संख्याः-845/78-1-2024-1099/87/2024

प्रेषक,

अनिल कुमार सागर,
प्रमुख सचिव,
उ0प्र0 शासन।

सेवा में,

समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव,
उ०प्र० शासन।

आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-1 **लखनऊःदिनांकः 29 मई,2024**

विषयः- विभागों में Critical Information Infrastructure (CII) का चिन्हांकन किये जाने के सम्बन्ध में।

महोदय,

उपर्युक्त विषयक के संबंध में अवगत कराना है कि साइबर सुरक्षा की दृष्टि से Critical Information Infrastructure (CII) अत्यन्त संवेदनशील है, जिसके कारण इस पर साइबर हमलों की आशंका निरन्तर बनी रहती है। साइबर हमला होने की दशा में प्रदेश/विभाग को निम्नवत् गंभीर दुष्परिणाम हो सकते हैः-

1. विभिन्न विभागों की होस्टेड एप्लीकेशन का परिचालन बाधित होगा।
2. संवेदनशील सरकारी डाटा की सुरक्षा का जोखिम बढ़ेगा।
3. राजस्व हानि होने की संभावना बढ़ेगी।
4. आम जनमानस का सरकारी संस्था के प्रति विश्वास पर नकारात्मक प्रभाव पड़ेगा।
5. कानूनी एवं विनियामक दुष्परिणाम होंगे।

2- अवगत कराना है कि भारत सरकार द्वारा महत्वपूर्ण / संवेदनशील डाटा तथा एप्लीकेशनन्स् की सुरक्षा की दृष्टिगत इन्फॉरमेशन सिक्योरिटी एक्ट 2000 की धारा 70ए के अन्तर्गत NCIIPC संस्था का गठन किया गया है, जिसे Critical Information Infrastructure के संरक्षण के सम्बन्ध में राष्ट्रीय नोडल एजेंसी के रूप में नामित किया गया गया है। NCIIPC ने "Critical Information Infrastructure Security Exercise (CII SECEX 2024)" में सात सेक्टर (1. Transport 2. Health 3. Telecom 4. Government 5. Power & Energy 6. Banking, Financial Services & insurance 7. Strategic & Public Enterprises) को Critical Infrastructure के रूप में चिन्हित किया है, जिसमें "Government" भी एक महत्वपूर्ण सेक्टर है।

3- उक्त के दृष्टिगत साइबर अपराधों व साइबर सुरक्षा विषयक स्टेक होल्डर्स डायलॉग की पुर्नसमीक्षा तथा भविष्य पर विचार किये जाने हेतु मुख्य सचिव, उ०प्र० शासन की अध्यक्षता में दिनांक 04 अप्रैल, 2024 को समीक्षा बैठक (कार्यवृत्त संलग्न (संलग्नक-1)) आहूत की गयी। कार्यवृत्त के बिन्दु सं0-4 के अनुपालन में यह अपेक्षा है कि अपने विभाग में CII का पूर्ण चिन्हांकन कर उसकी सुरक्षा सुनिश्चित करने हेतु अपने विभाग के Chief Information

Security Officer (CISO) को निर्देशित किया जाये एवं उसकी सूची आई०टी० एवं इलेक्ट्रानिक्स विभाग, उ०प्र० शासन को उपलब्ध कराया जाये। CII के चिन्हांकन हेतु National Critical Information Infrastructure Protection Centre (NCIIPC), भारत सरकार द्वारा जारी गाइडलाईन्स संलग्न (संलग्नक-2) है।

5- इस सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि प्रश्नगत प्रकरण में कृपया अपने-अपने विभागों में उपरोक्तानुसार आवश्यक कार्यवाही सुनिश्चित कराने का कष्ट करें।

<u>संलग्नकः यथोक्त।</u>

भवदीय,

Digitally signed by अखिल कुमार सागर
(अखिल कुमार सागर)
प्रमुख सचिव।
Date: 27-05-2024 13:20:34
Reason: Approved

<u>पृ0 संख्या-845(1)/78-1-2024, तद्‌दिनांक</u>

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषितः-

1-निजी सचिव, मुख्य सचिव, उ०प्र० शासन।

2-निजी सचिव, अपर मुख्य सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।

3-पुलिस महानिदेशक, उ०प्र० ।

4-निजी सचिव प्रमुख सचिव, नियोजन विभाग, उ०प्र० शासन।

5-राज्य सूचना विज्ञान अधिकारी, एन०आई०सी०, लखनऊ।

6-प्रबन्ध निदेशक, उत्तर प्रदेश डेवलपमेन्ट सिस्टम्स् कारपोरेशन लिमिटेड (यू०पी०डेस्को), उ०प्र०।

7-राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स, उ.प्र., अपट्रान बिल्डिंग, गोमती नगर, लखनऊ।

8-स्टेट, चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर (सी०आई०एस०ओ०), उ०प्र०।

9-समस्त विभागीय, चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर (सी०आई०एस०ओ०), उ०प्र०।

10-हेड, एस.ई.एम.टी., उ०प्र०।

11. गार्ड फाइल ।

आज्ञा से,

(नेहा जैन)

विशेष सचिव।

साइबर अपराधों व साइबर सुरक्षा विषयक स्टेकहोल्डर्स डायलॉग की पुनर्समीक्षा तथा भविष्य की रणनीति पर विचार करने हेतु मुख्य सचिव, उ0प्र0 शासन की अध्यक्षता में दिनांक 04.04.2024 को अपराह्न 6.30 बजे, आहूत प्रस्तुतीकरण बैठक के सम्बन्ध में।

उक्त आहूत प्रस्तुतीकरण बैठक में निम्नलिखित अधिकारियों द्वारा प्रतिभाग किया गया:

1. श्री दीपक कुमार, अपर मुख्य सचिव, गृह एवं गोपन विभाग, उ0प्र0 शासन।
2. श्री प्रशान्त कुमार, पुलिस महानिदेशक, उ0प्र0।
3. श्री नवीन अरोड़ा, अपर पुलिस महानिदेशक, तकनीकी सेवायें, उ0प्र0।
4. श्री संजीव गुप्ता, सचिव, गृह एवं गोपन विभाग, उ0प्र0 शासन।
5. श्री अनुराग यादव, सचिव, नियोजन विभाग, उ0प्र0 शासन ।
6. श्री ए.वी. राजामौलि, सचिव, गृह एवं गोपन विभाग, उ0प्र0 शासन।
7. श्रीमती रूपा एम0 निदेशक, I4C, गृह मंत्रालय, भारत सरकार, नयी दिल्ली.
8. श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ0प्र0।
9. श्री योगेश कुमार, विशेष सचिव, गृह एवं गोपन विभाग, उ0प्र0 शासन।
10. श्रीमती नेहा जैन, विशेष सचिव, आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 शासन।
11. श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ0प्र0।

प्रश्नगत प्रकरण में अमर शहीद चन्द्रशेखर आजाद, प्रेक्षागृह, भू-तल, सिग्नेचर बिल्डिंग (PHQ), लखनऊ में आहूत विस्तृत प्रस्तुतीकरण निम्निलिखित विशेषज्ञों द्वारा किया गया:

क्र0सं0	वक्ता का नाम/ पदनाम	विषय
01	श्री अभिषक सिंह, अपर सचिव, एम0ई0आई0टी0, भारत सरकार।	Cyber Crime & Cyber Security Emerging Challenges & Strategy For Future
02	श्री जी. के. गोस्वामी, अपर पुलिस महानिदेशक, फारेंसिक, उ0प्र0।	Cyber Crime & Cyber Security Role of Forensic Science
03.	श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ0प्र0	Cyber Crime in Uttar Pradesh.
04	श्री सुबोध कुमार, CEO, CERT-IN, GOI	Role of CERT-IN- Incident-Response
05	श्रीमती रूपा एम0 निदेशक, I4C	Presentation of Cyber Crimes by I4C MHA
06	श्रीमती नेहा जैन, विशेष सचिव, आई0टी0 एवं	Proposed UP Cyber Security Policy, CSIRT-UP, Role of CISOs

	इलेक्ट्रानिक्स विभाग, उ0प्र0 शासन।	
07	श्री बालू केन्चप्पा, R.D., R.B.I., KANPUR	Cyber Security, Customer Education & Protection- Role of RBI

उक्त प्रस्तुतीकरण/व्याख्यान के समापन के बाद मुख्य सचिव महोदय द्वारा प्रकरण से भिज्ञ वरिष्ठ अधिकारियों के साथ की गयी बैठक में गहन विचार विमर्शोपरान्त अधोलिखित बिन्दुओं पर कार्यवाही किये जाने का निर्णय लिया गया:-

(1) प्रकरण में भारत सरकार के सूचना एवं प्रौद्योगिकी मंत्रालय के अधीन स्थापित CERT-IN की भाँति उ0प्र0 में STATE CERT (S-CERT) स्थापित किया जाये एवं जिसे National Cyber Coordination Centre (NCCC) तथा साइबर स्वच्छता केन्द्र (CSK) के साथ समन्वय का कार्य सौंपा जाए।

(कार्यवाही- आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0)

(2) प्रदेश में साइबर सुरक्षा को दृष्टिगत रखते हुए एस-सर्ट (S-CERT) की सुचारू रूप से स्थापना किये जाने तथा बेहतर क्रियाशीलता हेतु 02-02 सदस्यों की टीम (उप पुलिस महानिरीक्षक, साइबर क्राइम, व एक अन्य तथा CISO आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 व एक अन्य) संरचना व प्रणाली में उत्कृष्ट कार्य कर रहे राज्य का भ्रमण कर उन राज्यों में स्थापित एस-सर्ट (S-CERT) की संरचना एवं उपयोग में लाये जा रहे सर्वोत्तम संव्यवहारों की सूचना/जानकारी प्राप्त की जाए। इस सम्बन्ध में CERT-IN संस्था का भी भ्रमण किया जाए एवं महानिदेशक, CERT-IN से अपेक्षित सहयोग प्राप्त किया जाए।

(कार्यवाही- आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 पुलिस महानिदेशक, साइबर क्राइम, उ0प्र0,)

(3) उ0प्र0 के साथ ही राष्ट्रीय परिदृश्य पर डिजिटल क्रांति के प्रसार को देखते हुए प्रदेश में SOC (Security Operations Center) एवं NOC(Network Operations Center) की स्थापना की जाए, जिससे साइबर सुरक्षा को भविष्य की आवश्यकताओं के दृष्टिगत मजबूत बनाया जा सके।

(कार्यवाही- आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0)

(4) बैठक में साइबर सुरक्षा के दृष्टिगत उ0प्र0 राज्य में CII (Critical Information Infrastructure) का पूर्ण चिन्हांकन कर लिया जाए एवं CII की सुरक्षा किस प्रकार से सुनिश्चित की जायेगी, के सम्बन्ध में विभागों हेतु SOP (Standard Operating Procedure) बनायी जाए।

(कार्यवाही- आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0)

(5) साइबर अपराधों से सम्बन्धित अन्वेषण की कार्यवाही गुणात्मक आधार पर सम्पन्न की जा सके, इस हेतु State Forensic Lab U/S 79 A of IT Act को अधिसूचित किया जाए।

(कार्यवाही- अपर पुलिस महानिदेशक, तकनीकी सेवायें, उ0प्र0 तथा गृह (पुलिस) अनुभाग-9)

(6) साइबर सुरक्षा को मजबूत करने एवं साइबर अपराधों पर प्रभावी अंकुश लगाये जाने के दृष्टिगत प्रदेश के समस्त विभागों में सी0आई0एस0ओ0 बनाये जायें उक्त के साथ ही तकनीकी रूप से दक्ष डिप्टी सी0आई0एस0ओ0 (Deputy CISO) भी बनाया जाए। प्रत्येक विभाग में बनाये गये सी0आई0एस0ओ0 / डिप्टी सी0आई0एस0ओ0 (Deputy CISO) को स्टेट सी0आई0एस0ओ0 द्वारा प्रशिक्षित किया जाए।

(कार्यवाही- समस्त विभाग, उ0प्र0 शासन तथा आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0)

(7) प्रदेश में साइबर सुरक्षा के दृष्टिगत सी0सी0एम0यू0 (Cyber Crisis Management Unit-CCMS) स्थापित किया जाए एवं विभागवार एस0ओ0पी0 तैयार की जाए जिससे आपात साइबर अटैक आदि को यथाशीघ्र निष्प्रभावी किया जा सके।

(कार्यवाही- आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0)

(8) प्रदेश में स्टेट साइबर ऑडिट टीम (SAT- Cyber) का निर्माण किया जाय, जिसके द्वारा विभिन्न विभागों द्वारा विकसित ऐपलिकेशन्स, वेबसाइट आदि का समय-समय आकस्मिक व नियमित समयबद्ध आडिट किया जाएगा।

(कार्यवाही- आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0)

(9) मा0 उच्च न्यायालय और न्याय विभाग से परामर्श प्राप्त कर साइबर अपराधों के सम्बन्ध में ई0- एफ0आई0आर0 की व्यवस्था स्वीकृत की जाय, जिससे राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (NCRP) की शिकायतों का सुचारू रूप से त्वरित निस्तारण कर पीडित का पैसा रिफण्ड किया जा सके।

(कार्यवाही- आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 तथा गृह एवं गोपन विभाग)

(10) CYBER CRIME PREVENTION AGAINST WOMEN AND CHILDREN (CCPWC) से सम्बन्धित साफ्टवेयर का नवीनीकरण किया जाय। उक्त साफ्टवेयर के नवीनीकरण हेतु अनुमानित धन व्यवस्था रू0-1.7 करोड़ तदनुसार प्रशासकीय विभाग वित विभाग की सहमति से निर्भया निधि से सुनिश्चित करें ।

(कार्यवाही-आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0, पुलिस महानिदेशक, उ0प्र0 तथा गृह(पुलिस)अनुभाग-15)

(11) गृह मंत्रालय, भारत सरकार की हेल्पलाईन न0.- 1930 द्वारा अधिकतम फोन कॉल्स ग्रहण करने किये जाने की आवश्यकता है। उक्त हेल्पलाईन व्यवस्था के अपग्रेडेशन के लिए आवश्यक धनराशि रू0- 54 लाख की व्यवस्था समयान्तर्गत सुनिश्चित कराया जाए ।

(कार्यवाही- आई.0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 तथा पुलिस महानिदेशक, उ0प्र0)

(12) प्रदेश में साइबर क्राइम की लगातार बढ़ती हुई संख्या के दृष्टिगत प्रदेश स्तर पर सक्षम विवेचनाधिकारी पुलिस सब-इंस्पेक्टर से विवेचना कराये जाने के सम्बन्ध में U/S 78 IT ACT में संशोधन किये जाने के सम्बन्ध मे सूचना एवं प्रौद्योगिकी मंत्रालय, भारत सरकार से तदनुसार अनुरोध/ सहमति प्राप्त किये जाने हेतु आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 के माध्यम से पुलिस महानिदेशक, साइबर क्राइम आवश्यक कार्यवाही सुनिश्चित करायी जाए ।

(कार्यवाही- पुलिस महानिदेशक, उ0प्र0 एवं पुलिस महानिदेशक, साइबर क्राइम, उ0प्र0, गृह एवं गोपन विभाग)

(13) साइबर फ्रॉड के माध्यम से विभिन्न पीड़ित व्यक्तियों का एक खाते में अन्तरित धनराशि बैंकों द्वारा होल्ड करने में होने वाले विलम्ब से साइबर अपराधी द्वारा अन्तरित धनराशि का कुछ भाग अथवा अधिकांश भाग बैंकिंग परिक्षेत्र से बाहर भेज दिया जाता है । शेष जब्त धनराशि को पीड़ितों के मध्य किस अनुपात में वितरित किया जाये इस सम्बन्ध में एक स्पष्ट नीति बनाये जाने की आवश्यकता है, जिससे होल्ड की गयी धनराशि पीड़ितों के मध्य अनुपातिक वितरण किया जा सके।

(कार्यवाही- पुलिस महानिदेशक, उ0प्र0 एवं पुलिस महानिदेशक, साइबर क्राइम, उ0प्र0)

(14) साइबर सुरक्षा को मजबूत किये जाने एवं साइबर अपराधों पर प्रभावी अंकुश लगाये जाने हेतु व्यापक जन-जागरुकता एवं वितीय-साक्षरता बढ़ाये जाने के सम्बन्ध में साइबर सुरक्षा एवं साइबर अपराध के विषय को सम्बन्धित विभाग/संस्थाओं से समन्वय स्थापित कर कक्षा-6 से कक्षा-12 तक के पाठ्यक्रमों में सम्मिलित किया जाए।

(कार्यवाही- माध्यमिक शिक्षा विभाग, क्षेत्रीय मुख्यालय रिजर्व बैंक ऑफ इण्डिया, लखनऊ एवं पुलिस महानिदेशक, साइबर क्राइम, उ०प्र०)

(15) साइबर सुरक्षा को मजबूत करने हेतु प्रदेश के प्रत्येक जनपद स्थित साइबर थानों पर तैनात इच्छुक उपनिरीक्षकों को साइबर कमाण्डोज के रूप में प्रशिक्षित कराया जाए । इसके लिए प्रति वर्ष प्रति जनपद 02 प्रतिभागी प्रशिक्षित किये जायेंगे जिसमें 150-150 के दो बैच संचालित किये जायेंगे।

(कार्यवाही- पुलिस महानिदेशक, उ०प्र० तथा पुलिस महानिदेशक, साइबर क्राइम, उ०प्र०)

(16) साइबर फ्रॉड से सम्बन्धित शिकायतों पर त्वरित कार्यवाही सुनिश्चित कराये जाने हेतु बैंकों के नोडल अधिकारियों द्वारा साइबर क्राइम से सम्बन्धित शिकायतों का निस्तारण 24X7 सुनिश्चित कराया जाए, जिससे बैंको द्वारा फ्रॉड धनराशि का अन्तरण बैंकिंग परिक्षेत्र से बाहर जाने से पूर्व उक्त धनराशि को फ्रीज/होल्ड समयान्तर्गत किया जा सके ।

(कार्यवाही- पुलिस महानिदेशक, साइबर क्राइम, उ०प्र० एवं क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, लखनऊ)

(17) वित्तीय अनियमितताओं/ साइबर अपराध से सम्बन्धित प्रकरणों पर विचार-विमर्श किये जाने हेतु गठित राज्य स्तरीय समन्वय समिति (SLCC) की बैठक समय-समय पर सुनिश्चित करायी जाए ।

(कार्यवाही- **SLCC Convenor RBI** व क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, कानपुर)

(18) राज्य स्तर पर गहन विश्लेषण ईकाई (यथा I4C में कार्यरत Threat Analytics Units) का गठन कर नागरिकों को सामान्यतया प्राप्त हो रहे एस०एम०एस०, ई.मेल, वॉइस कॉल्स, अन्य संदेशों, आदि का सुव्यवस्थित संकलन करते हुए सम्भावित साइबर खतरों के विषय में पूर्वानुमान लगाकर बड़ी साइबर त्रासदी को रोकने हेतु कारगर कदम उठाया जाय।

(कार्यवाही- पुलिस महानिदेशक, उ०प्र०, पुलिस महानिदेशक, साइबर क्राइम, उ०प्र०)

बैठक सधन्यवाद सम्पन्न हुई।

Digitally Signed by दीपक कुमार
Date: 13-04-2024 19:33:19
Reason: Approved

(दीपक कुमार)
अपर मुख्य सचिव।

उत्तर प्रदेश शासन,
गृह(गोपन) अनुभाग-8
लखनऊ: दिनांक: 15 अप्रैल, 2024

संख्या एवं दिनांक तदैव।

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

1- श्री प्रशान्त कुमार, पुलिस महानिदेशक, उ.0.प्र0।

2- श्री नवीन अरोड़ा, अपर पुलिस महानिदेशक, तकनीकी सेवायें, उ०प्र०।

3- श्री संजीव गुप्ता, सचिव, गृह एवं गोपन विभाग, उ०प्र० शासन।

4- श्री अनुराग यादव, सचिव, नियोजन विभाग, उ०प्र० शासन ।

5- श्री ए.वी. राजामौलि, सचिव, गृह एवं गोपन विभाग, उ0प्र0 शासन।

6- श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ0प्र0।

7- श्री योगेश कुमार, विशेष सचिव, गृह एवं गोपन विभाग, उ0प्र0 शासन।

8- श्रीमती नेहा जैन, विशेष सचिव, आई0टी0 एवं इलेक्ट्रानिक्स विभाग, उ0प्र0 शासन।

9- श्री पवन कुमार, उप पुलिस महानिरीक्षक, साइबर क्राइम, उ0प्र0।

10- श्रीमती रूपा एम0 निदेशक, I4C

11- निजी सचिव, मुख्य सचिव, उ0प्र0 शासन।

12- निजी सचिव, अपर मुख्य सचिव, गृह एवं गोपन विभाग, उ0प्र0 शासन।

13- निजी सचिव, अपर मुख्य सचिव, बेसिक शिक्षा विभाग, उ0प्र0 शासन।

14- निजी सचिव, अपर मुख्य सचिव, वित्त विभाग, उ0प्र0 शासन।

15- निजी सचिव, अपर मुख्य सचिव, माध्यमिक शिक्षा विभाग, उ0प्र0 शासन।

16- क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, लखनऊ।

17- क्षेत्रीय निदेशक, रिजर्व बैंक ऑफ इण्डिया, कानपुर।

18- गृह (पुलिस) अनुभाग-9

19- गृह (पुलिस) अनुभाग-15

आज्ञा से,

(योगेश कुमार)
विशेष सचिव ।

GUIDELINES FOR IDENTIFICATION

OF

CRITICAL INFORMATION INFRASTRUCTURE

NATIONAL CRITICAL INFORMATION

INFRASTRUCTURE PROTECTION CENTRE (NCIIPC)

All rights reserved. No part of this document may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage or retrieval system, without permission in writing from National Critical Information Infrastructure Protection Centre (NCIIPC).

Copyright © National Critical Information Infrastructure Protection Centre

Version 1.0 : August 2019

National Critical Information Infrastructure Protection Centre (NCIIPC)
(A unit under National Technical Research Organisation)
Block III, Old JNU Campus,
New Delhi – 110067

Toll Free : 1800 1144 30
Email : helpdesk1@nciipc.gov.in
helpdesk2@nciipc.gov.in

GUIDELINES FOR IDENTIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE (CII)

Relevant Acts and Rules

1. As per IT Act 2000 (amended 2008), **Critical Information Infrastructure (CII) means '*Computer Resource, the incapacitation or destruction of which, shall have debilitating impact on National Security, Economy, Public Health or Safety*'.**

2. Section 70 of the IT Act 2000 lays down that *the appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of CII, to be a 'Protected System'.*

3. Gazette Notification G.S.R 18(E) dated 16 Jan 2014 designates the National Critical Information Infrastructure Protection Centre (NCIIPC), an organisation under the National Technical Research Organisation (NTRO), as the national nodal agency in respect of Critical Information Infrastructure Protection.

4. Gazette Notification G.S.R. 19(E) dated 16 Jan 2014 lays down the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013. Key sections of the Rules are:

   (a) Section 2(e) of the Rules lays down that *"Critical Sector" means sectors, which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health or safety.*

   (b) Section 4(3) of the Rules mandates the *identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.*

   (c) Section 4(5) of the Rules mandates that *the basic responsibility for protecting critical information infrastructure system shall lie with the agency running that critical information infrastructure.*

   (d) Section 5 of the Rules lay down the *Manner of Performing Functions and Duties* and spell out the role and responsibilities of NCIIPC. It also lays down a mechanism for prioritization of actions against threats or vulnerabilities.

5. CII is very likely to be targeted by an attacker so as to disrupt or compromise an IT-enabled capability, service or process of national importance. These capabilities and services are delivered by organizations and enterprises in the critical sectors through various Business and/or Industrial Processes, which run on the underlying Information Technology (IT) and Operation Technology (OT) systems.

6. In order to have a consistent approach for identification of CII within and across all the Critical Sectors, a set of generic guidelines are enumerated in succeeding paras.

Identification and Assessment of CII

7. Assess the criticality of the Functions and Services provided by the Organization / Entity and the magnitude of impact on National Security, National Economy, Public Health or Public Safety in case of incapacitation / destruction of its ICT infrastructure based on the following parameters: -

(a) Impact on Customers, Business & Government functions based on:-

(i) Value of all types of Transactions per day.

(ii) Total number of Transactions per day.

(iii) Number of connected Devices and Network size.

(iv) Number of Customers of different categories.

(b) Timeframe (hours / days / weeks) after which the impact level of non-availability of the ICT infrastructure will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business and Government (shorter timeframe indicates more critical).

(c) Geographical or Environmental impact, if any, of incapacitation / destruction of the underlying ICT infrastructure (area, city, district, state, region, nation-wide or even across international boundary).

(d) Level of Dependency to include:-

(i) Cascading impact of non-availability of functions and services due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other critical sectors / sub-sectors.

(ii) Dependence of essential functions and services on other critical sectors / sub-sectors.

8. If the above assessment indicates that functions and services of the organization / entity have a significant impact nationally, there is a need to evaluate various Business and/or Industrial Processes of the organization / entity from the point of view of identifying those computer resources, the incapacitation or destruction of which may have a debilitating impact on National Security, National Economy, Public Health or Public Safety. Following parameters can be considered for identification of critical business and/ or industrial processes of the organisation:-

(a) Size & Economic Value of the Business /Industrial Process based on:-

(i) Value of all types of Transactions processed per day.

(ii) Total number of Transactions processed per day.

(iii) Number of connected Devices and Network size of the Business /Industrial Process.

(iv) Number of Customers of different categories serviced.

(b) Criticality of the Business Process and estimated magnitude of impact on National Security, National Economy, Public Health, Public Safety, Customers, Business and Government in case of incapacitation/ destruction of the underlying ICT infrastructure.

(c) Timeframe (hours / days / weeks) after which the impact level of non-availability of the Business /Industrial Process will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business and Government (shorter timeframe indicates more critical).

(d) Level of Dependency.

(i) Impact of non-availability of Business /Industrial Process due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other Critical Sectors.

(ii) Dependence of the Business / Industrial Process on other critical sectors/sub sectors.

9. Based on expert judgement and estimation of the above parameters, various Business and/or Industrial Processes are then grouped as critical or non-critical. NCIIPC may be consulted for any clarification in the CII identification process. Consequently, the underlying computer resources of critical processes along with their interconnected dependencies will be categorized to be CII.

10. The appropriate government may, in consultation with NCIIPC, declare the identified CII of the concerned organization through an 'Office Memorandum'. If needed, it may further choose to declare any computer resource which directly or indirectly affects the facility of CII, to be a 'Protected System' through notification in the Official Gazette.

11. For Protected Systems as well as the declared CIIs, *'Rules for the Information Security Practices and Procedures for Protected System'*, promulgated vide Gazette Notification dated 22 May 2018 (Regd No D.L.-33004/99), shall be suitably adapted by the Information Security Steering Committee (ISSC) of the organization.