Making India's Advanced Metering Infrastructure Resilient

Analysis from a Cyber Security Perspective

Dhruvak Aggarwal, Simran Kalra, and Shalu Agrawal

Issue Brief | March 2023

Image: IntelliSmart

Executive summary

Smart electricity meters are the last-mile technology to help make the power grid become more flexible, and financially and technically efficient. With supporting infrastructure, smart meters can instantly communicate energy consumption, power demand on/off status, tamper information, etc. to utilities, facilitating real-time power supply and demand balancing, efficient billing, and network maintenance. To realise these benefits, there is an aggressive push by the Government of India and electricity distribution companies (discoms) to install 250 million smart meters by March 2025 (MoP 2021) in place of conventional meters. However, this advanced metering infrastructure (AMI) is an information and communication technology (ICT) network operating within a network of legacy electrical and electro-mechanical machines. Like any ICT, the smart meter network carries cyber vulnerabilities that can put the physical system's confidentiality, integrity, availability and accountability at risk (Cleveland 2008). This brief explains the risks and vulnerabilities that can hinder India's smart meter and related infrastructure rollout and facilitate a deeper discourse on this critical issue.

The national critical infrastructure cyber security framework and guidelines are quite comprehensive. The *Information Technology Act, 2000* contains specific provisions for the cyber protection of critical infrastructure. The Act set up the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Indian Computer Emergency Response Team (CERT-In) to provide incident response and operational support to critical infrastructure operators. Six sectoral CERTs have been established for securing power infrastructure, with one of them dedicated to the distribution sector. Further, the standard bidding document (SBD) for advanced metering infrastructure service providers (AMISPs) notified by REC Limited specifies security-related compliances by relevant stakeholders. A detailed examination of actual contracts of 5 discoms with AMISPs and semi-structured interviews with 18 stakeholders from discoms, electricity regulators and planners, public sector undertakings, AMI vendors, and security consultants complements our review of the overall power sector cyber security policy framework.

We find that discoms currently lack the technical capacity to act on the relevant CERT's advisories. As AMI grows in size and complexity, the risks to the power system could amplify as discoms struggle to procure the tools and services to bolster their security posture due to financial constraints. The AMISP contracts contain varying compliance measures across discoms. For example, among the reviewed states, Haryana's discoms have the most comprehensive requirements for the AMISP on data retention, system security, and disaster recovery. Rajasthan's discoms have focused on the physical integrity of the system, but measures on system availability and AMISP's accountability can be improved. Discoms in Assam impose higher maximum penalties on AMISP for non-compliance with contract provisions than the other states. Furthermore, the role of discoms in AMI operation is mainly supervisory. Contractual obligations on the AMISP for training discom staff may be inadequate to equip them for situational awareness of the system, leading to principal-agent problems. The frequency of event reporting and security audits, meant to provide discoms with detailed information on the system's preparedness to deal with cyber threats, varies from monthly in Jammu & Kashmir to quarterly in Haryana to annually in Maharashtra.

> The national power sector cyber security framework is robust but discoms need support to implement it.

Based on our analysis, the theory of security economics in networked systems, and international practices in securing AMI, we make four key recommendations:

- **Harmonise critical provisions to a common baseline in all discom–AMISP contracts.** The SBD issued by REC partly resolves the issue of lack of uniform contractual obligations by providing a baseline for all contracts signed from September 2022 onwards. However, the Forum of Regulators (FoR) must work with state electricity regulators to harmonise critical contractual obligations across contracts, such as audit requirements and non-compliance penalties.
- **Resolve the information asymmetry between discoms and AMISPs.** AMISPs may have greater visibility on system security than discoms, which would restrict discoms from fulfilling their regulatory and legal obligations. A deeper technical capacity to vet and act on audit reports and dedicated teams to monitor system operations and security within discoms can help resolve information asymmetries. Further, vendors/solution providers must be held responsible for disclosing vulnerabilities in the supplied hardware and software solutions. They must also be mandated to ensure the availability of necessary update patches and mitigating controls in a time-bound manner.
- **Provide deeper technical support to discoms and develop a local ecosystem for security services.** Central government agencies such as the Central Electricity Authority and CERT-In must actively collaborate with other stakeholders in the system, such as public sector undertakings and the private sector, to create a security ecosystem. Discoms can be supported by creating a pool of qualified vendors to provide AMI-specific services, developing tools and metrics to help them assess and improve their security preparedness, real-time analytical support, and physical infrastructure such as equipment testing facilities.
- **Strengthen the provisions to hold discoms and vendors accountable for lapses in cyber security.** Efficient disclosure of relevant information helps improve accountability and therefore build resilience to future threats. Information disclosure obligations at all levels and penalties for non-disclosure play a critical role in improving the cyber security posture of ICT systems. Regulations must incorporate incentives and mandates to ensure that discoms and vendors of critical AMI components adhere to the highest standards of security and disclosure practices.

Cyber security not only requires guarding against known threats but also preparing for unknown threats. It is as much about technology as about people, processes and governance. Given that AMI is likely to witness a rapid expansion in the next few years, all key stakeholders across the various levels of government, the discoms, the regulators, and the private sector have to act in a collaborative manner to build a resilient and smart power system.

1. Introduction

India's electricity grid is undergoing a rapid transition driven by stiff decarbonisation targets and an influx of new technologies. On the supply side, India has set an ambitious goal of non-fossil fuel-based sources contributing to 50 per cent of installed capacity by 2030, a significant share of which would come from variable renewable energy (VRE, solar and wind). Demand is also likely to show unexpected variations as consumers embrace solar rooftop systems and transition to electric vehicles (EVs). The power grid needs to provide power to projected 102 million EVs via 2.9 million public charging stations under India's 2030 vision for electric mobility (Singh et al. 2020). The transition to EVs and a decarbonised grid needs to be managed even as the power distribution companies (discoms) are taking steps to improve the quality of power supply and bring down their aggregate technical and commercial (AT&C) losses, which stood at 22 per cent in the fiscal year 2020–21 (FY21) (Power Finance Corporation 2022).

Advanced metering infrastructure (AMI), or smart electricity meters and related infrastructure, can enable the transition through real-time demand and supply monitoring, network maintenance, dynamic tariffs and demand-side response (Agrawal et al. 2020). More importantly, AMI would play a crucial role in enhancing billing and revenue collection efficiency and reducing losses. Under the recently launched *Revamped Distribution Sector* (RDS) *scheme*, the Government of India (GoI) has set a target of installing 250 million smart meters (MoP 2021). As of February 2023, nearly 5.5 million smart meters have already been installed in India (NSGM 2023).

However, AMI brings with it known and unknown risks. Using smart meters and other information and communication technologies (ICT) in a network of legacy electrical and electro-mechanical machines can pose new risks to the legacy power infrastructure. The World Economic Forum (WEF) has consistently stressed that cyber threats are one of the top risks to the global economy (WEF 2020a, 2021), with "low barriers to entry for cyber threat actors, more aggressive attack methods, a dearth of cyber security professionals and patchwork governance mechanisms" identified as aggravators of risk (WEF 2022, 9). Deploying ICT within critical infrastructures such as energy and water utilities and government services makes them susceptible to cyber-attacks (Praveen 2021; Yadav 2022).

Events in India in the past two years bear this out: in August 2020, an unauthorised remote disconnection signal caused a power outage for nearly 158,000 smart meter users in Uttar Pradesh (Mishra 2020); in March 2021, investigations following an October 2020 power outage in Mumbai, Maharashtra revealed a heavy presence of malware in system operators' computer systems (Vidya 2021); since February 2021 there have been multiple reports of cyber intrusion campaigns on Indian power infrastructure (Recorded Future 2021; Dasgupta 2022).

The importance of AMI in transitioning to a low-carbon and financially sustainable power system is clear, but a safe and secure power system is an essential backbone of the Indian economy. The digitised power system must operate in a secure environment and be resilient to vulnerabilities. Poor quality hardware and software, inadequate due diligence and testing during deployment, loopholes in communication and information disclosure protocols, or a lack of accountability can expose the power infrastructure and its users to security and safety risks. Is the existing regulatory framework in India designed to identify and manage vulnerabilities and mitigate impacts effectively? What steps can be taken to make AMI rollout in India secure? This brief aims to answer these questions, preceded by a discussion of AMI, its vulnerabilities, and select examples of international practices to secure the digitised electricity grid. The study findings are based on a detailed review of secondary literature (national guidelines, model and actual contracts of 5 discoms with AMI service providers) and semi-structured interviews with 18 stakeholders from discoms, electricity regulators and planners, public sector undertakings, AMI vendors, and security consultants.

> **Using ICT such as AMI in a network of legacy electrical and electro-mechanical machines can pose new risks to the power infrastructure.**

2. AMI and its vulnerabilities

AMI is the integrated system of smart meters, data management systems, and the communication network that allows storing and processing of energy usage data (Figure 1). AMI allows two-way communication between the utility and energy meters at the consumer or the feeder levels. The utility can utilise the real-time data obtained through AMI for higher-order analysis of losses, energy consumption, billing and payment frequency, etc.

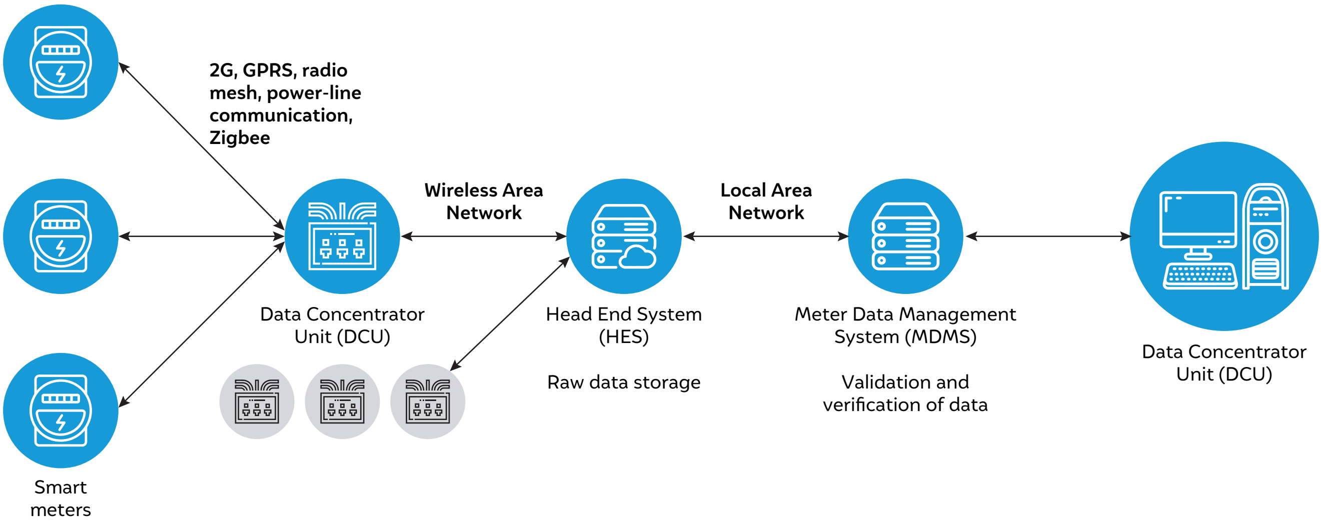
AMI consists of a network of ICT-based devices in different parts of the electricity supply chain that collect, transmit, store and analyse data in real time. Like any other ICT system, AMI carries vulnerabilities that can put users and the physical power supply network at risk. These vulnerabilities threaten the four pillars of an ICT system (Cleveland 2008):

- **Confidentiality:** Exposure of sensitive data, such as electricity consumption data recorded and transmitted by smart meters, to malicious users.[1]
- **Integrity:** Malicious users can modify data during transmission or at the transmitting and receiving terminals to produce false billing records or to mislead operators, also known as 'data spoofing'. Unauthorised control over data collector units (DCUs) and headend system (HES) might lead to the disconnection of smart meters or transmission of false pricing signals, which may seem like accidental errors if undetected.
- **Availability:** 'Invisibility' of hardware in the network can lead to broken links in the chain of communication, causing delays and interruptions in real-time services. Non-availability of system components prevents users and operators from receiving time-sensitive information and imposes losses due to service unreliability.
- **Accountability:** Detected glitches or undesirable behaviour of AMI components should be recorded and validated in real time. Incomplete logging practices and inspection mechanisms can render *ex-post* investigation of such events inconclusive, precluding accountability of responsible actors and preparedness of the system to prevent future incidents.

The vulnerabilities that threaten these pillars can creep in during design and deployment. They may arise due to

- Poor quality of hardware and software components.
- Lapses in checks and balances that ensure adherence to standards during deployment and before commissioning.
- Absence of transparency about potential system vulnerabilities.

Figure 1 AMI contains a large number of networked ICT devices at different levels of the supply chain


2G, GPRS, radio mesh, power-line communication, Zigbee
Wireless Area Network
Local Area Network
Smart meters
Data Concentrator Unit (DCU)
Head End System (HES)
Raw data storage
Meter Data Management System (MDMS)
Validation and verification of data
Data Concentrator Unit (DCU)

Source: Authors' illustration

[1] The aspect of data privacy and the rules around data sharing are not addressed in this study. 'Confidentiality' here refers only to the measures required to limit exposure of sensitive data owned by the discom and its contracted entities.

AMI faces threats at various levels of the system architecture with varying levels of adverse impacts.

Adherence to robust technology standards, communication protocols, and process guidelines becomes imperative to guard against vulnerabilities at the design and deployment stage. The Energy Expert Cyber Security Platform (EECSP) of the European Union identified the interconnectedness of technologies and market players, new and legacy system interfaces, outsourcing of infrastructure services, and human resource constraints as challenges to cyber security in the energy sector (Healey et al. 2016). The European Union Agency for Network and Information Security (ENISA 2015) classifies participants in the cyber security domain into:

- **Users**: Entities deriving value from ICT software, hardware, and services, for example, discoms, transmission utilities, power exchanges, etc.
- **Vendors**: Developers, manufacturers, and suppliers of software, hardware, and services.
- **Finders**: The community of individuals that identify and report vulnerabilities.
- **Coordinators**: Intermediaries between finders and vendors that ensure disclosure and mitigation, such as Computer Emergency Response Teams (CERTs).
- **Governments**: They can act as finders, vendors, and coordinators, as well as acquire or maintain vulnerabilities for national security purposes.
- **Media**: Entities that bring transparency by reporting on and disseminating vulnerabilities.
- **Adversarial actors**: Entities that may exploit vulnerabilities.

AMI is also heavily exposed to remote cyber-attacks during the operational phase. As far back as 2007, the United States of America's Department of Energy commissioned work to understand the threats emerging from AMI. Parks (2007) identified three kinds of threats: (1) the cheating customer, (2) insider threat, and (3) the nation-state or the terrorist threat.[2]

The *cheating customer* has physical access to the meter at their premises and is characterised by a low to high level of cyber skills, low funding, and a long time horizon to achieve their goal of lowering electricity bills. Customers could reconfigure the meters through physical access, flood the upstream communication channels, and prevent the utility from communicating with the downstream meters. Although tampering with smart meters requires access to proprietary manufacturer information, the probability of a customer with the skills and willingness to exploit this threat grows with the number of smart meter installations. The threat multiplies if a customer can sell this malicious solution to other customers.

The *insider threat* occurs when a utility employee colludes with the power generator to artificially increase electricity demand or conceals billing and collection inefficiencies. On the other hand, utility employees may also collude with customers to manipulate power bills for monetary gain. 'Insiders' can also subdue commercial inefficiencies in system operation, given their high physical access to the relevant systems. 'Insiders' are characterised by a low level of cyber skills, low funding, and a moderate time horizon for manipulation.

The *nation-state threat* puts the bulk electricity system or systems outside the electricity system at risk, such as healthcare and transportation. Depending on the AMI architecture, gaining access to the bulk system is possible from the customer endpoint. For example, access to the upstream communication may provide access to other meters or the local DCU, the HES, and other systems connected to it, up to the system operator. Once access to the bulk system is available, false pricing and operational signals that dramatically increase or decrease the load could be sent to the meters, impacting grid security.

An ICT network is only as secure as its weakest link (Livingston et al. 2018). Vulnerabilities in one part of the network can compromise the reliability of the entire system. All the key entities involved in deploying and operating the power system need to behave optimally to secure the system from vulnerabilities. The following section reviews the global practices that ensure optimal behaviour of the power system entities.

[2] Wei et al. (2011) provide an alternative classification of threats based on the system architecture: component-level, protocol-level, and topology-level.

3. International practices in securing the electricity sector

Security risks to the power system carry the threat of cascading impact on multiple other sectors, such as public health, security, the financial system, and general economic activity. In view of its importance, various jurisdictions have classified the power system as 'critical infrastructure' (Livingston et al. 2018) and enacted regulations to govern its security and data management practices. This section briefly reviews these practices in two progressive jurisdictions, the European Union and the United States.

3.1 The European Union

European Union (EU)-level directives provide the baseline objectives of the legislation, which the EU Member States must transmute into their respective national laws. The Network and Information Systems Directive (NISD) provides the Member States with a legal basis to impose penalties for non-compliance with minimum standards (European Parliament and Council of the EU 2016). The NISD stipulates the Member States to identify electricity suppliers, distributors, and system operators as operators of essential services (OES). Companies providing services such as online marketplaces, online search engines, and cloud computing to OES are designated digital service providers (DSP). The degree of risk to the DSP is deemed to be lower than to the OES and is, therefore, subject to relatively relaxed regulatory compliances. The NISD also requires each member state to have a 'single point of contact' (SPoC), which forms part of an EU-wide 'Cooperation Group' to facilitate strategic cooperation among the Member States for cyber security. If a cyber-incident in one-member state also affects OES and DSP in the other Member States, the SPoC must circulate the incident information and report the same to the Cooperation Group.

> Security risks to the power system carry the threat of cascading impact on other critical economic sectors.

Beyond directives, EU-level regulations apply directly to all its Member States at the national level. In April 2019, the EU enacted Regulation No. 881/2019 ('the Cybersecurity Act'), which widened the mandate of the EU Agency for Network and Information Security (ENISA), initially established in 2004 (European Parliament and the European Council 2019). ENISA serves as the reference point for knowledge exchange and best practices for the Member States and private stakeholders, for the European Commission on sectoral policies concerning cyber security, and for direct collaboration with 'computer security incident response teams' (CSIRTs) (Markopoulou et al. 2019). The Act provides for structural cooperation between ENISA, the EU's Computer Emergency Response Team (CERT-EU), and the Cooperation Group. ENISA has developed tools that help organisations and the Member States assess and improve their cyber security maturity (ENISA 2022b).

Further, the EU has also implemented a cyber security certification framework in which ENISA develops compliance standards and evaluation criteria for ICT products, services, and processes, and the Conformance Assessment Body certifies compliance (ENISA 2022a). Where reporting of incidents involves processing private data, it is done as per the relevant EU regulations governing data, for example, Regulation (EU) 2016/679, better known as the General Data Protection Regulation (GDPR).

3.2 The United States

The US Department of Energy's (USDOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) coordinates the electricity sector's cyber security preparedness. AMI pilots funded by the DOE require participants to identify cyber security risks and mitigation strategies, criteria used for vendor and device selection, the standards or best practices to be followed, and accountability to ensure implementation (USDOE 2016). Further, CESER supports three primary instruments (CESER 2022):

- **The Cybersecurity Risk Information Sharing Program (CRISP)** under which the Electricity Information Sharing and Analysis Center (E-ISAC) provides operators of critical electricity infrastructure with information on threat actors, analytics to identify anomalies, and event and incident statistics (CESER, n.d.). Together with the Pacific Northwest National Laboratory and the Argonne National Laboratory, E-ISAC analyses voluntarily shared data against the known catalogue of threats and informs the industry of the steps to identify and mitigate threats.
- **The Cybersecurity Capability Maturity Model (C2M2)** is a tool developed by CESER in collaboration with the industry and in alignment with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. The

tool contains 10 domains, each with objectives and practices that an organisation can use to improve its risk management capability.[3] The progression of implementation of each practice can be tracked using three maturity indicator levels: initiated, performed, and managed.

- **The Risk Management Process (RMP) guideline** was co-developed by the USDOE, NIST, and the North American Electric Reliability Corporation (NERC), which oversees grid reliability in the United States, Canada, and some parts of northern Mexico. RMP provides a cyber risk management approach to organisations active in electricity generation, transmission, distribution, and marketing of electricity and vendors to these organisations (USDOE 2012).

Despite an enabling framework and instruments against cyber threats, the US Government Accountability Office (USGAO) found that the potential impacts of cyber threats to the distribution sector are poorly understood. The USDOE's efforts do not adequately address distribution sector threats (USGAO 2021). The World Economic Forum's (WEF) analysis of the European and North American cyber security laws also identified a few gaps (WEF 2020b):

- Utilities do not have the capacity or detailed guidance on mapping risks emanating from vendors and mitigating them via contracts.
- Absence of clear definitions and measurability of cyber resilience.
- Inadequate mechanisms for information and threat data sharing by utilities in terms of incident definitions and participation by private sector players.

Our review of international practices to secure distribution infrastructure underscores the importance of having a robust regulatory framework with information-sharing and capacity-building platforms built in collaboration with the private sector. It also guides our policy recommendations after comparing the institutional mandates and governance practices between EU, the United States, and India. In the next section, we analyse the framework for AMI deployment in India using notified guidelines and the contractual arrangements between discoms and service providers.

4. Review of India's AMI deployment framework

This section reviews the guidelines and standards notified by various regulating entities for AMI in India and the roles and responsibilities defined in the state-level deployment contracts. The institutional framework for cyber security rests on a decentralised power sector governance framework. Discoms in each state are accountable to independent state electricity regulators, while Government of India agencies govern matters relevant to multiple states, such as technical specifications of grid infrastructure. Within this framework, numerous agencies govern different aspects of AMI deployment.

4.1 India's cyber security institutional framework

The principal legislation on cyber security in India is the *Information Technology (IT) Act, 2000* (amended in 2008). The *IT Act* is complemented by the *National Cyber Security Policy* (NCSP), 2013, drafted by the erstwhile Ministry of Communications and Information Technology (now the Ministry of Electronics and Information Technology, MeitY) with the vision to "build a secure and resilient cyberspace for citizens, businesses and Government" (MeitY 2013).

In line with the NCSP 2013, the National Critical Information Infrastructure Protection Centre (NCIIPC) was formed under the *IT Act* in January 2014 as the nodal agency for critical information infrastructure protection (Government of India 2000).[4] NCIIPC is responsible for collecting and analysing data for policy guidance on national-level threats to critical infrastructure, but the primary responsibility of securing the infrastructure lies with its operator (Government of India 2014).[5] NCIIPC is also tasked with coordinating with the Indian Computer Emergency Response Team (CERT-In) and the international community to develop strategies to protect critical infrastructure and conduct research. CERT-In is the primary agency for cyber security incident reporting, providing analysis and forensics of cyber security incidents, incident response, and information security assurance and audits. It is also responsible for coordinating with sectoral CERTs in preventing and responding to cyber security incidents.[6]

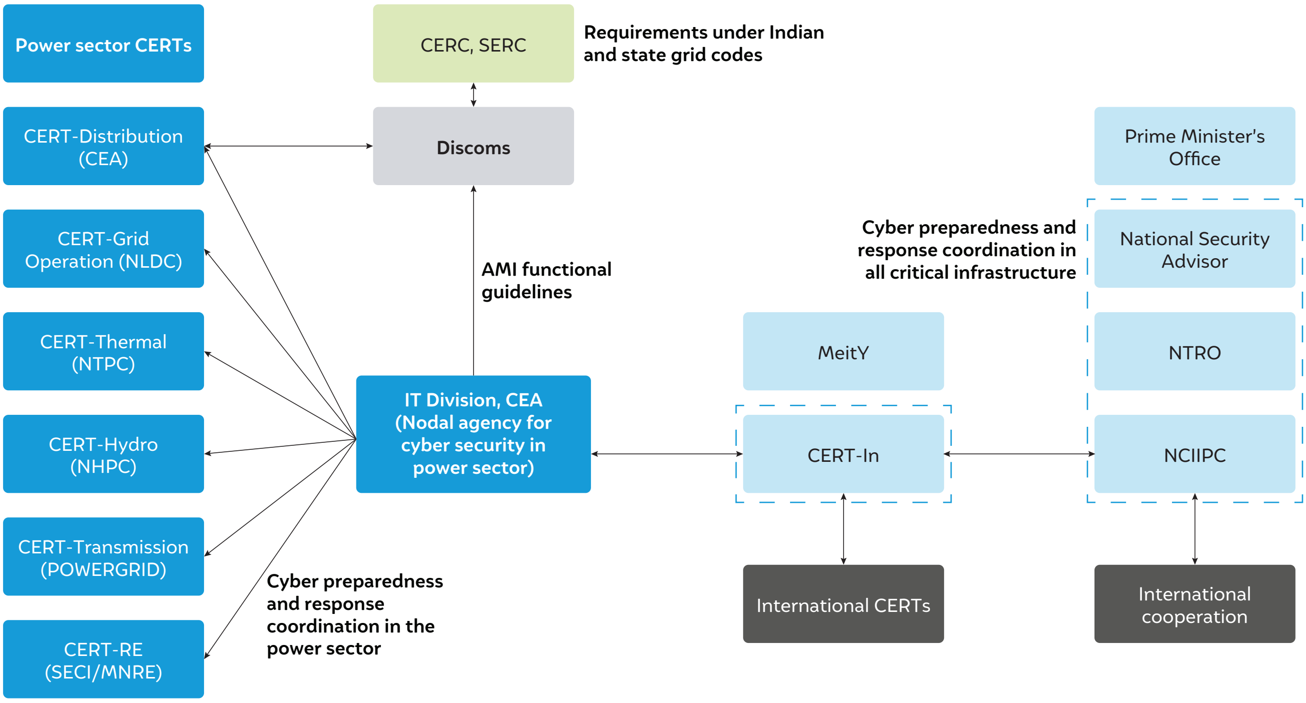
[3] Some domains are 'Asset, Change, and Configuration Management', 'Event and Incident Response, Continuity of Operations', 'Third-Party Risk Management', and 'Identity and Access Management', among others.

[4] Under sub-section 1 of Section 70 of the IT Act, 2000, critical information infrastructure is defined as "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety" (Government of India 2000). Currently, transport, power and energy, telecom, government, banking, financial services and insurance, and strategic and public enterprises are the six critical infrastructures.

[5] For example, the primary responsibility of securing the electricity grid lies with stakeholders involved in its daily operations.

[6] CERT-In was formed under Section 70B of the IT Act, and its roles and functions were notified in January 2014 (Government of India 2014b).

Figure 2 India has a comprehensive cyber security preparedness and response framework


Power sector CERTs
CERT-Distribution (CEA)
CERT-Grid Operation (NLDC)
CERT-Thermal (NTPC)
CERT-Hydro (NHPC)
CERT-Transmission (POWERGRID)
CERT-RE (SECI/MNRE)
CERC, SERC
Requirements under Indian and state grid codes
Discoms
AMI functional guidelines
IT Division, CEA (Nodal agency for cyber security in power sector)
Cyber preparedness and response coordination in the power sector
Prime Minister's Office
Cyber preparedness and response coordination in all critical infrastructure
National Security Advisor
MeitY
NTRO
CERT-In
NCIIPC
International CERTs
International cooperation

Source: Authors' illustration

The Ministry of Power has formed six sectoral CERTs, with the CERT-Distribution housed in the Distribution Planning and Technology Division at the Central Electricity Authority (CEA 2022). The Information Sharing and Analysis Centre-Power (ISAC-Power) is a portal for information sharing and coordination between the power sector CERTs (CERT-In 2020). The IT Division of the CEA governs cyber security in the power sector, houses CEA's own computer security incident response team (CSIRT) and is the coordinating agency for power sector CERTs.

Outside the ambit of the *IT Act*, the Central Electricity Regulatory Commission's (CERC) *Indian Electricity Grid Code* (IEGC) requires all utilities to identify critical cyber assets and take steps to protect them to ensure reliable grid operation (CERC 2010). As per the *Electricity Act, 2003*, the State Electricity Regulatory Commissions (SERCs) are responsible for specifying the state grid codes based on the IEGC and other standards on supply reliability for discoms. Figure 2 summarises this institutional framework.

4.2 National-level cyber security framework for the power sector

The institutional framework mandates the CEA as the primary entity responsible for policy guidance on cyber security preparedness and response in the power sector. Accordingly, the CEA released mandatory guidelines for cyber security in the power sector in October 2021 (CEA 2021). The guidelines provide power sector-specific cyber security measures by operationalising the NCSP 2013. Some important provisions of the guidelines as applicable to discoms are as follows:

- Appointment of a Chief Information Security Officer (CISO) who heads the Information Security Division (ISD) and shall be responsible for cyber security planning and activities, coordination with the sectoral CERT, and sharing incident response reports with CERT-In.
- Drafting, annual review, and implementation of a Cyber Security Policy via the ISD, including Cyber Risk Assessment and Mitigation Plans and a Cyber Crisis Management Plan.
- Identification of critical information infrastructure and critical business processes, with a mapping of the impact and risk profile.
- Mandatory ISO/IEC 27001 certification, including sector-specific controls as per ISO/IEC 27019.[7]
- Identify IT equipment that is nearing end-of-life or is left without development support and phase it out.
- Conduct routine security audits, tests, and training.

[7] The ISO/IEC 27000 family of standards provide guidelines for keeping information assets secure. ISO/IEC 27001 and 27002 contain requirements of information security management systems and a code of practice for information security controls, respectively. These standards include practices such as privileged access management, encryption of organisational systems, and storage, communication and destruction of information. ISO/IEC 27019 provides guidance based on ISO/IEC 27002 applied to process control systems used by the energy utility industry.

Further, the guidelines stipulate that smart meters are procured only from vendors notified in the CEA's 'Trusted Vendors' list.[8] If a discom wants to procure smart meters from a vendor not on this list, the CEA shall approve the procurement after verifying the vendor's certifications for supply chain management, secure product development practices, and a cyber security conformance test of the product. There are three designated laboratories in India for testing smart meters as per the procedure.

The CEA has also prescribed the main functional requirements and standards for AMI components (see Annexure I). The functional requirements provide standards for smart meters, DCUs, and integration of HES with meter data management system (MDMS), as well as general requirements to secure the AMI (CEA 2016) including:

- Securing access controls by defining and limiting authorised user access to software environments and applications and adopting best practices from security enterprises
- Maintaining logs of all attempts at unauthorised access to controls, privilege change requests, user actions affecting security such as password changes, etc.,
- Weeding out all insecure protocols and unnecessary hardware or software packages from the system

> **The national-level guidelines place obligations on discoms to verify component certifications and improve cyber preparedness.**

- Detecting malicious software, installing anti-virus software in all the software configurations, including applications, servers, and databases
- Securing the network architecture of HES through encryption and primary and host-based firewalls.

Thus, the national-level cyber security guidelines for AMI and the distribution sector are quite comprehensive. Obligations are placed on discoms to verify component certifications and establish institutional practices for cyber preparedness and incident response. The guidelines cover the operational aspects of infrastructure and require the supply chain actors to follow international standards and obtain certifications.[9] However, stipulating comprehensive requirements does not guarantee their efficient implementation. The mass disconnection event in Uttar Pradesh in 2020 (see Box 1) demonstrated that lapses could happen despite meeting all requirements on paper. The following section reviews the AMI deployment model in India and examines how vulnerabilities could creep into the AMI within the existing rollout framework.

Box 1 The Uttar Pradesh smart meter outage event in August 2020

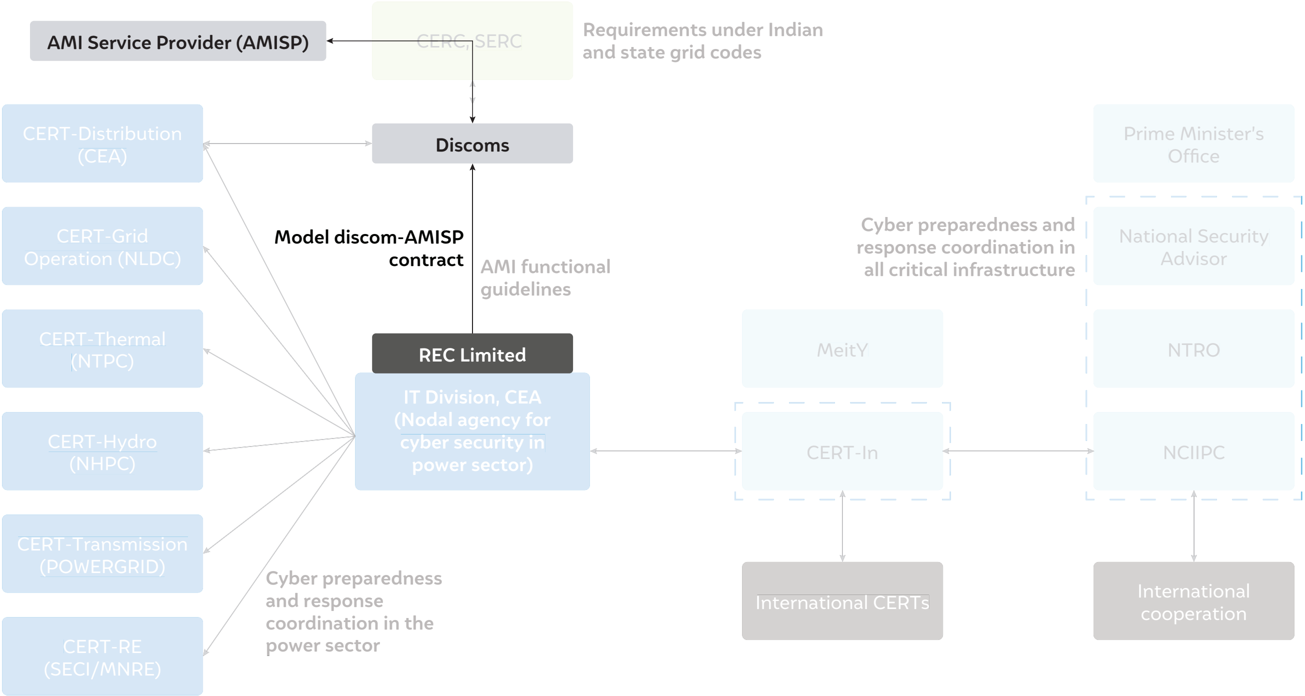
On 12 August 2020, nearly 158,000 households connected with smart meters in Uttar Pradesh suffered an outage that continued for several hours (Mishra 2020). The Energy Efficiency Services Limited (EESL), the entity contracted by the Uttar Pradesh Power Corporation Limited (UPPCL) for AMI rollout, reported that the event occurred due to a 'technical glitch' inside the premises of the system integrator. EESL explained that the executive responsible for manning the HES, i.e., the communication system between consumers' meters and the central MDMS, transmitted a wrong command for disconnecting 1.2 million smart-metered consumers. However, EESL truncated the disconnection process mid-way, limiting the blackout to only about 158,000 consumers (Mishra 2020).

Preliminary assessments of the incident revealed the presence of multiple unauthorised user accounts in the system (Mishra 2020). Taking *suo moto* cognisance of the matter, the Uttar Pradesh Electricity Regulatory Commission (UPERC) halted smart meter deployment in the state. It issued a show-cause notice to UPPCL to explain the reasons behind the event (UPERC 2020). Citing that the event violated the standards of performance provisions of *UPERC Electricity Supply Code 2005*, the commission also advocated for compensation to affected consumers by UPPCL. However, the discom contested this proposal, stating that the causes for the outage were beyond their control.

[8] The 'trusted vendors' list has not been notified by the CEA by the time of publication of this study.

[9] Certification is a best practice as it reduces information asymmetries and adverse selection, leaving networked systems vulnerable to cyber threats (Clayton et al. 2017).

Figure 3 The discom–AMISP contracts are a critical feature defining cyber preparedness of AMI


AMI Service Provider (AMISP)
CERC, SERC
Requirements under Indian and state grid codes
CERT-Distribution (CEA)
Discoms
Prime Minister's Office
CERT-Grid Operation (NLDC)
Model discom-AMISP contract
AMI functional guidelines
Cyber preparedness and response coordination in all critical infrastructure
National Security Advisor
CERT-Thermal (NTPC)
REC Limited
MeitY
NTRO
IT Division, CEA (Nodal agency for cyber security in power sector)
CERT-Hydro (NHPC)
CERT-In
NCIIPC
CERT-Transmission (POWERGRID)
Cyber preparedness and response coordination in the power sector
International CERTs
International cooperation
CERT-RE (SECI/MNRE)

Source: Authors' illustration

4.3 AMI deployment model and operation contracts

The dominant model of smart meter deployment combines the meter leasing and metering services agency models (Pillai et al. 2017). As the upfront cost of smart meters and associated infrastructure is high, most discoms in India prefer to contract out procurement, project management, installation, and operation and maintenance of AMI. Discoms pay the contracted AMI Service Provider (AMISP) a per meter per month fee over the contract duration for its services as an operational expenditure (opex). About two-thirds of all smart meter installations across states by July 2022 were done following the 'opex' model or one of its variations where the AMISP is paid a part of the lifecycle cost upfront (the total expenditure or 'totex' model) (NSGM 2022a). A bulk of the current deployments are being done based on these two models and also on REC's standard bidding document (SBD) for contracting AMISPs (RECL 2022).[10]

Figure 3 depicts the AMI deployment scenario in India. Discoms are the legal entities responsible for the secure operation of AMI, but all functions related to AMI are outsourced to the AMISP. In this scenario, discom–AMISP contractual arrangements assume critical importance for the cyber preparedness and resilience of the Indian power system. The SBD defines the cyber security provisions and responsibilities of various supply chain actors, including hardware and software vendors, AMISPs, and discoms. We assess parameters of the SBD and categorise them into the four pillars of ICT systems discussed in Section 2.

We analyse the latest version of the SBD circulated by REC in September 2022. The SBD contains multiple provisions under each pillar of ICT systems[11] and follows CEA's technical requirements for AMI, in addition to providing operational specifications. For instance, AMISPs must ensure the replication of HES and MDMS data at a safe location to ensure that the system does not suffer disruption if one part is compromised. In case the system is compromised, definitive deadlines are prescribed for response and resolution, categorised based on the severity level of the threat. Contract conditions also require the AMISP to maintain system integrity by logging and reporting tamper events at each communication node, securing sensitive information like passwords and giving limited access based on the legitimate purpose of the module.[12]

[10] In June 2021, the GoI launched the Revamped Distribution Sector Scheme (RDSS) (Cabinet Committee on Economic Affairs 2021), under which the GoI will provide financial assistance to discoms to convert all non-agricultural electricity meters to smart meters by March 2025. The GoI assistance is only for installations under the totex model and based on the SBD circulated by the RECL (RECL 2022b). RECL is the nodal agency for the national scheme supporting smart meter deployment.

[11] The classification of clauses under the various pillars is done by the authors for the purpose of the analysis and is not presented as such in the SBD.

[12] Here, a module can be a process, a user, or a program.

The SBD prescribes detailed provisions for the security of cloud services, including segregation of the end-user and the non-live environments and prevention of distributed denial of service (DDoS) attacks. The SBD makes the discom the sole custodian of data, and the AMISP is required to take permission from the discom to modify or delete any data. The discom and the consumers' consent are required based on the purpose of sharing data with third parties. Additionally, the SBD includes provisions on reporting, auditing, and penalties to ensure accountability of the AMISP. Table 1 summarises our assessment.

Table 1 Cyber security provisions in the SBD

ICT system pillar	Cyber security provisions
Availability	**Communication system** • AMISP to provide disaster recovery and redundancy mechanism for HES and MDMS[13] • Communication network, set up by AMISP, to have dynamic and self-healing capabilities **Backup system** • AMISP to provide online monitoring diagnostic programs for verifying the availability of the backup equipment **Breach plan: Response and resolution** • In case of a breach, AMISP should provide information on system issues and availability to be flagged at three different severity levels, with different response and resolution times for each level. The different severity levels are defined by their immediacy in causing system failure and have response time ranging from 15 minutes for high-severity cases to 10 days for low-severity cases.
System integrity	**Communication system** • AMISP to ensure continuous logging and reporting of tamper events, provision of secure access control and authorisation control based on the least-privilege concept[14] **Cloud** • Segregation of non-production and production environments[15] • Provision of Web Application Firewall and DDoS protection
Confidentiality	**Ownership of data and data sharing** • Discom is the sole custodian of data • Sharing part/complete database with third-party subject to review and consent of the discom and consumers (in relevant cases) • Consumer consent on sharing and processing data is segregated as either 'not required' or 'opt-out'.[16] **Integrity check** • AMISP to ensure data integrity checks on all metered data **Communication system** • HES shall encrypt data for secure communication **Cloud** • Cloud service provider (CSP) to ensure compliance with the latest version of the standards for information security management systems, including ISO 27018 and PCI DSS, for data privacy • CSP to include provisions for data management, including encryption of data in transit or at rest, and ask for the consent of the discom for deletion/modification of any data **Data documentation, privacy, and breach** • 'Breach of data privacy' is defined as a severity level 2 threat, and AMISP is required to respond to the threat and resolve it within 30 minutes to 24 hours of its occurrence • AMISP is to submit the 'privacy by design' document to the discom, which contains all the policies, practices, processes, and technologies employed to manage and process the data • AMISP to create and submit a 'data breach plan' to the discom

[13] Disaster recovery relies upon the replication of data and computer processing in an off-premises location not affected by the disaster. Software redundancy refers to adding some modules at the design stage so that the system completes the required tasks even if a component fails.

[14] The least privilege concept entails that any process, user, or program must be able to access only the information and resources that are necessary for its legitimate purpose (Rosenberg 2017).

[15] A 'non-production environment' is any environment that is not used by the end users, like software development and testing environments.

[16] Consumer consent is not required in the following cases:
For the purpose of generating bills, identifying theft, network planning, load forecasting, or any related activities that can enable the utility to fulfil its duty as a licensee. If any type of smart meter data is requested by the law enforcement agencies. If aggregated or anonymised data is shared with not-for-profit academics, policy research, and civil society organisations for research that can benefit the sector in general. The option of opting-out is provided to consumers if data is to be shared with any third-party commercial entity to provide services other than as enabled by regulation.

ICT system pillar	Cyber security provisions
Accountability	**Capacity building** • AMISP to provide a week-long network and cyber security training course to five discom trainees **Audits** • AMISP is responsible for annual third-party audits on privacy and cyber security measures • Audit of CSP for compliance with the following standards: ISO 27001, 27017, 27018 and 27017:2015 • AMISP is responsible for conducting third-party data privacy audit at least once every year • Discom to provide consultation to AMISP on actions required to be performed following the audit **Reporting** • AMISP to provide a status report to the discom on the security breach and action taken • AMISP to provide annual reports on patch updates, cyber security monitoring, audits, and implementation of recommendations during the audit **Penalty** • Deduction of 0.4 per cent of AMISP monthly fee for every 0.5 per cent or part thereof[17] reduction in availability (capped at 4 per cent penalty). A maximum penalty of 4 per cent shall be deducted when system availability is < 95 per cent [18]

Source: Authors' analysis based on the review of SBD

The latest version of the SBD follows the previous versions circulated by RECL in September and October 2021, which are in turn based on SBDs circulated by the National Smart Grid Mission (NSGM) in July 2020 and January 2021 (NSGM 2022). Different versions of the model discom–AMISP contract are available in various versions of the SBD, introducing diversity in actual contract provisions signed by discoms. We look at how the terms of contracts actually signed by discoms diverge from the current model contract.

4.4 Diversity in discom–AMISP contracts

We compare the contracts signed by discoms in five states with AMISPs since 2018. The comparison reveals some deviations from the latest version of the SBD.

- **Uttar Haryana Bijli Vitran Nigam (UHBVN), one of the two discoms in Haryana, has strengthened the reporting and penalty component of the contract to make it more robust.** UHBVN requires the AMISP to develop (i) a data backup, archival, and retention policy, (ii) a security policy, and (iii) a business continuity and disaster recovery policy. These policies must comply with the relevant ISO standards, made in consultation with the discom and updated every six months. There are penalty provisions for non-availability of the system, non-submission of audit reports, and other non-compliances (implementation of audit recommendations or security policy), which seek to hold the AMISP accountable to the discom.
- **Jaipur Vidyut Vitran Nigam Ltd. (JVVNL), a discom in Rajasthan, has added a provision to secure the physical infrastructure** by directing the AMISP to have at least three data centres in at least two different seismic zones in India. **However, many provisions related to 'accountability' and 'availability' are missing.** There are no penalty provisions and no requirements mentioned for system availability. This may be because the contract was signed in 2018, before any of the SBDs were prepared by NSGM or REC. As per the contract between JVVNL and AMISP, the latter must get the system audited by a certified third party on an 'as-needed' basis instead of annually, as mentioned in the model contract. JVVNL also does not contain any provisions related to securing data apart from performing data integrity checks on the metered data.
- **Assam Power Corporation Ltd. (APCL) has raised the penalty for non-compliance with system availability standards** and capped it at six per cent of the AMISP's monthly fee, instead of four per cent as mentioned in the model contract.

Further, the frequency of event-reporting and security audits vary across the discoms, from monthly in Jammu & Kashmir to quarterly in Haryana to annually in Maharashtra and the model contract. Across the contracts we reviewed, improvements on the SBD are limited to a few clauses, such as requirements for drafting policies and penalties for reduced availability. Transparency and confidentiality clauses mostly remain unchanged. It is also important to note that the role of discoms in governing the AMI is limited to oversight

[17] For example, for 0.6 per cent reduction in availability the deduction will be 0.8 per cent of AMISP's monthly fee.

[18] For system availability, the availability is computed as THM – (S1 X 1+S2 X 0.8+S3 X 0.5)/THM; where THM is total hours in the month when power supply to AMI system is available, S1/S2/S3 is the total non-available hours as per different severity levels.

or providing feedback. At the same time, the AMISP is primarily responsible for performing different functions ranging from security provisions, system audits, and training the discom staff. If a third-party vendor is involved in the capacity of a CSP, the AMISP is also responsible for defining cloud security services and cloud security audit. Annexure II lists the roles and responsibilities of each actor.

5. Towards cyber-resilient AMI

Based on the analysis of the principles of securing AMI as an ICT system, the Indian legislative and institutional framework on critical infrastructure cyber security, and the actual AMI rollout process, we provide four recommendations for making the power system more resilient to cyber threats.

5.1 Bring all discom-AMISP contracts to a common baseline

Variations in provisions in discom–AMISP contracts with regard to critical clauses such as audit requirements, implementation of audit recommendations, penalties for non-availability, and discom training can lead to vulnerabilities in the power system. Cyber security as an economic good suffers from the existence of free riders, and its adequate provision requires collective action (Kianpour et al. 2022). Further, AMI's security is determined by the actions of the weakest link (Livingston et al. 2018). Variations in AMISPs' cyber security obligations, non-compliance penalties across discoms, and the varying capacity of discoms to enforce contractual terms pose risks to the power system. SERCs must ensure that all discom–AMISP contracts reflect AMI's latest best practices with regard to cyber security provisions.

The structure of the RDSS partly solves the diversity in contracts because certain prerequisites during procurement need to be met by discoms to be eligible for financial assistance. The SBD forms a baseline for all contracts signed after September 2022, and discoms are encouraged only to strengthen its provisions. However, past installations have been made based on previous versions of the SBD, which may not be as comprehensive as the current version and may not reflect the current technological landscape. In large discoms with more than 4–5 million consumers, multiple AMISPs contracted in different years may exist. A convergence in contractual provisions between and within discoms is essential for system resilience. The CEA must work with the Forum of Regulators (FoR) and SERCs to harmonise critical contractual obligations across states.

5.2 Resolve the principal–agent problem in AMI deployment

The totex model of AMI deployment vests the AMISP with more information than the discom on hardware and software quality, system architecture and vulnerabilities, and operational data, etc. However, the Indian power sector regulations and cyber security legal framework make discoms accountable for power system reliability, availability, and confidentiality. Inadequate incentives and penalties for AMISPs to disclose relevant information to the discom can restrict the latter's ability to fulfil their regulatory obligations. Also, when adequate information is not available, the ability of discoms to respond to incidents in coordination with agencies such as CERT-Distribution and CERT-In would be restricted.

Based on our discussions with representatives of several discoms, we find information asymmetry to be prevalent. At the installation and deployment stage, the discoms rely on certifications and testing reports provided by the AMISP or entities hired by the AMISP. Discoms mostly do not have dedicated discom staff with the technical expertise to vet the information provided by the AMISP. The outage event in Uttar Pradesh highlights a potential fallout of the present practices, where a mass disconnection signal was sent out without authorisation from discom staff (see Box 1). Thus, discoms must ensure that incentives and penalties within their contracts with AMISPs are sufficient and enforceable to ensure efficient and timely information disclosure by AMISPs. Further, broader guidelines for accountability of vendors and hardware and software providers for security failures may be developed by the CEA in consultation with discoms.

> Diverse contract provisions and information asymmetries are sources of risk in the current rollout model.

5.3 Provide deeper technical support to discoms to maintain cyber resilience and foster a local ecosystem for security services

The cyber security frameworks in the United States and the EU show that central or federal provision of technical know-how on cyber security for utilities is needed for a secure power system. Due to the dynamic and evolving technological environment, cyber security resilience involves protecting the system against known risks and building the capability to manage unknown risks. Discoms need more actionable guidance and step-wise processes to build resilience against cyber threats. Such detailed guidance for discoms is currently missing. While AMISPs are required to train discom staff as part of the contract, their effectiveness in institutionalising best practices for training is questionable. Given the poor financial health of the discoms, they may not be able to develop such capacity for testing or for purchasing the relevant test tools from the market. Further, central law enforcement agencies and internet service providers are better equipped to investigate, track, and address the root cause of security threats.

As the nodal agency for cyber security in the power sector, the CEA, in coordination with the CERT-In and the NCIIPC, must provide deeper technical support to discoms. Support must include training the discom staff to monitor compliances and certifications during deployment and maintain operational oversight and supervision during the operation phase. Tailored training and awareness programs, including mock drills or threat simulation exercises, may be organised for personnel responsible for managing AMI to help them stay updated with the latest threats and best practices. Developing a standard security metric or index for measuring discoms' cyber security maturity would help discoms self-assess their preparedness. A periodic review of the indices would also provide central agencies like the CEA, CERT-In, and the NCIIPC clear information on discoms' capability to respond to cyber security threats and their progression over time. Beyond tools and training, discoms need facilities that provide support services. For example, stakeholders highlighted the limited number of certified laboratories for smart meter testing as a concern during consultations, which poses difficulties in following the rollout schedules and dispute resolution with consumers. As the demand for smart meters increases, more certified testing laboratories will be required.

The CEA can leverage expertise available with central public sector undertakings (CPSUs), MeitY, and private stakeholders to provide training and analytical support to discoms. For example, CESER, under the USDOE, regularly collaborates with industry experts to develop tools that help utilities assess their cyber security maturity levels (see section 3.2). The provision of guidance from the CEA could also make investments in cyber security more cost-effective for already financially stretched discoms. CERT-In currently provides a list of empanelled third-party auditors for the cyber security of IT systems. The cost of each audit is currently about INR 30–40 lakh,[19] and as the system grows in size and complexity, the cost and frequency of such audits are bound to increase. Due to the public good characteristics of cyber security, government investment in this activity is vital. Initial public procurement of security services would also signal demand to the market, fostering a local ecosystem for AMI-based technology and security solutions.

5.4 Strengthen the regulatory provisions to hold discoms and vendors accountable for cyber security failures

The aftermath of the UP smart meter outage incident highlighted the need for stronger accountability provisions, not only for AMISPs but also for discoms. Although the contracts hold AMISPs accountable to discoms, in order to fulfil their legal obligation of providing reliable supply, the discoms need to be made accountable to the respective SERCs. Further, regulations must also enable discoms to hold AMISPs and vendors liable for security lapses and compromises. Cyber security lapses can lead to financial losses through theft, physical safety threats to human resources, or breaches of sensitive consumer data. Hence, it should be discoms' responsibility to provide full disclosure in case of a security incident, and discoms must be equipped to extract full disclosure from the supply chain of vendors. Penalties and information disclosure obligations can lead to a higher level of security within the system (Kianpour et al. 2022).

> Developing standard metrics for measuring cyber security maturity would help discoms self-assess and improve their preparedness.

[19] Based on conversations with discom officials.

The CEA can play an advisory and supportive role, but enforcement at the discom and state-level has to be ensured by the respective SERCs. This means that SERCs across states would also require technical expertise in drafting regulations for cyber security and maintaining regular oversight in an increasingly digitised power system. The FoR must play an active role by drafting model regulations and assisting SERCs develop in-house technical capacity for cyber security by leveraging the technical expertise available with agencies such as the CEA, REC, NCIIPC, CERT-In, CPSUs, and the private sector.

6. Conclusion

With the dual objective of energy transition and discom health in mind, the GoI has set an ambitious target for AMI deployment. Meeting this target would require installing more than 270,000 meters daily over the next 2.5 years. However, while pursuing these ambitious targets, it is essential to ensure that the deployment process does not overlook necessary robustness and security checks and that the electricity supply chain is equipped to deal with the massive scale of digitisation. It is crucial to institute a robust regulatory framework and equip stakeholders to enforce the regulations.

An assessment of the national cyber security framework and power sector-specific guidelines shows that India has a comprehensive framework for ensuring the cyber security of the power system. Institutions to ensure incident response and preparedness are already in place. The SBD issued by REC provides a baseline set of practices for all discoms to ensure that the power systems are safe.

However, a deeper assessment of how the framework cascades into actual contracts and equips discoms to enforce the regulations reveals some key gaps. The analysis underscores the need for interventions to harmonise critical contract provisions to a baseline, especially those integral to maintaining system integrity and availability. Discoms should have operational capacity and situational awareness of the AMI system to carry out their legal and regulatory obligations. For achieving this capacity, adequate incentives for AMISPs to disclose information to the discoms need to be put in place along with deeper technical and financial assistance to discoms from central agencies. And finally, state electricity regulators must do more to hold discoms accountable for lapses in the system. Penalties and information disclosure obligations play critical roles in improving cyber security in ICT systems.

Given that AMI is a relatively nascent technology in the Indian power sector and is likely to witness a sudden expansion, it would be imperative to prepare and guard against known and unknown cyber security risks. Devising effective solutions to address the issues highlighted in this issue brief would require a collective effort of all key stakeholders.

References

Agrawal, Shalu, Sunil Mani, Karthik Ganesan, and Abhishek Jain. 2020. “What Smart Meters Can Tell Us.” New Delhi: Council for Energy, Environment and Water.

Cabinet Committee on Economic Affairs. 2021. “Cabinet Approves Revamped Distribution Sector Scheme: A Reforms Based and Results Linked Scheme”.” June 30, 2021. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1731473.

CEA. 2016. “Functional Requirements of Advanced Metering Infrastructure (AMI) in India.” New Delhi: Central Electricity Authority. http://www.cea.nic.in/reports/others/god/dpd/ami_func_req.pdf.

CEA. 2021. “CEA (Cyber Security in Power Sector) Guidelines, 2021.” New Delhi: Central Electricity Authority. https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf.

CERC. 2010. “Indian Electricity Grid Code.” New Delhi: Central Electricity Regulatory Commission. https://cercind.gov.in/Regulations/Signed-IEGC.pdf.

CERT-In. 2020. “ISAC-Power.” 2020. https://www.cert-in.org.in/s2cMainServlet?pageid=ISACPower.

CESER. 2022. “Energy Sector Cybersecurity Preparedness.” Energy.Gov. 2022. https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness.

CESER. n.d. “Cybersecurity Risk Information Sharing Program (CRISP).” US Department of Energy.

Clayton, R., E. Leverett, and R. Anderson. 2017. “Standardisation and Certification of Safety, Security and Privacy in the ‘Internet of Things.’” Luxembourg: Publications Office of the European Union. https://publications.europa.eu/en/publication-detail/-/publication/80bb1618-16bb-11e8-9253-01aa75ed71a1/language-en.

Cleveland, F. M. 2008. “Cyber Security Issues for Advanced Metering Infrastructure (AMI).” In *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 1–5. https://doi.org/10.1109/PES.2008.4596535.

Dasgupta, Binayak. 2022. “Chinese Hackers Targeted 7 Indian Power Hubs, Govt Says Ops Failed.” Hindustan Times. April 8, 2022. https://www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html.

ENISA. 2015. “Good Practice Guide on Vulnerability Disclosure: From Challenges to Recommendations.” Athens: European Union Agency for Cybersecurity.

ENISA. 2022a. “EU Cybersecurity Certification - FAQ.” Page. ENISA. 2022. https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq.

ENISA. 2022b. “Tools.” Folder. ENISA. 2022. https://www.enisa.europa.eu/tools.

European Parliament and the European Council. 2019. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. *881/2019*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

European Parliament and Council of the EU. 2016. “Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union” 59 (July): 1–36. https://doi.org/10.1007/978-1-137-54482-7_33.

Government of India. 2000. *Information Technology Act, 2000*. http://indiacode.nic.in/handle/123456789/1999.

Government of India. 2014. *Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013*. https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=nciipc_function_and_duties_rule_2013.pdf.

Healey, David, Sacha Meckler, Usen Antia, and Edward Cottle. 2016. “Cyber Security in the Energy Sector.” Brussels: European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf.

Kianpour, Mazaher, Stewart James Kowalski, and Harald Øverby. 2022. “Advancing the Concept of Cybersecurity as a Public Good.” *Simulation Modelling Practice and Theory* 116 (April): 102493. https://doi.org/10.1016/j.simpat.2022.102493.

Livingston, S., S. Sanborn, A. Slaughter, and P. Zonneveld. 2018. “Managing Cyber Risk in the Electric Power Sector.” Deloitte. https://www2.deloitte.com/be/en/pages/risk/articles/managing-cyber-risk-power-sector.html?_lrsc=8ab4ef65-7db4-4fc6-879e-685ce8599850&id=wl:2sm:3li:4elevate:5awa:6oth:233077:798917.

Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul de Hert. 2019. “The New EU Cybersecurity Framework: The NIS Directive, ENISA’s Role and the General Data Protection Regulation.” *Computer Law & Security Review* 35 (6): 105336. https://doi.org/10.1016/j.clsr.2019.06.007.

MeitY. 2013. “National Cyber Security Policy.” New Delhi: Ministry of Communication and Information Technology, Government of India. https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.

Mishra, Twesh. 2020. “Uttar Pradesh Smart Meter Shutdowns Due to Sabotage: EESL Official.” @ *businessline*, August 13, 2020, sec. National. https://www.thehindubusinessline.com/news/national/smart-meters-across-seven-cities-in-up-disconnected-due-to-technical-error/article32341021.ece.

MoP. 2021. “Cabinet Approves Revamped Distribution Sector Scheme: A Reforms Based and Results Linked Scheme”.” June 30, 2021. https://pib.gov.in/PressReleasePage.aspx?PRID=1731473.

NSGM. 2022. “NSGM Model SBD for Appointment of AMISP (Totex).” National Smart Grid Mission, Ministry of Power, Government of India. July 2022. https://www.nsgm.gov.in/en/amisp-sbd.

NSGM. 2023. “Smart Metering Status | National Smart Grid Mission, Ministry of Power, Government of India.” March 9, 2023. https://www.nsgm.gov.in/en/sm-stats-all.

Parks, Raymond C. 2007. "Advanced Metering Infrastructure Security Considerations." New Mexico, USA: Sandia National Laboratories.

Pillai, Reji Kumar, Rupendra Bhatnagar, and James Sprinz. 2017. "AMI Roll-Out Strategy and Cost-Benefit Analysis for India." New Delhi: India Smart Grid Forum and BNEF. https://indiasmartgrid.org/reports/AMI%20Roll-Out%20Strategy%20and%20Cost-Benefit%20Analysis%20for%20India_ISGW2017.pdf.

Power Finance Corporation. 2022. "Report on Performance of Power Utilities 2020-21." New Delhi: Power Finance Corporation. https://www.pfcindia.com/DocumentRepository/ckfinder/files/Operations/Performance_Reports_of_State_Power_Utilities/Report%20on%20Performance%20of%20Power%20Utilities%202020-21%20(1).pdf.

Praveen, M. P. 2021. "India's Critical Infrastructure like Gas and Water Vulnerable to Cyber Attacks: Study." *The Hindu*, October 23, 2021, sec. Technology. https://www.thehindu.com/sci-tech/technology/indias-critical-infrastructure-like-gas-and-water-vulnerable-to-cyber-attacks-study/article37137665.ece.

RECL. 2022. "Model Standard Bidding Document for Appointment of Advanced Metering (AMI) Service Provider for Smart Prepaid Metering in India on DBFOOT Basis." Gurgaon, Haryana: Rural Electrification Corporation. https://recindia.nic.in/uploads/files/SBD-Version-3.pdf.

Recorded Future. 2021. "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions." Massachusetts: Recorded Future.

Rosenberg, J. 2017. "Chapter E6 - Embedded Security." In *Rugged Embedded Systems*, edited by Augusto Vega, Pradip Bose, and Alper Buyuktosunoglu, e1–74. Boston: Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-802459-1.00011-7.

Singh, Vaibhav Pratap, Kanika Chawla, and Saloni Jain. 2020. "Financing India's Transition to Electric Vehicles." New Delhi: Council for Energy, Environment and Water.

UPERC. 2020. "Uttar Pradesh Electricity Regulatory Commission Order Dated 19/08/2020." Uttar Pradesh Electricity Regulatory Commission. https://www.uperc.org/App_File/SmartMeter-pdf819202061255PM.pdf.

USDOE. 2012. "Cybersecurity Risk Management Process Guideline." Washington D.C.: US Department of Energy. https://www.energy.gov/sites/default/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf.

USDOE. 2016. "Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investment Grant Program." Washington D.C., USA: US Department of Energy. https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf.

USGAO. 2021. "Report to Congressional Requesters: Electricity Grid Cybersecurity." Washington D.C., USA: US Government Accountability Office. https://www.gao.gov/assets/gao-21-81.pdf.

Vidya. 2021. "Maharashtra Cyber Cell Submits Report on Mumbai Power Outage, Confirms Malware Attack Hit Power Grid." India Today. March 1, 2021. https://www.indiatoday.in/india/story/maharashtra-cyber-cell-mumbai-power-outrage-1774522-2021-03-01.

WEF. 2020a. "The Global Risks Report 2020." Geneva, Switzerland: World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

WEF. 2020b. "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors." Geneva, Switzerland: World Economic Forum. https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Policy_makers_2020.pdf.

WEF. 2021. "The Global Risks Report 2021." Geneva, Switzerland: World Economic Forum.

WEF. 2022. "The Global Risks Report 2022." Geneva, Switzerland: World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

Yadav, Arjun. 2022. "New Study Shows Increasing Cyber Attacks On India's Critical Infrastructure." BW Businessworld. March 6, 2022. http://businessworld.inhttps://www.businessworld.in/article/New-Study-Shows-Increasing-Cyber-Attacks-On-India-s-Critical-Infrastructure-/23-04-2022-426354.

Annexure I Technical standards followed for components of AMI

Table A1 provides a summary of the technical standards to be followed by different components of an AMI. Along with technical requirements, these standards contain some functional security requirements, such as tamper-proofing, remote firmware upgrades, encryption, etc.

Table A1 AMI technical requirements and standards

Component	Functional requirements	Standards followed
Smart Meter	• Records electrical energy usage • Two-way communication with Head End System (HES) • Remote connect/ disconnect/ load limiting • Tamper event detection • Remote firmware upgrade • Prepaid functionality • Net Metering (kWh) features	**Electrical and Mechanical requirements** **IS 13779** with the latest Amendments for AC Static Watt-hour Meter (Class 1 and 2). **IS 15884** with the latest Amendments for Alternating Current Direct Connected Static Prepayment Meters for Active Energy (Class 1 and 2)- Specification. **General and Smart meter functional requirements (Communication module)** **IS 16444** Part 1 with the latest amendments for AC Static Direct Connected Watt Hour Smart Meter (Class 1 and 2)—Specification. **Data security and encryption protocols** **IS 15959** Part 1 and Part 2 with the latest amendments for Data Exchange for Electricity Meter, Reading, Tariff and Load Control-companion Standards
Communication Infrastructure	• Data concentrator unit (DCU) acting as a gateway of communication between smart meters and HES • Network configuration can be RF-based mesh network/ cellular/ PLC based upon the geography	**Definition of DCU Communication Architecture**—IS 16444 **Testing of equipment**—IP-55 Security measures to be implemented by the AMI Implementing Agency (AIA)
Head End System	• Acquisition of meter data on demand and at a user-selectable periodicity • Two-way communication with meter/ DCU • Sending signals for connection and disconnection of switches present in endpoints like meter • Encryption of data for secure communication • Store raw data for a defined duration • Critical and non-critical reporting functionality	**Integration of HES with MDMS** CIM / XML / IEC 61968/ Any other open standard Security measures to be implemented by the AIA No interoperable standards for security measures
Meter Data Management System	• Central data repository to support storage, archiving, retrieval, and validation of data • Analysis of meter data and various other MIS along with validation and verification algorithms	No standards

Source: Authors' compilation based on CEA' Functional requirements of Advanced Metering Infrastructure in India, 2016, and the technical specification of single phase whole current smart meters, 2020

Annexure II Roles and responsibilities of actors in the AMI supply chain

Table A2 Roles and responsibilities of actors in the AMI supply chain

Task/category	Discom	AMISP	Vendors
Meter	-	-	Ensure compliance with IS 15959 Part 2
HES/MDM/ DCU	-	Follow the given security provisions	-
Cloud	-	Defining the services for CSPs	Follow the given security provisions
System availability	Enforce penalty provisions upon gaps in system availability	Provide online monitoring diagnostic system	CSP is responsible for Disaster Recovery Services
Audits	Track and verify audit reports submitted by AMISPs	• Conducting CSP Audit • Subject the security system to Annual Security Audit from CERT-In listed auditors	-
Training	Receive training (five trainees for one week)	Provide training to utility personnel	-
Reporting	Provide feedback on the status report	• Provide status report to the discom on the security breach and action taken • Provide annual reports on patch updates, cyber security monitoring, audits and implementation of recommendations during an audit	-

Source: Authors' analysis

The authors

Dhruvak Aggarwal
dhruvak.aggarwal@ceew.in I @AggarwalDhruvak

Dhruvak works on demand-side management and wholesale power market reforms in India using data, operations engineering, and industrial organisation lenses. He holds a Master of Philosophy from the University of Cambridge and a Bachelor of Technology from Manipal University Jaipur.

Simran Kalra
simran.kalra@ceew.in I @simrankalra441

Simran works on issues related to electricity policy and governance, demand-side management, and energy sustainability. She holds Masters in Public Policy and Governance from Azim Premji University and undergraduate degree in English Literature (Hons.) from Ramjas College, Delhi University.

Shalu Agrawal
shalu.agrawal@ceew.in I @ShaluAgrawal12

Shalu leads The Council's work on residential energy access, demand-side management, and power sector reforms. She uses data to study the changing energy landscape and devise strategies to ensure universal access to affordable, reliable, and sustainable energy. She is an alumnus of University College London and IIT Roorkee.

Suggested citation: Aggarwal, Dhruvak, Simran Kalra, Shalu Agrawal. 2023. *Making India's Advanced Metering Infrastructure Resilient: Analysis of Power Systems from a Cyber Security Perspective*. New Delhi: Council on Energy, Environment and Water.

Disclaimer: The views expressed in this study are those of the authors and do not necessarily reflect the views and policies of the Council on Energy, Environment and Water.

Acknowledgments: We would like to thank Rachna Pathak for valuable contributions to earlier drafts of this document. We owe a debt of gratitude to the various stakeholders who generously provided insights about the burgeoning field of cyber security.

Peer reviewers: Dr Faruk Kazi, Dean, Research, Development & Consultancy, Veermata Jijabhai Technological Institute, Mumbai & Chair, Working Group on Digital Architecture & Cyber Security, India Smart Grid Forum; Aamir Hussain Khan, Chief Information Security Officer, Tata Power Delhi Distribution Limited; and Chanmeet Singh, Programme Lead, CEEW.

Publications team: Kartikeya Jain (CEEW); Alina Sen (CEEW); The Virtual Paper; Madre Designs; and FRIENDS Digital Colour Solutions.

Organisation: The **Council on Energy, Environment and Water (CEEW)** is one of South Asia's leading not-for-profit policy research institutions. The Council uses data, integrated analysis, and strategic outreach to explain—and change—the use, reuse, and misuse of resources. It prides itself on the independence of its high-quality research, develops partnerships with public and private institutions, and engages with the wider public. In 2020, CEEW has once again been featured across nine categories in the *2019 Global Go To Think Tank Index Report*. It has also been consistently ranked among the world's top climate change think tanks. Follow us on Twitter @CEEWIndia for the latest updates.

COUNCIL ON ENERGY, ENVIRONMENT AND WATER (CEEW)

ISID Campus, 4 Vasant Kunj Institutional Area
New Delhi - 110070, India
T: +91 (0) 11 4073 3300

info@ceew.in | ceew.in | @CEEWIndia | ceewindia