सत्यमेव जयते

महाराष्ट्र शासन

उद्योग, ऊर्जा व कामगार विभाग

दुरध्वनी क्र. : ०२२-२२८८३४११/१५
ईमेल - shraddha.kocharekar@nic.in
prafull.karekar@nic.in

मंत्रालय (मुख्य इमारत), मादाम कामा मार्ग,
हुतात्मा राजगुरु चौक, मुंबई - ४०००३२

क्रमांक:- संदर्भ-२०२१/सं.क्र.३०८/ऊर्जा-४

दिनांक: २२ मार्च, २०२१

प्रति,

१) अध्यक्ष तथा व्यवस्थापकीय संचालक,
महाराष्ट्र राज्य विद्युत निर्मिती कंपनी
मर्या.,प्रकाशगड,वांद्रे(पूर्व),मुंबई-४०० ०५१

२) अध्यक्ष तथा व्यवस्थापकीय संचालक,
महाराष्ट्र राज्य विद्युत वितरण कंपनी
मर्या.,प्रकाशगड, वांद्रे (पूर्व),
मुंबई- ४०० ०५१

३) व्यवस्थापकीय संचालक,
दि. टाटा पॉवर लि. कंपनी,
बॉम्बे हाऊस,२४ होमी मोदी स्ट्रिट,
मुंबई- ४०० ००१

४) व्यवस्थापकीय संचालक,
अदानी पॉवर महाराष्ट्र लि.
६२, मेकर चेंबर III, नरिमन पॉईट,
मुंबई- ४०० ०२१

५) महाव्यवस्थापक,
बृह्न्मुंबई विद्युत पुरवठा आणि परिवहन उपक्रम,
बेस्ट भवन, बेस्ट मार्ग, मुंबई ४०००05

६) कार्यकारी संचालक,
नॅशनल थर्मल पॉवर कार्पोरेशन लि,
समृद्ध वेंचर पार्क, एमआयडिसी,
अंधेरी- (पूर्व) मुंबई - ४०००९३

७) रत्नागिरी गॅस ॲन्ड प्रा.लि
समृद्धी वेंचर पार्क ,
५ वा मजला एमआयडीसी,मरोळ
अंधेरी (पूर्व) मुंबई - ४०००९३

विषय : श्री. आलोक कुमार, भाप्रसे, सचिव भारत सरकार, विद्युत मंत्रालय यांचे दिनांक ०८.०३.२०२१ चे पत्र.

महोदय,

श्री. आलोक कुमार, भाप्रसे, सचिव भारत सरकार, विद्युत मंत्रालय यांनी दिनांक ०८.०३.२०२१ च्या पत्रान्वये पॉवर सेक्टरवर होणाऱ्या सायबर अटॅकच्या अनुषंगाने खालील बाबींवर तात्काळ कार्यवाही करण्याचे नमूद केले आहे.:-

1. **Identification of Chief Information Security Officer (CISO) and alternate CISO and regular updation of their details on ISAC-Power portal.**
2. **Preparation of Cyber Crisis Management Plan (C-CMP) on the basis of model C-CMP circulated by their repsetive sectoral CERT and to get vetted by CERT-In. All CERTs to**

submit a soft copy of their organization C-CMP as well as Sector Specific Model C-CMP to MoP & CISO-MoP.

3. **ISO:27001 Certification/ Implementation of Information Security Management System (ISMS).**
4. **Identification of Critical Information Infrastructure (CII) in coordination with NCIIPC and CISO-MoP. The list of notified CIIs and Protected Systems to be forwarded to MoP.**
5. **Conduction cyber mock drill at regular interval in coordination with sectoral CERTs and CERT-In.**
6. **Cyber Audit as per specified periodicity from CERT-In empanelled Auditor.**
7. **Incident Reporting within specified time limit to CERT-In, sectoral CERT and CISO-MoP. Detailed report to cover incident detail, incident response and measures taken for prevention in future and leanings from incident handling.**
8. **To develop SOP based on the internationally followed best practice by power sector utilities in ensuring cyber security of CII.**
9. **A dedicated cyber security cell may be created with dedicated IT professionals.**
10. **Impart regular cyber training to IT/OT officers to create cyber awareness in the organization.**
11. **Immediate examination of the system, if it comes under cyber attack. Forensic analysis may also be carried out with the help of CERT-In and NCIIPC.**
12. **SLDCs may be advised to take extra precautions and carry out quarterly checks of their OT and IT systems.**

श्री. आलोक कुमार, भाप्रसे, सचिव भारत सरकार, विद्युत मंत्रालय यांनी उपरोक्त मुद्यांच्या अनुषंगाने तात्काळ कार्यवाही करण्याबाबतचे अवगत केले आहे जेणेकरुन पॉवर सिस्टिम चा बचाव करता येईल. उपरोक्त मुद्यांच्या अनुषंगाने कार्यवाही करुन आपला अहवाल आठ दिवसात शासनास सादर करावा, ही विनंती.

आपली विश्वासू,

(श्रध्दा कोचरेकर)

अवर सचिव, महाराष्ट्र शासन

सोबत : श्री. आलोक कुमार, भाप्रसे, सचिव भारत सरकार, विद्युत मंत्रालय यांच्या दिनांक ०८.०३.२०२१ च्या पत्राची व सहपत्राची प्रत.

आवक क्रमांक केंद्रीय २८/ऊर्जा-४
दिनांक : १९/०३/२०२१

Urgent
तातडीचे

ऊर्जा-४

Please call urgent meeting on the subject on 22/3/2021 @ 10:30

आलोक कुमार, भा.प्र.से.
सचिव
भारत सरकार
Alok Kumar, I.A.S.
Secretary
Government of India
D.O 1/2/2021/IT

सत्यमेव जयते
Ministry of Power
Shram Shakti Bhawan
New Delhi - 110001

विद्युत मंत्रालय
श्रम शक्ति भवन
नई दिल्ली–110001
Tele : 23710271/23711316
Fax : 23721487
E-mail : secy-power@nic.in
March 8, 2021

Call Director (OP) MSETCL, ED(Trans) MSETCL, CE(CA&I) MSETCL, ED (SLDC), Representative of Cyber Cell (Maharashtra), ELY Inspector etc.

Coordinate with MSETCL to organise this meeting 17/3 19/3

Dear Chief Secretary,

Power system is one of the critical infrastructures of the nation and needs to be protected from any kind of attack. Recently, attempts of cyber attacks to disrupt the power system operation have been observed by cyber security monitoring agencies of Government of India.

2. As power system is getting increasingly smarter with deployment of latest technology including ICT devices for increased automation and control in power system, challenges have become more pronounced. Cyber attackers are increasingly targeting power sector, hence, taking preventive measure and mitigating threats to protect Indian power system need special attention of all power sector stakeholders.

3. CERT-In under MeitY and NCIIPC a unit of NTRO are the national nodal agencies for responding to computer security incidents and protection of Critical Information Infrastructure (CII) respectively.

4. In order to secure power system infrastructure, MoP has set up four sectoral CERTs viz. CERT-Thermal, CERT-Hydro, CERT-Transmission and CERT-Distribution housed at NTPC, NHPC, PGCIL and CEA respectively. These CERTs coordinate with all power sector utilities in their respective sectors. MoP has also designated Chief Engineer (IT), CEA as Chief Information Security Officer (CISO- MoP) to coordinate with all sectoral CERTs. The contact details of CISO and nodal officer of the sectoral CERTs are placed at Annexure-I.

5. Following activities are strictly to be carried out/complied at utility level for securing Power System Infrastructure: -

(i) Identification of Chief Information Security Officer (CISO) and alternate CISO and regular updation of their details on ISAC-Power portal.

(ii) Preparation of Cyber Crisis Management Plan (C-CMP) on the basis of model C-CMP circulated by their respective sectoral CERT and to get vetted by CERT-In. All CERTs to submit a soft copy of their organization C-CMP as well as Sector Specific Model C-CMP to MoP & CISO-MoP.

(iii) ISO:27001 Certification/ Implementation of Information Security Management System (ISMS).

(iv) Identification of Critical Information Infrastructure (CII) in coordination with NCIIPC and CISO-MoP. The list of notified CIIs and Protected Systems to be forwarded to MoP.

(v) Conducting cyber mock drill at regular interval in coordination with sectoral CERTs and CERT-In.

(vi) Cyber Audit as per specified periodicity from CERT-In empanelled Auditor.

अ.स.-व-OSD.
ह्रो.
19/03/2021

9
18/3

~~Atmatr~~
क्रद (श्री [illegible])

४७
/03/21

RIGHT TO INFORMATION

मुख्य सचिव
महाराष्ट्र शासन

प्र.स.(ऊर्जा)

Contd/........

स्वच्छ भारत
एक कदम स्वच्छता की ओर

from pre-page:

(vii) Incident Reporting within specified time limit to CERT-In, sectoral CERT and CISO-MoP. Detailed report to cover incident detail, incident response and measures taken for prevention in future and leanings from incident handling.

(viii) To develop SOP based on the internationally followed best practice by power sector utilities in ensuring cyber security of CII.

(ix) A dedicated cyber security cell may be created with dedicated IT professionals.

(x) Impart regular cyber training to IT/OT officers to create cyber awareness in the organization.

(xi) Immediate examination of the system, if it comes under cyber attack. Forensic analysis may also be carried out with the help of CERT-In and NCIIPC.

(xii) SLDCs may be advised to take extra precautions and carry out quarterly checks of their OT and IT systems.

6. The latest status of CISO, C-CMP, CII and ISMS/ISO:27001 shared by power utilities of your State/UT with their sectoral CERTs is also enclosed as Annexure-II.

7. I request you to instruct the concerned power sector utility of your State/UT to coordinate with sectoral CERTs, CERT-In and NCIIPC for implementation of measures mentioned above to prevent any cyber-attack for ensuring cyber security of power system. I also request you to take regular review at your level to assess the preparedness of Power utilities in your State to deal with cyber threats. Compliance of steps listed in para 5 above may kindly be ensured. I will much appreciate your response within a fortnight.

Regards

Yours sincerely,

(Alok Kumar)

Encl : as above

Chief Secretary of all States/UTs

All Administrators of UTs

All Advisers to the Administrators of UTs