



भारत का राजपत्र

The Gazette of India

असाधारण
EXTRAORDINARY
भाग I—खण्ड 1
PART I—Section 1
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 143] नई दिल्ली, मंगलवार, जुलाई 2, 2013/आषाढ़ 11, 1935
No. 143] NEW DELHI, TUESDAY, JULY 2, 2013/ASADHA 11, 1935

संचार और सूचना प्रौद्योगिकी मंत्रालय
(इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग)

अधिसूचना

नई दिल्ली, 2 जुलाई, 2013

विषय : राष्ट्रीय साइबर सुरक्षा नीति - 2013 (एनसीएसपी - 2013) पर अधिसूचना।
राष्ट्रीय साइबर सुरक्षा नीति - 2013 (एनसीएसपी - 2013)

सं.2(35)/2011-सर्ट-इन.—आमुख

1. साइबर स्पेस, लॉगो, सॉफ्टवेयर और सेवाओं के बीच अंतःक्रियाओं का एक जटिल परिवेश है जिसे सूचना और संचार प्रौद्योगिकी (आईसीटी) युक्तियों और नेटवर्कों के विश्वव्यापी वितरण में समर्थन मिलता है।
2. प्रौद्योगिकी उन्नतियों द्वारा मिलने वाले अपार लाभों को देखते हुए आज साइबर स्पेस नागरिकों, व्यापार, महत्वपूर्ण सूचना मूल संचयन, सेना और सरकार द्वारा सामान्य रूप से उपयोग होने वाला एक पुल है, जिसे हम प्रकार इस्तेमाल किया जाता है कि इन अलग-अलग समूहों के बीच एक स्पष्ट सीमा रेखा बनाना कठिन है। साइबर स्पेस के आने वाले समय में और भी अधिक जटिल बनने की संभावना है, जब हमें जुड़े नेटवर्क और युक्तियों की संख्या में कई गुना वृद्धि होगी।
3. सूचना प्रौद्योगिकी (आईटी) उन महत्वपूर्ण क्षेत्रों में से एक है जो साइबर स्पेस में चलनी और निवास करनी है। यह भारतीय अर्थव्यवस्था के सर्वाधिक उल्लेखनीय वृद्धि उद्योगों में से एक के रूप में उभरी है। भारत की अर्थव्यवस्था को ऊर्जा देने के अलावा यह क्षेत्र विभिन्न सामाजिक-आर्थिक पैरामीटरों जैसे रोजगार, जीवन स्तर और अन्य के अलावा विविधता में प्रत्यक्ष और अप्रत्यक्ष योगदान के माध्यम से लोगों के जीवन पर सकारात्मक प्रभाव भी डालता है। हम क्षेत्र में विश्वस्तरीय प्रौद्योगिकी समाधान प्रदान करने और आईटी व्यापार सेवाओं में एक वैश्विक अभिकारक के रूप में

ISO / IEC 27032-2012

2893 GI/2013

(1)

भारत की छवि को रूपांतरित करने में एक महत्वपूर्ण भूमिका निभाई है। सरकार आईटी आधारित उत्पादों और आईटी समर्थित सेवाओं को लोक सेवाओं (सरकार से नागरिक सेवाएं, नागरिक पहचान, लोक वितरण प्रणालियों) स्वास्थ्य देखभाल (दूर चिकित्सा, दूरस्थ परामर्श, मोबाइल क्लिनिकल, शिक्षा (ई-अधिगम, आभासी कक्षाकक्ष आदि) और वित्तीय सेवाओं (मोबाइल बैंकिंग / भुगतान गेटवे) आदि को लगातार अपनाने में प्रमुख प्रेरक रही है। इन प्रयासों से क्षेत्रगत सुधारों और राष्ट्रीय कार्यक्रमों के माध्यम से देश में आईटी को लगातार अपनाने की सक्षमता बनी है, जिससे नैगम/ निजी भागीदारी के साथ बड़े पैमाने पर आईटी मूल संरचना का सृजन हुआ है।

4. देश में आईटी क्षेत्र की वृद्धि के प्रकाश में तीव्र सामाजिक रूपांतरण और समावेशी वृद्धि की महत्वाकांक्षी योजनाएं और आईटी वैश्विक बाजार में भारत की प्रमुख भूमिका से सुरक्षित कम्प्यूटिंग परिवेश के सृजन और इलेक्ट्रॉनिक लेन-देन, सॉफ्टवेयर, सेवाओं, युक्तियों और नेटवर्कों में पर्याप्त भरोसा और विश्वास देश की बाध्यकारी प्राथमिकताओं में से एक बन गई है। ऐसे फोकस से देश में वैश्विक नेटवर्क से जुड़े परिवेश के अनुसार एक उपयुक्त साइबर सुरक्षित पारिस्थितिकी प्रणाली के सृजन की सक्षमता बनती है।

5. साइबर स्पेस अनेक प्रकार की घटनाओं के प्रति सुभेद्य है, चाहे ये जानबूझ कर हों या दुर्घटनावश, मानव रचित हों या प्राकृतिक और साइबर स्पेस में विनिमय किए गए डेटा को राष्ट्रव्यापी और गैर राष्ट्र कारकों द्वारा कुटिल प्रयोजनों के लिए उपयोग किया जा सकता है। साइबर हमले जो मूल संरचना या अंतर्निहित आर्थिक कल्याण पर लक्षित हैं, एक राष्ट्र का कल्याण प्रभावी रूप से उपलब्ध राज्य संसाधनों को घटा सकते हैं और उनकी समर्थन संरचना में भरोसे को कम कर सकते हैं। राष्ट्रीय महत्व की साइबर संबंधी घटना कोई भी रूप ले सकती है, एक संगठित साइबर हमला एक अनियंत्रित विस्फोट जैसे कम्प्यूटर वायरस या बर्म या अन्य कोई दुर्भावना पूर्ण सॉफ्टवेयर कोड, एक राष्ट्रीय आपदा के साथ उल्लेखनीय साइबर परिणाम या अन्य संबंधित घटनाएं जो सूचना मूल संरचना या प्रमुख परिसंपत्तियों को व्यापक नुकसान पहुंचा सकती है। बड़े पैमाने पर साइबर घटनाओं से सरकार, जनता और निजी क्षेत्र के संसाधनों और सेवाओं को नुकसान पहुंच सकता है तथा महत्वपूर्ण सूचना प्रणालियों के कार्य में बाधा आ सकती है। उक्त परिमाण के विनाश की जटिलताओं में जीवन का जोखिम, अर्थव्यवस्था और राष्ट्रीय सुरक्षा शामिल हैं। शीघ्र पहचान, सूचना का आदान प्रदान, जांच और समन्वित प्रक्रिया तथा उपाय करने से दुर्भावनापूर्ण साइबर स्पेस गतिविधि द्वारा हुई हानि का शमन किया जा सकता है। साइबर हमलों से व्यक्तियों, व्यापार और सरकार को होने वाले नुकसान के कुछ उदाहरण हैं पहचान की चोरी, फिशिंग, सोशल इंजीनियरी, हेकटीविज्म, साइबर आतंकवाद, मोबाइल युक्तियों और स्मार्ट फोन पर लक्षित मिश्रित जोखिम, डिजिटल प्रमाणपत्रों में समस्या, उन्नत स्थायी जोखिम, सेवाओं को अस्वीकार करना, बोट नेट, आपूर्ति श्रृंखला पर हमले, डेटा का रिसाव आदि। सूचना मूल संरचना की सुरक्षा और गोपनीयता, निष्ठा और साइबर स्पेस में सूचना की उपलब्धता का संरक्षण सुरक्षित साइबर स्पेस का सारांश है।

6. साइबर सुरक्षा चुनौतियों को संबोधित करने के लिए सरकार के विभिन्न कार्यक्रम और गतिविधियां जारी हैं, जिससे एक ऐसे मंच के सृजन में उल्लेखनीय योगदान मिला है, जो साइबर स्पेस को सुरक्षित रखने के प्रयासों को समर्थन देने और स्थायी बनाने में सक्षम हैं। साइबर स्पेस के गतिशील प्रकार को देखते हुए अब यह इन कार्रवाइयों की जरूरत है जिसे राष्ट्रीय साइबर सुरक्षा नीति के तहत एकीकृत किया जाए, जिसमें समेकित संकल्पना और कार्यान्वयन के लिए स्थायी तथा समन्वित कार्यनीतियों का सैट शामिल हो।

7. साइबर सुरक्षा नीति एक विकासशील कार्य है और यह आईसीटी प्रयोक्ताओं और प्रदाताओं सहित घरेलू प्रयोक्ताओं एवं छोटे, मध्यम तथा बड़े उद्यमों और सरकार तथा गैर सरकारी इकाइयों में संपूर्ण स्पेक्ट्रम को आपूर्ति करती है। यह साइबर स्पेस की सुरक्षा से संबंधित कार्यों को परिभाषित तथा मार्गदर्शित करने के लिए एक व्यापक रूपरेखा के तौर पर कार्य करती है। यह वैयक्तिक क्षेत्रों और संगठनों को उपयुक्त साइबर सुरक्षा नीतियों की डिजाइन की सक्षमता प्रदान करती है जो उनकी जरूरतों के अनुरूप है। नीति में एक सिंहावलोकन प्रदान किया गया है, जिससे यह प्रभावी रूप से सूचना, सूचना प्रणालियों और नेटवर्क को सुरक्षा प्रदान करती है और साथ ही देश में साइबर स्पेस की सुरक्षा के लिए सरकार के मार्ग और कार्यनीति में एक अंतरदृष्टि प्रदान करती है। यह सहयोगात्मक कार्य की सक्षमता हेतु सार्वजनिक और निजी क्षेत्र के सभी प्रमुख कारकों के लिए कुछ बिन्दु तैयार करती है ताकि देश की सूचना और सूचना प्रणालियों को सुरक्षा प्रदान की जा सके। अतः इस नीति का लक्ष्य एक साइबर सुरक्षा रूपरेखा का सृजन करना है, जिससे देश के साइबर स्पेस की सुरक्षा संरचना को बढ़ाने के लिए विशिष्ट कार्य और कार्यक्रम किए जा सकें।

I. संकल्पना

नागरिकों, व्यवसायों और सरकार के लिए एक सुरक्षित और लचीले साइबर स्पेस का निर्माण करना

II. मिशन

साइबर स्पेस में सूचना और सूचना मूल संरचना की सुरक्षा करना, साइबर हमलों की रोकथाम और प्रतिक्रिया के लिए क्षमताओं का निर्माण, सुभेद्यता घटना तथा संसाधन संरचना, जन, प्रक्रमों, प्रौद्योगिकी तथा सहयोग के संयोजन द्वारा साइबर घटनाओं को कम करना।

III. उद्देश्य

- 1) देश में एक सुरक्षित साइबर पारिस्थितिकी तंत्र बनाने के लिए पर्याप्त विश्वास और आईटी सिस्टम और साइबर स्पेस में लेनदेन में विश्वास पैदा करने और इस प्रकार अर्थव्यवस्था के सभी क्षेत्रों में सूचना प्रौद्योगिकी को अपनाने में वृद्धि करना।
- 2) सुरक्षा नीतियों की डिजाइन के लिए और वैश्विक सुरक्षा मानकों के अनुपालन को बढ़ावा देने और समर्थनकारी कार्य तथा अनुरूपता आकलन (उत्पाद, प्रक्रिया, प्रौद्योगिकी और लोगों) द्वारा सर्वोत्तम प्रथाओं हेतु एक आश्वासन रूपरेखा का सृजन।

- 3) एक सुरक्षित साइबरस्पेस पारिस्थितिकी तंत्र को सुनिश्चित करने के लिए नियामक रूपरेखा को मजबूत बनाना।
- 4) आईसीटी मूल संरचना पर खतरों के विषय में सामरिक सूचना प्राप्त करने हेतु राष्ट्रीय और क्षेत्रगत स्तर पर 24 x 7 प्रक्रियाओं का संवर्धन और मूजन, निवारक, सुरक्षा, प्रतिक्रिया और राहत कार्यों के माध्यम से प्रभावी पूर्वानुमान, प्रतिक्रिया, संकल्प और संकट प्रबंधन के लिए परिदृश्यों का निर्माण।
- 5) राष्ट्रीय महत्वपूर्ण सूचना मूल संरचना संरक्षण केंद्र (एनसीआईआईपीसी) के 24 x 7 प्रचालन द्वारा राष्ट्र की महत्वपूर्ण सूचना की मूल संरचना की सुरक्षा और लचीलापन, बढ़ाना और सूचना संसाधनों के डिजाइन, अधिग्रहण, विकास, उपयोग, और प्रचालन से संबंधित सुरक्षा प्रथाओं का अधिदेश।
- 6) सीमा प्रौद्योगिकी अनुसंधान, समाधान उन्मुख अनुसंधान, अवधारणा के प्रमाण, पायलट विकास, संक्रमण, प्रसार और व्यावसायीकरण के माध्यम से उपयुक्त स्वदेशी सुरक्षा तकनीकों का विकास करना जिससे सामान्य तौर पर सुरक्षित आईसीटी उत्पादों / प्रक्रियाओं की बड़े पैमाने पर तेनाती और विशेष रूप से राष्ट्रीय सुरक्षा आवश्यकताओं को संबोधित किया जा सके।
- 7) इन उत्पादों की सुरक्षा के परीक्षण और सत्यापन के लिए मूल संरचनात्मक सुविधाओं की स्थापना द्वारा आईसीटी उत्पादों और सेवाओं की अखंडता की दृश्यता में सुधार लाना।
- 8) अगले 5 वर्षों में साइबर सुरक्षा में 500,000 कुशल पेशेवरों का क्षमता निर्माण, कौशल विकास और प्रशिक्षण के माध्यम से एक कार्यबल का मूजन।
- 9) मानक सुरक्षा प्रथाओं और प्रक्रियाओं को अपनाने के लिए व्यवसायों में वित्तीय लाभ प्रदान करना।
- 10) सूचना के संसाधन, हैडलिंग, भंडारण और पारगमन के दौरान इस सुरक्षा ताकि नागरिक डेटा की गोपनीयता की रक्षा के साथ और साइबर अपराध या डेटा चोरी के कारण आर्थिक नुकसान को किया जा सके।
- 11) साइबर अपराध की प्रभावी रोकथाम, जांच और अभियोजन तथा उपयुक्त विधायी हस्तक्षेप के माध्यम से कानून प्रवर्तन क्षमताओं में वृद्धि।
- 12) साइबर सुरक्षा तथा गोपनीयता की एक संस्कृति के मूजन से जिम्मेदार प्रयोक्ता व्यवहार और कार्यों को सक्षम बनाने की एक प्रभावी संचार और बढ़ावा देने की कार्यनीति तैयार करना।
- 13) साइबर स्पेस की सुरक्षा बढ़ाने के लिए तकनीकी और प्रचालन सहयोग और योगदान के माध्यम से प्रभावी सार्वजनिक निजी भागीदारी और सहयोगात्मक कार्यों को विकसित करना।
- 14) आपसी समझ को बढ़ावा देने और साइबर स्पेस की सुरक्षा के कारणों को उन्नत बनाने के लिए संबंधों द्वारा वैश्विक सहयोग बढ़ाना।

IV. कार्य नीतियां

क. एक सुरक्षित साइबर पारिस्थितिकी तंत्र का निर्माण

- 1) देश में साइबर सुरक्षा से संबंधित सभी मामलों के समन्वय के लिए स्पष्ट रूप से परिभाषित भूमिकाओं और जिम्मेदारियों के साथ, एक राष्ट्रीय नोडल एजेंसी नामित करना।
- 2) साइबर सुरक्षा प्रयासों और पहलों के लिए जिम्मेदार मुख्य सूचना सुरक्षा अधिकारी के रूप में वरिष्ठ प्रबंधन के एक सदस्य को नामित करने के लिए निजी और सार्वजनिक सभी संगठनों को प्रोत्साहित करना।
- 3) सभी संगठनों को अपनी व्यापार की योजना के साथ एकीकृत सूचना सुरक्षा नीतियों को विकसित करने और अंतरराष्ट्रीय सर्वोत्तम प्रथाओं के अनुसार ऐसी नीतियों को लागू करने के लिए प्रोत्साहित करना। इन नीतियों में सुरक्षित सूचना प्रवाह (प्रक्रिया, हैडलिंग, भंडारण और पारगमन) के मानक और तंत्र, संकट प्रबंधन योजना, सक्रिय सुरक्षा आसन मूल्यांकन और विधिविज्ञान की दृष्टि से सूचना मूलसंरचना शामिल होना चाहिए।
- 4) सभी संगठनों द्वारा यह सुनिश्चित करना कि उनके पास साइबर सुरक्षा प्रयास को लागू करने के लिए और साइबर घटनाओं से उत्पन्न आपात प्रतिक्रिया की बैठक के लिए एक विशिष्ट बजट उद्दिष्ट किया गया है।
- 5) संस्थाओं को साइबर सुरक्षा के संबंध में मूल संरचना स्थापित करने के लिए प्रोत्साहित करने, मजबूत और उन्नत बनाने के लिए वित्तीय योजनाएं और प्रोत्साहन प्रदान करना।
- 6) प्रौद्योगिकी विकास, साइबर सुरक्षा अनुपालन और सक्रिय कार्यों को प्रोत्साहन देने के माध्यम से साइबर घटनाओं की घटना और पुनरावृत्ति को रोकना।

- 7) बहाली के प्रयामों में महयोग के लिए और माइवर सुरक्षा की घटनाओं की पहचान और प्रतिक्रिया के लिए जानकारी वांटने के लिए एक तंत्र स्थापित करना ।
- 8) मंथ्याओं को बरगेसेमंद आईसीटी उत्पादों की खरीद के लिए दिशा निर्देशों को अपनाने के लिए प्रोत्साहित करना और सुरक्षा निहितार्थ वाले देश में ही निर्मित आईसीटी उत्पादों की खरीद की म्विधा प्रदान करना ।

ख. एक आश्वासन रूपरेखा बनाना

- 1) मूचना सुरक्षा और अनुपालन में वैश्विक सर्वोत्तम प्रथाओं को अपनाने का बहावा देना और डम प्रकार माइवर सुरक्षा प्रथा को बहावा देना ।
- 2) माइवर सुरक्षा सर्वोत्तम प्रथाओं, मानकों और दिशा निर्देशों (उदाहरण के लिए आईएमओ 27001 आईएमएमएम प्रमाणीकरण, आईएम प्रणाली परीक्षण, प्रवेश परीक्षण / सुभेद्यता आकलन, अनुप्रयोग सुरक्षा परीक्षण, वेब सुरक्षा परीक्षण) अनुपालन के अनुरूपता मूल्यांकन और प्रमाणीकरण के लिए मूल संरचना रूपरेखा तैयार करना ।
- 3) मभी मंथ्याओं द्वारा सरकार के अंदर और बाहर और महत्वपूर्ण क्षेत्रों में विघटन के खतरे को कम करने तथा सुरक्षा व्यवस्था में सुधार लाने के लिए औपचारिक जोखिम मूल्यांकन और जोखिम प्रबंधन, व्यापार निरंतरता प्रबंधन और माइवर संकट योजना प्रबंधन में वैश्विक सुरक्षा की सर्वोत्तम प्रथाओं के कार्यान्वयन को मक्षम बनाना ।
- 4) सुरक्षा के अनुरूप संरक्षण उपायों के लिए जोखिमकी अवधारणा के संबंध में इकाई स्तर पर मूचना मूल संरचना म्विधाओं और परिमंपत्तियों की पहचान और वर्गीकृत करना ।
- 5) वैश्विक सर्वोत्तम प्रथाओं पर आधरित सुरक्षित अनुप्रयोग / माॉफ्टवेयर विक्रम की प्रक्रिया को प्रोत्साहित करना ।
- 6) माइवर सुरक्षा पर सर्वोत्तम प्रथाओं, मानकों और दिशा निर्देशों के अनुपालन के आवधिक गत्यापन के लिए अनुरूपता मूल्यांकन रूपरेखा बनाना ।
- 7) मभी मंथ्याओं को समय - समय पर आईटी सिस्टम और नेटवर्क में तकनीकी और प्रचालन सुरक्षा नियंत्रण उपायों की पर्याप्तता और प्रभावशीलता के लिए परीक्षण और मूल्यांकन करने के लिए प्रोत्साहित करना ।

ग. खूले मानकों को प्रोत्साहित करना

- 1) विभिन्न उत्पादों या सेवाओं के बीच अंतर और डेटा विनिमय की म्विधा के लिए खूले मानकों के इस्तेमाल को प्रोत्साहित करना ।
- 2) खूले मानकों के आधार पर परीक्षण और प्रमाणित आईटी उत्पादों की उपलब्धता बढाने के लिए सरकार और निजी क्षेत्र के एक संघ को बहावा देना ।

घ. विनियामक ढांचे को मजबूत बनाना

- 1) माइवर स्पेस में प्रौद्योगिकी संबंधी विक्रमों में उत्पन्न चुनौतियों माइवर सुरक्षा को संबोधित करने के लिए एक गतिशील कानूनी रूपरेखा को विक्रमित करना और इसकी आवधिक ममीक्षा (जैसे क्लाउड कंप्यूटिंग, मोबाइल कंप्यूटिंग, एन्क्रिप्टेड सेवाओं और सोशल मीडिया) और इंटरनेट शरामन में संबधित सहित अंतरराष्ट्रीय रूपरेखा के साथ इनका सुमेलन ।
- 2) विनियामक रूपरेखा के संबंध में मूचना की मूलसंरचना की सुरक्षा की पर्याप्तता और प्रभावशीलता की आवधिक लेखा परीक्षा और मूल्यांकन का अधिदेश, जैसा उपयुक्त हो ।
- 3) विनियामक रूपरेखा के बारे में सक्षमता, शिक्षित और जागरूकता लाने की म्विधा ।

ड. सुरक्षा खतरे से पूर्व चेतावनी, सुभेद्यता प्रबंधन और सुरक्षा खतरों पर प्रतिक्रिया के लिए तंत्र बनाना

- 1) मौजूदा और संभावित माइवर सुरक्षा खतरों की आवश्यक स्थितिजन्य परिदृश्य में उत्पन्न और बैयक्तिक मंथ्याओं द्वारा सक्रिय, निवारक और सुरक्षात्मक कार्यों के लिए समय पर जानकारी साझा करने के लिए राष्ट्रीय स्तर की प्रणालियां, प्रक्रियाएं, संरचना और तंत्र बनाना ।
- 2) माइवर सुरक्षा आपातकालीन प्रतिक्रिया और संकट प्रबंधन के लिए मभी प्रयामों के समन्वय के लिए एक नोडल एजेंसी के रूप में कार्य करने के लिए एक 24x7 राष्ट्रीय स्तर के कंप्यूटर आपातकालीन प्रतिक्रिया दल मर्ट इन प्रचालित करना। मर्ट इन क्षेत्रीय मर्ट के निर्माण और प्रचालन माइवर संकट की स्थिति में निपटने में संचार और समन्वय कार्यों की म्विधा प्रदान करने के लिए एक केंद्रीय संगठन के रूप में कार्य करेगा ।

- 3) घटना की प्रभावी प्रतिक्रिया और संकल्प और साइबर संकट प्रबंधन के लिए संबंधित क्षेत्रों के अंदर सभी समन्वय और संचार कार्यों के लिए 24 x 7 क्षेत्रीय सर्ट को प्रचालित करना।
- 4) महत्वपूर्ण राष्ट्रीय प्रक्रियाओं को प्रभावित करने वाली या राष्ट्रीय, क्षेत्रीय और साथ ही इकाई के स्तर पर अच्युत तरह से समन्वित, बहु विषयक दृष्टिकोण के माध्यम से, राष्ट्र की सार्वजनिक सुरक्षा और सुरक्षा को खतरे में डालने वाली से जुड़ी घटनाओं से निपटने के लिए साइबर साइबर आपदा प्रबंधन योजना को कार्यान्वित करना।
- 5) साइबर सुरक्षा की घटनाओं की रोकथाम और इनसे निपटने के लिए राष्ट्रीय, क्षेत्रीय और इकाई के स्तर पर आपातकालीन तैयारियों के स्तर का आकलन के लिए नियमित रूप से साइबर सुरक्षा अभ्यास और अभ्यास आयोजित करना और सुविधा प्रदान करना।

च. ई - शासन सेवाओं को सुरक्षित बनाना

- 1) देश में वैश्विक सुरक्षा सर्वोत्तम प्रथाओं, व्यापार निरंतरता प्रबंधन और सभी ई प्रशासन की पहल के लिए साइबर संकट प्रबंधन योजना के कार्यान्वयन के अधिदेश से विघटन के खतरे को कम करना और सुरक्षा व्यवस्था में सुधार।
- 2) सरकार के अंदर भरोसेमंद संचार और लेनदेन के लिए सार्वजनिक कुंजी मूल संरचना (पीकेआई) के व्यापक उपयोग को प्रोत्साहित करना।
- 3) ई शासन प्रयास में सहायता देने के लिए सूचना सुरक्षा पेशेवरों/ संगठनों को नियुक्त करना और सर्वोत्तम सुरक्षा प्रथाओं के लिए अनुरूपता सुनिश्चित करना।

छ. महत्वपूर्ण सूचना मूल संरचना का संरक्षण और लचीलापन

- 1) इकाई स्तर पर महत्वपूर्ण सूचना मूल संरचना के संरक्षण और व्यापार की योजना के साथ एकीकरण के लिए एक योजना विकसित करना और ऐसी योजना को लागू करना। योजनाओं में सुरक्षित सूचना प्रवाह (प्रक्रिया में, हैडलिंग, भंडारण और पारगमन में), दिशा निर्देश और मानक, संकट प्रबंधन योजना, सक्रिय सुरक्षा आसन मूल्यांकन और विधि विज्ञान की दृष्टि से सक्षम सूचना की मूलसंरचना में शामिल होंगे।
- 2) देश में महत्वपूर्ण सूचना मूल संरचना की सुरक्षा के लिए नोडल एजेंसी के रूप में कार्य करने के लिए एक राष्ट्रीय महत्वपूर्ण सूचना मूल संरचना संरक्षण केंद्र (एनसीआईआईपीसी) 24 x 7 प्रचालन।
- 3) महत्वपूर्ण सूचना मूल संरचना के संरक्षण के लिए योजना के आधार पर पहचान, प्राथमिकता, मूल्यांकन, सुधार, और महत्वपूर्ण मूल संरचना और प्रमुख संसाधनों के संरक्षण की सुविधा देना।
- 4) सभी महत्वपूर्ण क्षेत्र की संस्थाओं द्वारा विघटन के खतरे को कम करने के लिए और सुरक्षा व्यवस्था में सुधार के लिए वैश्विक सुरक्षा सर्वोत्तम प्रथाओं, व्यापार निरंतरता प्रबंधन और साइबर संकट प्रबंधन योजना के कार्यान्वयन का अधिदेश।
- 5) मान्य और प्रमाणित आईटी उत्पादों के उपयोग को प्रोत्साहित करना और उचित रूप में अधिदेश देना।
- 6) एक आवधिक आधार पर महत्वपूर्ण सूचना मूल संरचना का सुरक्षा परीक्षण अधिदेश प्रदान करना।
- 7) सीआईएसओ/सीएसओ से आरंभ करते हुए महत्वपूर्ण जानकारी बुनियादी सुविधाओं के प्रचालन में शामिल लोगों के लिए सभी सुरक्षा भूमिकाओं के लिए प्रमाणन अधिदेश प्रदान करना।
- 8) सर्वोत्तम वैश्विक प्रथाओं पर आधारित सुरक्षित अनुप्रयोग/ सॉफ्टवेयर विकास (डिजाइन से अंत के) प्रक्रिया के लिए अधिदेश प्रदान करना

ज. साइबर सुरक्षा के क्षेत्र में अनुसंधान एवं विकास का संवर्धन

- 1) संक्षिप्त अवधि, मध्यम अवधि और लंबी समय अवधि के लक्ष्यों के विकास सभी पहलुओं को संबोधित करने के उद्देश्य से अनुसंधान एवं विकास कार्यक्रम। अनुसंधान एवं विकास कार्यक्रमों में भरोसेमंद प्रणालियों, उनके परीक्षण, तैनाती और जीवन चक्र के दौरान रखरखाव के सभी पहलुओं को संबोधित किया जाएगा तथा आधुनिकतम सुरक्षा प्रौद्योगिकियों पर अनुसंधान एवं विकास भी शामिल होगा।
- 2) निर्यात बाजार के लिए साइबर सुरक्षा की चुनौतियों और लक्ष्य की एक व्यापक रेंज को पूरा करने के लिए लागत प्रभावी, आवश्यकतानुसार स्वदेशी सुरक्षा समाधान का उत्पादन करने के लिए अनुसंधान और विकास को प्रोत्साहित करना।
- 3) सार्वजनिक और निजी क्षेत्रों में उपयोग के लिए बाणिज्यिक उत्पादों और सेवाओं में संक्रमण, प्रसार और अनुसंधान एवं विकास के परिणामों के व्यावसायीकरण की सुविधा प्रदान करना।

2893 45/13-2

- 4) साइबर स्पेस की सुरक्षा के मुद्दे के लिए सामरिक महत्व के क्षेत्रों में उत्कृष्टता केन्द्रों की स्थापना करना ।
- 5) सीमावर्ती प्रौद्योगिकियों और समाधान उन्मुख अनुसंधान के क्षेत्र में उद्योग और शिक्षा के साथ संयुक्त अनुसंधान एवं विकास परियोजनाओं में सहयोग करना ।

झ. आपूर्ति शृंखला के जोखिम कम करना

- 1) वैश्विक मानकों और प्रथाओं के अनुसार परीक्षण मूल संरचना और आईटी सुरक्षा उत्पाद मूल्यांकन सुविधाओं का सृजन और अनुरक्षण तथा अनुपालन सत्यापन ।
- 2) उत्पाद/प्रणाली विक्रेताओं और सेवा प्रदाताओं के साथ भरोसेमंद संबंधों का निर्माण से प्रत्येक बिंदु पर आपूर्ति शृंखला सुरक्षा दृश्यता में सुधार लाना ।
- 3) सूचना प्रौद्योगिकी (उत्पाद, प्रणाली या सेवाओं) से संबंधित आपूर्ति शृंखला जोखिमों के प्रबंधन के लिए संगठनों/निकायों के बीच धमकी, सुभेद्यताओं और सुरक्षा संबंधी उल्लंघन के परिणामों के प्रति जागरूकता पैदा करना ।

ञ. मानव संसाधन विकास

- 1) देश की साइबर सुरक्षा की जरूरत का समर्थन और क्षमता निर्माण करने के लिए औपचारिक और अनौपचारिक दोनों क्षेत्रों में शिक्षा और प्रशिक्षण कार्यक्रमों को बढ़ावा देना ।
- 2) सार्वजनिक निजी साझेदारी व्यवस्था के माध्यम से देश भर में साइबर सुरक्षा प्रशिक्षण के मूलसंरचनात्मक रूपरेखा की स्थापना करना ।
- 3) प्रमुख क्षेत्रों में जागरूकता और कौशल विकास के लिए साइबर सुरक्षा संकल्पना प्रयोगशाला स्थापित करना ।
- 4) कानून प्रवर्तन एजेंसियों के लिए क्षमता निर्माण के लिए संस्थागत तंत्र स्थापित करना ।

ट. साइबर स्पेस की सुरक्षा के प्रति जागरूकता पैदा करना

- 1) साइबर स्पेस की सुरक्षा पर एक व्यापक राष्ट्रीय जागरूकता कार्यक्रम को बढ़ावा देना और आरंभ करना ।
- 2) नागरिकों को साइबर सुरक्षा की चुनौतियों के बारे में पता लगाने में मदद करने के लिए इलेक्ट्रॉनिक मीडिया के माध्यम से सुरक्षा साक्षरता जागरूकता और प्रचार अभियान का रखरखाव ।
- 3) साइबर सुरक्षा कार्यशालाएं/सेमिनार और प्रमाणन आयोजित करना, समर्थन देना और सक्षम बनाना ।

ठ. प्रभावी सार्वजनिक निजी भागीदारी का विकास

- 1) साइबर सुरक्षा के क्षेत्र में सामान्य रूप से और महत्वपूर्ण सूचना महत्वपूर्ण मूल संरचना की सुरक्षा में विशेष रूप से साइबर खतरों, सुभेद्यताओं, उल्लंघनों, संभावित सुरक्षा उपायों, और सर्वोत्तम प्रथाओं को अपनाने से संबंधित कार्यों के लिए निजी क्षेत्र सहित हितधारक संस्थाओं के बीच सहयोग और सहयोग की सुविधा देना ।
- 2) सभी संगत पणधारकों के साथ सहयोग और नियोजन के लिए मॉडल बनाना।
- 3) साइबर सुरक्षा नीति आदानों, चर्चा और विचार विमर्श के लिए एक विचार समूह बनाना ।

ड. जानकारी साझा करना और सहयोग

- 1) अन्य देशों के साथ साइबर सुरक्षा के क्षेत्र में द्विपक्षीय और बहुपक्षीय संबंधों को विकसित करना ।
- 2) सुरक्षा एजेंसियों, प्रमाणपत्र, रक्षा एजेंसियों और बलों, कानून प्रवर्तन एजेंसियों और न्यायिक व्यवस्था के बीच राष्ट्रीय और वैश्विक सहयोग बढ़ाना ।
- 3) महत्वपूर्ण सूचना मूल संरचना सहित प्रणालियों की प्राप्ति और लचीलेपन के प्रयासों को सुविधाजनक बनाने लिए उद्योग के साथ तकनीकी और प्रचालन पक्षों से संबंधित बातचीत के तंत्र का सृजन ।

ढ. कार्यान्वयन के लिए प्राथमिकता परक पहल (प्रयास)

नीति के कार्यान्वयन के लिए एक प्राथमिकता परक पहल को अपनाना जिससे कि पहली बार में ही सर्वाधिक महत्वपूर्ण क्षेत्रों का समाधान किया जा सके ।

V. नीति का प्रचालन

इस नीति को साइबर स्पेस की सुरक्षा की चुनौतीपूर्ण आवश्यकताओं का पता लगाने के लिए उपयुक्त विभिन्न स्तरों जैसे राष्ट्रीय, क्षेत्रीय, राज्य, मंत्रालय, विभाग और उद्यम के रूप में विस्तृत दिशानिर्देश और योजनाओं की कार्रवाई के माध्यम से प्रचालित किया जाएगा।

जे. सत्यनारायण, सचिव

MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY
(Department of Electronics and Information Technology)

NOTIFICATION

New Delhi, the 2nd July, 2013

Subject : Notification on National Cyber Security Policy-2013 (NCSP-2013) National Cyber Security Policy-2013 (NCSP-2013)

F. No. 2(35)/2011-CERT-In.—Preamble

1. Cyberspace¹ is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking/ payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate/ private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation and inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust and confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can

¹ISO / IEC 27032-2012

mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a **National Cyber Security Policy**, with an integrated vision and a set of sustained and coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government and non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems and networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public and private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

- ✓ To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

- 1) To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- 2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology and people).
- 3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.
- 4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
- 5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.
- 6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.
- 7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing and validation of security of such products.
- 8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.
- 9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

- 10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.
- 11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.
- 12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.
- 13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.
- 14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

15) Strategies

A. Creating a secure cyber ecosystem

- 1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.
- 2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.
- 3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage and transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- 4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.
- 5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.
- 6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.
- 7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.
- 8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

- 1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.
- 2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing/Vulnerability assessment, application security testing, web security testing).
- 3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.
- 4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.
- 5) To encourage secure application/software development processes based on global best practices.
- 6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

2893 अ/ 13-3

- 7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

- 1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.
- 2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

- 1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.
- 2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.
- 3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

- 1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
- 2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.
- 3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response and resolution and cyber crisis management.
- 4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.
- 5) To conduct and facilitate regular cyber security drills and exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

- 1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.
- 2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.
- 3) To engage information security professionals/organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

- 1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage and transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- 2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.
- 3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

- 4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.
- 5) To encourage and mandate as appropriate, the use of validated and certified IT products.
- 6) To mandate security audit of critical information infrastructure on a periodic basis.
- 7) To mandate certification for all security roles right from CISO/CSO to those involved in operation of critical information infrastructure.
- 8) To mandate secure application/software development process (from design through retirement) based on global best practices.

H. Promotion of Research and Development in cyber security

- 1) To undertake Research and Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research and Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.
- 2) To encourage Research and Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.
- 3) To facilitate transition, diffusion and commercialisation of the outputs of Research and Development into commercial products and services for use in public and private sectors.
- 4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.
- 5) To collaborate in joint Research and Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

- 1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.
- 2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.
- 3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

- 1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.
- 2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.
- 3) To establish cyber security concept labs for awareness and skill development in key areas.
- 4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

- 1) To promote and launch a comprehensive national awareness program on security of cyberspace.
- 2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.
- 3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

- 1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in

particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

- 2) To create models for collaborations and engagement with all relevant stakeholders.
- 3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

- 1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.
- 2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.
- 3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

J. SATYANARAYANA, Secy.