवह इसे बाहरी रूप से प्रदान कर सकता है। रूट या इंटरमीडिएट सीएके रूप में काम करना चाहिए और सर्टिफिकेट प्रबंधन के लिए स्वयं सहायता पोर्टल का सपोर्ट करना चाहिए।	
3	एससीईपीऔर ईएसटी (आरएफसी 7030)प्रोटोकॉल का उपयोग करके तृतीय-पक्ष अनुप्रयोगों को अंतर्निहित सीएजनरेटेड सर्टिफिकेट के वितरण का सपोर्ट करना।	
4	यदि कोई यूजर संगठन छोड़ देता है या मोबाइल डिवाइस खो जाता है या चोरी हो जाता है, तो विशिष्ट मोबाइल डिवाइस के लिए रेपिड रिवोकेशन और सर्टिफिकेट का डिलिशन सुनिश्चित करना।	
5	ऑनलाइन सर्टिफिकेट स्टेटस प्रोटोकॉल (OCSP) का समर्थन करना।	
6	प्रति यूजर ऑन-बोर्ड किए जा सकने वाले उपकरणों की संख्या और उनके सर्टिफिकेट की वैधता को परिभाषित करने में सक्षम।	
7	ऑनबोर्डिंग के लिए प्रायोजक अनुमोदन के साथ स्वचालित डिवाइस सर्टिफिकेट प्रोविजनिंग/इंस्टालेशनविकल्प आवश्यक है।	
8	सर्टिफिकेटप्रोविजनिंग को उसके नोड्स के फेलओवर के बाद भी काम करना चाहिए।	
9	ओएयूटीएचऔर एसएएमएल 2.0 पहचान प्रदाता का सपोर्ट करना चाहिए , जो क्लाउड या ऑन-प्रिमाइस अनुप्रयोगों पर निर्बाध एकल साइन-ऑन (SSO) की अनुमति देता है।	
10	एकाधिक बहु-कारक प्रमाणकों (MFA/2FA) का सपोर्ट करना आवश्यक है।	
	सुरक्षित सर्टिफिकेट आधारित ऑनबोर्डिंग और स्वचालित डिवाइस सर्टिफिकेटप्रोविजनिंग/ इंस्टालेशन का समर्थन करना चाहिए।	

इ	**इंडप्वाइंट पोस्टर चेकिंग**	
1	सपोर्ट डिवाइस कनेक्ट होने से पहले संगठन के अनुपालन को सुनिश्चित करने के लिए उन्नत एंडपॉइंट स्थिति का एसेसमेंट करना।	ओईएमटेकब्रोशरऔरकंसोलसॉफ्टवेयरके साथसत्यापन
2	निम्नलिखित ऑपरेटिंग सिस्टम और संस्करणों का समर्थन करनाः- माइक्रोसाफ्ट विंडोज 7 एवं इससे ऊपर एवं एप्पल एमएसीओएस 10.10और इससे ऊपर।	
3	सपोर्ट अनहेल्दीइंडप्वाइंटयूजर जो अनुपालन आवश्यकताओं को पूरा नहीं करते हैं, उन्हें एंडपॉइंट की स्थिति के बारे में एक संदेश और अनुपालन प्राप्त करने के निर्देश प्राप्त होने चाहिए।	
4	सपोर्टइंडप्वांइट पोस्चरऔर हेल्थ चेक में इंस्टाल्ड अनुप्रयोग, एंटी वायरस , फ़ायरवॉल, नेटवर्क कनेक्शन, प्रक्रियाएं, पैच प्रबंधन, पीयर टू पीयर अनुप्रयोग, वर्चुअल मशीन, यूएसबी डिवाइस आदि शामिल होने चाहिए।	
5	स्वचालित सुधार और नियंत्रण के साथ इंडप्वाइंट की नॉनस्टॉप निगरानी प्रदान करने के लिए ऑपरेटिंग सिस्टम के लिए स्थायी एजेंट का सपोर्ट।	
6	पर्सनल एवं नॉन-आईटी-दृश्य उपकरणों की इंडप्वाइंट अनुपालन जांच के लिए वेब-आधारित डिसोलवेवल एजेंट सपोर्ट ऑफरहोना।	
7	एकाधिक नेटवर्क इंटरफेस का पता लगाने और इसे नियंत्रित करने में सहायता करनी चाहिए।	
8	यूएसबीका पता लगाने, उसे अक्षम करने और हटाने में सहायता करनी चाहिए।	
9	सपोर्ट को 24/7 नेटवर्क नीति अनुपालन जांच और प्रवर्तन के साथ मानक आधारित शून्य ट्रस्ट एसेस नेटवर्क सुरक्षा ढांचे को सुनिश्चित करना चाहिए।	
एफ	**प्रबंधन और रिपोर्टिंग**	
1	रिपोर्टिंग के लिए पूर्वनिर्धारित टेम्पलेट उपलब्ध होने चाहिए।	ओईएमटेकब्रोशरऔरप्रबंधनसॉफ्टवेयरके साथसत्यापन
2	सॉल्यूशन में अंतर्निहित निगरानी, रिपोर्टिंग और ट्राबुलशूंटिग कंसोल होना चाहिए, ताकि हेल्पडेस्क संचालकों और एडमिनिस्ट्रेटर को स्ट्रीमलाईन ऑपरेशन में सहायता मिल सके।	
3	सॉल्यूशन को नेटवर्क के भीतर किसी भी अनधिकृत एसेस गतिविधि पर फोरेंसिक साक्ष्य एकत्र करना और रखना होगा,	

	जैसा कि नीचे बताया गया है: इवेंट टाइमस्टैम्प, अनुक्रम में नेटवर्क इवेंट, होस्ट जानकारी, आईपी पता, मैक पता, स्विच जानकारी, आदि।	
4	सॉल्यूशन को हार्डवेयर (मेमोरी, रैम, एचडीडी, पेरिफेरल उपकरण, आदि), संस्करण के साथ सभी स्थापित सॉफ्टवेयर, खुले पोर्ट, सर्विस रनिंग, प्रोसेस रनिंग और प्रबंधित विस्तारित उद्यम में अनुप्रयोग सूची के लिए रिपोर्ट तैयार करने की क्षमता का सपोर्ट करना चाहिए।	
5	सॉल्यूशन को इंटरैक्टिव तरीके से सूचना नोटिफिकेशन प्रदर्शित करने में सक्षम होना चाहिए, जैसे बबल नोटिफिकेशन, ईमेल, आदि।	
6	एनएसी सॉल्यूशन को एसआईईएम सॉल्यूशनऔर अन्य एसओसी घटकों के साथ एकीकृत करने में सक्षम होना चाहिए।	
7	प्रस्तावित एनएसी सॉल्यूशन को उपयोगकर्ता-अनुकूल नीति प्रबंधन (नीति खोज, नीति अद्यतन, इंपोर्ट/एक्सपोर्ट नीतियां, आदि) प्रदान करना चाहिए।	
8	विशिष्ट आवश्यकताओं के लिए समयबद्ध तरीके से मान्य टेम्पलेट्स वितरित करने की विधि प्रदान करने के लिए एक रिपोर्टिंग विकल्प उपलब्ध होना चाहिए।	
9	प्रवृत्तियों, अनुपालन और फोरेंसिक विश्लेषण को समझने के लिए अतीत में चयनित समय-सीमाओं के साथ-साथ वर्तमान डेटा पर रिपोर्ट तैयार करने की क्षमता की आवश्यकता होती है, अर्थात विशिष्ट तिथि और समय सीमा।	
10	निर्णय लेने के लिए आवश्यक जानकारी उपलब्ध कराने तथा डेटा ओवरलोड को न्यूनतम करने के लिए रिपोर्टिंग प्रणालियों को मजबूत फ़िल्टरिंग विकल्प उपलब्ध कराने चाहिए।	
11	ईमेल के माध्यम से नोटिफिकेशन के लिए सपोर्ट होना चाहिए।	
12	वेब-आधारित उपयोगकर्ता इंटरफ़ेस जो पॉलिसी कॉन्फ़िगरेशन, निगरानी और समस्या निवारण को सरल बनाता है।	
जी	**मौजूदा अप्रबंधित स्विच सहित क्षमताएँ**	

	प्रस्तावित एनएसी सॉल्यूशन ग्राहक नेटवर्क से कनेक्ट होते ही समापन बिंदु का पता लगाने में सक्षम होना चाहिए।	ओईएमटेकब्रोशरऔरप्रबंधनसॉफ्टवेयरकेसाथसत्यापन
	प्रस्तावित एनएसी समाधान को गैर-अनुपालक डिवाईस तक संचार को प्रतिबंधित करने में सक्षम होना चाहिए, जो हब/अप्रबंधित स्विच से जुड़ा हुआ हैएवं अन्य अनुपालक डिवाईस को कार्यात्मक रहना चाहिए।	
एच	**संपूर्ण डिवाइस इन्वेंटरी और कॉन्टेक्स्ट बनाने की क्षमता।**	
1	सॉल्यूशन को नेटवर्क से जुड़े अधिकृत उपकरणों और नेटवर्क को सक्षम करने वाले अधिकृत उपकरणों की अद्यतन/केंद्रीकृत इन्वेंटरी बनाए रखनी चाहिए।	OEM टेकब्रोशरऔरप्रबंधन सॉफ्टवेयरऔररिपोर्टिंगटूलकेसाथसत्यापन
2	सॉल्यूशन को स्वचालित तरीके से संपूर्ण डिवाइस इन्वेंटरी और कॉन्टेक्स्ट के साथ ड्रू-अप एंटरप्राइज़ एंडपॉइंट डेटा प्रदान करना चाहिए।	
3	सॉल्यूशन विंडोज़ पर हार्डवेयर प्रोपर्टीज जैसे हार्डवेयर कंप्यूटर, डिस्क, मॉनिटर, मदरबोर्ड, नेटवर्क एडाप्टर, फिजिकल डिवाइस, फिजिकल मेमोरी, प्लग एंड प्ले डिवाइस, प्रोसेसर आदि के लिए अनुपालन प्रदान करने में सक्षम होना चाहिए।	
4	सॉल्यूशन को हार्डवेयर की विस्तृत जानकारी के साथ-साथ विस्तारित उद्यम नेटवर्क में आईपी-कनेक्टेड ऐसेट्स की सूची को स्वचालित करना चाहिए जैसे डिस्क, मॉनिटर, मदरबोर्ड, नेटवर्क एडाप्टर, फिजिकल डिवाइस, फिजिकल मेमोरी, प्लग एंड प्ले डिवाइस, प्रोसेसर, आदि सभी आईपी-कनेक्टेड चीजों के वास्तविक समय के स्थान इंगित औरसभी आईपी-कनेक्टेड उपकरणों का निरंतर और सटीक रूप से आकलन।	
आई.	**आवश्यकता सारांश (रिटायरमेंट समरी)**	
1	सॉल्यूशन हार्डवेयर उपकरण पर आधारित होना चाहिए। सॉल्यूशन को पहले दिन से ही कम से कम 500 (**उपयोगकर्ता विभाग द्वारा निर्धारित संख्या) एंडपॉइंट सपोर्ट का समर्थन करना चाहिए।**	ओईएमटेकब्रोशरऔरप्रबंधनसॉफ्टवेयरकेसाथसत्यापन
2	सॉल्यूशन802.1x/RADIUS/TACACS+/Guest के लिए प्रति सेकंड न्यूनतम 200 प्रमाणीकरणों और एंडपॉइंट पोस्चर जाँच के लिए प्रति न्यूनतम 50 क्लाइंट/सेकेंड का समर्थन करना चाहिए।	

3	एएए, एंडपॉइंट पोस्चर चेक, गेस्ट एक्सेस, (**यूजर डिपार्टमेंट द्वारा तय की गई संख्या**) एंडपॉइंट प्रोफाइलिंग और (**यूजर डिपार्टमेंट द्वारा तय की गई संख्या) बीबाईओडीडिवाइस के लिए पहले दिन से ही** कम से कम 500 (**यूजर डिपार्टमेंट द्वारा तय की गई संख्या**) समवर्ती सत्रों का समर्थन करने वाले लाइसेंस। भविष्य में सॉल्यूशन को समाधान उपयोगकर्ता विभाग के अनुसार स्केलेबल होना चाहिए	
4	पर्पेटुअल/सदस्यता लाइसेंस के साथ 5 वर्ष की 24x7 हार्डवेयर और सॉफ्टवेयर वारंटी।	
एच	**ओईएमऔर उत्पाद पात्रता/अनुपालन**	
1	सॉल्यूशन नेटवर्क एक्सेस कंट्रोल (NAC) सॉल्यूशन के लिए कॉमन क्राइटेरियानेटवर्क डिवाइस सहयोगी सुरक्षा प्रोफ़ाइल (NDcPP) और प्रमाणीकरण सर्वर मॉड्यूल के लिए विस्तारित पैकेज दोनों के तहत प्रमाणित होना चाहिए। प्रमाणपत्र को संदर्भ के रूप में संलग्न किया जाएगा।	फर्म OEM प्रमाणपत्र प्रदान करेगी
2	ओईएमके पास भारत में आर एंड डी की सुविधा होनी चाहिए; यदि आवश्यक हो तो साइट विजिट की व्यवस्था की जाएगी।	फर्म OEM प्रमाणपत्र प्रदान करेगी
3	एएएको न्यूनतम पांच वर्ष की हार्डवेयर वारंटी के साथ 24X7 ओईएमप्रत्यक्ष सपोर्ट तथा सॉफ्टवेयर अपडेट/अपग्रेड के साथ प्रस्ताव किया जाएगा।	फर्म OEM प्रमाणपत्र प्रदान करेगी
4	साइट पर ओईएमप्रमाणित इंजीनियरिंग (उपयोगकर्ता विभाग द्वारा तय किया जाएगा)	