

CYBER SECURITY VISION FOR 2030



August 2021

CYBER SECURITY VISION FOR 2030

INTRODUCTION

Mission-critical infrastructure is a target in cyber attacks perpetrated by state-sponsored actors, criminal gangs, and terrorist organizations. The frequency and potential severity of these attacks are increasing.

The Electric Power Research Institute (EPRI) described the current state of cyber security for the electricity subsector in its white paper titled [“Preparing for the 2030 Energy System: Why We Need a New Cyber Security Vision.”](#) As noted in that white paper, the electricity subsector must revise its concepts of Operations Technology (OT) cyber security and its role to safeguard against future attacks conducted for profit or for other motives. To most effectively do that, cyber security must transition into an essential embedded design in utility operations. This 2030 Security Vision identifies the critical future states for cyber security in the Electric Sector and the gaps that will need to be overcome to get there.

Our first actions were to organize a collaborative group of utilities and other stakeholders to discuss four electricity subsector metatrends and their OT cyber security impacts. Our discussions focused on the impacts utility cyber security professionals are seeing firsthand. This series of discussions were conducted over several months and culminated in identification of drivers, objectives, needs, and impacts to the electricity subsector. This 2030 Cyber Security Vision documents these discussions and while the focus is on OT cyber security, some of the needs, like those invoking utility workforces, have ramifications beyond the human resources involved in cyber security.

“The cyber security threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation.”

- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 2021

ROADMAP DEVELOPMENT PROCESS

This cyber security collaborative roadmap development process consisted of these phases:



CURRENT STATE: WHERE IS CYBER SECURITY TODAY?

The previous white paper identified a significant and dangerous gap for the electricity subsector. We lacked a clear cyber security strategy that helps utilities and other stakeholders move beyond event-driven actions that are too often based on news like the Solarwinds and Colonial Pipeline attacks. EPRI's Cyber Security research team focused on power delivery (transmission and distribution to grid edge) and generation-initiated activities to address this strategic gap.

DRIVERS: WHICH FORCES ARE SHAPING CYBER SECURITY DEVELOPMENT AND USE?

- Foundational security and resilience – the increasing reliance on electricity services increases the importance of strong cyber security.
- Value transformation – the increasing recognition of the strategic role of OT cyber security in utilities.
- Digital transformation – the transformation to software-defined grid operations.
- Decarbonization – the shift of generation sources from carbon-intensive to low-carbon.

CYBER SECURITY VISION FOR 2030

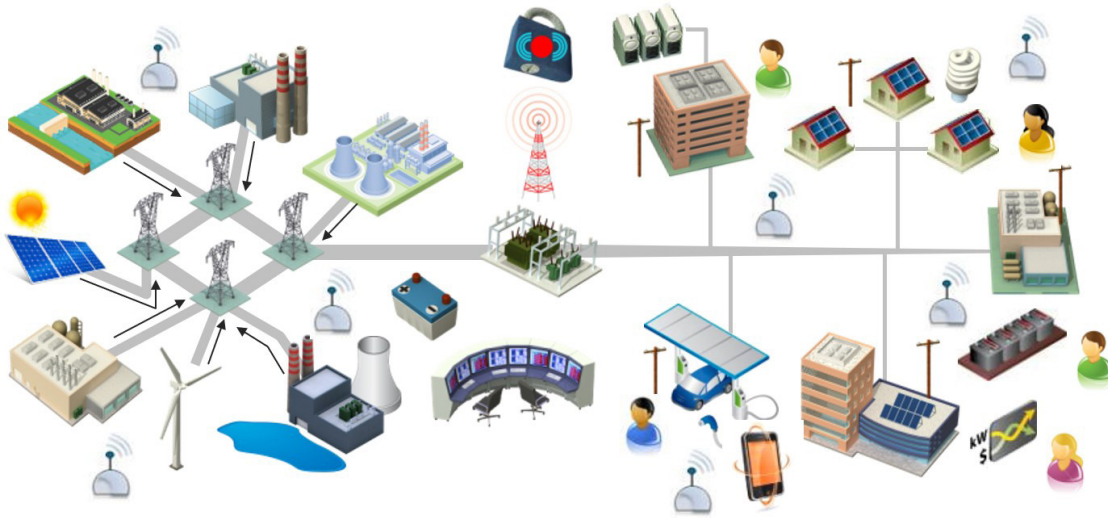






Figure 1: State, national and international policies and corporate strategies addressing climate change are driving the change point that will result in a significant evolution in how electricity will be generated and consumed, how the grid will be managed, what energy services will be offered and by which stakeholders.

FUTURE STATES: CYBER SECURITY FOR 2030

			
FOUNDATIONAL SECURITY AND RESILIENCE	VALUE TRANSFORMATION	DIGITAL TRANSFORMATION	DECARBONIZATION
Identify <ul style="list-style-type: none"> Standardized Digital Models of Assets, Systems, and Networks Asset and configuration management Supply chain security 	Strategic cyber security investments reflect a resiliency-based approach	Have the right data at the right time	Secure deployment of ubiquitous electrification, efficiency, and environmental stewardship
Protect <ul style="list-style-type: none"> Access control System architecture and isolation Risk-based remote access 	Use of standard, industry-accepted OT cyber security metrics for strategic and tactical decisions	Maintain effective critical infrastructure operations that meet changing expectations at the lowest possible cost	Secure transactive energy markets, grid services, and distributed dispatchability
Detect <ul style="list-style-type: none"> Anomalies and events Continuous security monitoring 	Ubiquitous board-level cyber security governance	Security by Design (SbD) for OT systems	Affordability and Adaptability
Respond/Recover <ul style="list-style-type: none"> Automated responses Robust OT forensics capabilities Rapid isolation capabilities 	Shift from reactive to proactive cyber security planning	Have the right workforce skills at the right time	
	Asset lifecycle		
	Ingrained cyber security culture		



FOUNDATIONAL SECURITY AND RESILIENCE

DRIVERS, FUTURE STATES AND GAPS

The future states are further described below, including the gaps that must be addressed enable this future vision for cyber security.

FOUNDATIONAL SECURITY AND RESILIENCE

Drivers

- Future threats to critical infrastructure – existing cyber security programs may lack the responses to new types of attacks or zero-day exploits.
- Evolving power delivery, control system, and communications technologies – new innovations in the design and operation of the power system challenge OT cyber security resources to create programs and policies that accommodate the new technologies in parallel with legacy technologies.
- Regulatory oversight is expanding – national and state regulations impact more utility systems and go beyond transmission grids and into the increasingly dynamic distribution grids.
- Critical infrastructure is expected to be resilient – resiliency measures must support graceful degradation of systems to prioritize and protect key components and critical operational capabilities during significant events.

Identify: Future States and Gaps

Security posture and status is continuously tracked for all intelligent components and systems within the grid infrastructure. Security solutions account for isolated legacy designs as well as emerging standards based on new technologies. Key dependencies and relationships between systems are well understood to maintain overall grid resilience.

STANDARDIZED DIGITAL MODELS OF ASSETS, SYSTEMS, AND NETWORKS

Accurate, accessible, standardized, and machine-readable system design and configuration data that describes architecture and behavior is widely available and used to accurately represent complex OT systems. This capability is leveraged to optimize security controls, model and simulate cyber security risks, streamline contingency analysis, and enable the widespread use digital twin technologies.

Cyber Security Gaps:

- Limited adoption of a standard data format to structure and

format engineering and design documentation or configuration data

- Current engineering and design documentation has been formatted visually for human consumption
- Minimal integration of engineering and design documentation across organizational silos to reduce data duplication and eliminate inaccurate data
- Need to eliminate siloed practices and data storage sites so data and information is readily accessible to growing number of internal and external stakeholders
- Need for IT, OT, and communications teams to identify priorities, system dependencies and risks, and processes for standardization, normalization, and optimization of utility cyber security processes

ASSET AND CONFIGURATION MANAGEMENT

All relevant characteristics of critical assets are continuously tracked and validated to ensure appropriate security controls are in place. Critical hardware, software, and system design information is documented to provide an authoritative resource to verify that systems are configured properly. Information is available for various levels of analysis from individual components within a vendor device scaling up thru systems that incorporate multiple devices. All information is contained within standard information models and file formats to minimize duplication and leverage the same data across multiple systems.

Cyber Security Gaps:

- Need for innovative solutions to automate collection of asset and configuration information across a wide range of proprietary systems
- No single source of truth to reconcile cyber security asset and configuration information incorporated into asset management solutions
- Duplicate information is represented in multiple views for different purposes, no authoritative truth
- Need for more context between priorities that span business functions including IT, OT, and Communications
- Common understanding of risk and dependencies among different systems



FOUNDATIONAL SECURITY AND RESILIENCE

- Address existing technology and process silos to standardize the management of asset data and normalize priorities at the enterprise level
- Information models should accommodate both commodity IT assets and embedded and proprietary systems

SUPPLY CHAIN SECURITY

Vendors provide complete, machine-readable documentation of all 3rd party components, including hardware and software, to enable accurate assessments of supply chain risks.

Cyber security gaps:

- Need for more effective risk assessments that reflect the long-term outlooks for vendor support
- Lack of commonly referenced product security certifications
- Difficult for utility personnel to easily evaluate vendor code development practices
- No industry standard data model for vendor-provided documentation to support automated assessment tools such as EPRI's Cyber Security Data Sheet (CSDS)
- Lack of widespread adoption of standardized Software Bill of Materials (SBOM), Hardware Bill of Materials (HBOM), and Digital Bill of Materials (DBOM) in the operations technology vendor ecosystem
- Lack of vendor accountability for vulnerabilities resulting from poor security practices

"The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services. "

- Executive Order 14017 on America's Supply Chains, February 2021

Protect: Future States and Gaps

Appropriate protection based on risk-informed methodologies is applied at multiple levels to harden critical systems using minimal resources without negative impacts to power system operations. OT security controls prioritize system availability over data confidentiality where the two objectives conflict. Next-generation electric power system architectures are designed with multi-layered security strategies. Security solutions are interoperable and extensible and support dynamic trust levels.

ACCESS CONTROL

Comprehensive access control, logging, and federated identity solutions are employed to monitor and protect all OT grid control and communications systems. Where legacy systems are still in service without native security controls, modular security solutions are employed to support to provide a base level of access control.

Cyber Security Gaps:

- Lack of zero trust concepts and solutions developed and tested for OT environments
- Need for utility deployment of more granular network segmentation solutions for OT environments without excessive maintenance requirements
- Lack of a standard approach to federated identity solutions for OT systems
- Need for improved coordination between cyber and physical security controls to enhance cyber protections for assets deployed outside the protected substation boundaries

SYSTEM ARCHITECTURE AND ISOLATION

Electric power control and communication systems are categorized based on a systematic risk assessment process. Using relative risk metrics, system architecture is engineered and designed to enable appropriate network segmentation and zero-trust principles to limit the impact of compromised systems. Dependencies and relationships among critical systems are well documented, and communications networks are designed to support isolation during an active cyber event.

Cyber Security Gaps:

- Lack of accurate documentation that captures cross-system dependencies



FOUNDATIONAL SECURITY AND RESILIENCE

- Limited perspective of risk associated with specific systems due to organizational and technology silos
- Need for more granular and dynamic evaluation of trust at all system levels

RISK-BASED REMOTE ACCESS

Critical systems support remote and automated management without introducing excessive risk of unauthorized access or misuse. All required vendor support access is enabled only after a detailed risk assessment and access systems are limited to enable only the minimum required functionality.

Cyber Security Gaps:

- Need for additional validation measures for remote reconfiguration or updates to mitigate compromise or system failure
- Technical security controls need to be tied to explicit security policy to enforce conditions for remote access
- Enhance visibility and granularity of configuration to enforce policy using technical controls
- Lack of confidence in remote updates manually deployed from a central location
- Need for targeted workforce training on secure use of remote access and automated management systems.

Detect: Future States and Gaps

Utilities continuously monitor all critical OT systems for anomalies, detect incidents in real time by fusing a variety of data sources including threat intelligence, security, and operations events and can share data to support a national framework for security monitoring.

ANOMALIES AND EVENTS

All relevant events and logs are aggregated and contextualized to assist electric power stakeholders with detection of any unauthorized or malicious activity. Events should be presented in a way that prioritizes relative risk and enables operators to make fully informed decisions rapidly. Anomalous events are characterized by their deviation from expected operation of the system "as-designed" based on a digital model and not solely in reference to an initial baseline.

Cyber Security Gaps:

- No existing information models are commonly used to describe relationships within and between power systems, control systems, and communication systems
- Organizational and information silos complicate the effort to provide context to received events
- Current practices rely on initial system baselines to define expected vs anomalous events
- Need for utility adoption of digital twin modeling and other technologies to support real-time emulation of the system to described expected behavior and communications traffic
- Need for vendor-provided documentation to support to the creation of virtual environments to baseline expected system behavior
- Expanded standard information models to describe relationships within and between power systems, control systems, communications systems, and cyber security controls
- Need for new operations tools to support maturity progression from event notification through event prediction to automated event response

CONTINUOUS SECURITY MONITORING

Continuous security posture monitoring for all electric power system architectures and across cyber-physical domains is widely adopted by electric power asset owners and operators.

Cyber Security Gaps:

- Lack of solutions that support layered scanning from device to system levels and report potentially compromised devices for additional investigation
- Need for network architectures and capacities to accommodate continuous, real-time monitoring from grid edge to control center
- Need for solutions that can support continuous safe scanning or device interrogation in legacy and heterogeneous environments



FOUNDATIONAL SECURITY AND RESILIENCE

Respond/Recover: Future States

Electric power stakeholders quickly mitigate cyber incidents, continue operating in degraded conditions during cyber incidents, expedite return to normal operations, and derive lessons learned from incidents.

AUTOMATED RESPONSES

Utility security systems have extensive, computer-readable playbooks that inform automated and manual responses to incidents in real time.

Cyber Security Gaps:

- Lack of trust in automated systems to replace and/or supplemental human-initiated incident responses
- Limited integration of OT systems in the security information and event management (SIEM) and security orchestration, automation, and response (SOAR) environment
- Realization of artificial intelligence (AI) and machine learning (ML) tools to offset need for Tier 1 analysts
- Lack of basis to understand the risks and rewards of letting automation react to threats in an operational environment
- Lack of tools to support automated response that leverage AI or other advanced data applications

ROBUST OT FORENSICS CAPABILITIES

Utility OT systems deploy a common data model that enables consistent extraction of low-level device metrics to improve rapid forensics analysis.

Cyber Security Gaps:

- Lack of vendor support for full, low-level system access to collect forensics data from control and security systems

- Lack of solutions that accommodate legacy and heterogeneous environments in control centers and substations

RAPID ISOLATION CAPABILITIES

Rapidly deployed isolation capabilities can mitigate attack impacts and preserve critical operations.

Cyber Security Gaps:

- Limited use of flexible isolation techniques in OT environments limits granularity of isolation actions
- Insufficient availability of data flow models and understanding of dependencies between OT systems
- Incomplete and insufficient modeling of data flows, relationships, and dependencies across corporate and OT systems
- Lack of resources to safely design and test rapid network isolation technologies

“The threat from cyber attacks by nation states, terrorist groups, and criminals is at an all-time high. Now more than ever, grid security is inextricably linked to reliability. The North American bulk power system (BPS) is among the nation’s most critical infrastructures. Virtually every critical sector depends on electricity.”

*- James B. Robb, President and Chief Executive Officer,
North American Electric Reliability Corporation,
Testimony Before the Committee on Energy and Commerce
Subcommittee on Energy
July 2019*



VALUE TRANSFORMATION

VALUE TRANSFORMATION

Drivers

- Resiliency expectations and requirements for new grid operations will trigger significantly larger investments in cyber security.
- Performance accountability - Utility executives and boards need metrics that track performance and communicate the value of cyber security investments.
- Increasing stakeholder awareness of importance of cyber security for critical infrastructure based on publicized cyber-attacks.
- Current reactive business practices and approaches have proven to be ineffective against explosive growth of new threat actors and attack vectors.

Future States and Gaps

STRATEGIC CYBER SECURITY INVESTMENTS REFLECT A RESILIENCY-BASED APPROACH

Utilities must intelligently invest in cyber security to defend against existing and emerging threats and improve recovery from cyber-attacks.

Cyber Security Gaps:

- A cost recovery model for cyber security investments is needed to offset the increased spending requirements
- Need process modifications to ensure spending aligns with strategic objectives and that proposed solutions integrate with existing and future cyber security architecture

WIDE USE OF STANDARD, INDUSTRY-ACCEPTED OT CYBER SECURITY METRICS FOR STRATEGIC AND TACTICAL DECISIONS

Quantitative metrics about OT cyber security support data-driven decisions that increase the effectiveness and value of cyber security programs.

Cyber Security Gaps:

- The utility sector needs an accepted de facto standard for cyber security metrics, benchmarks, and performance goals to gauge performance
- Need standard return-on-investment (ROI) model for OT cyber security investments

UBIQUITOUS BOARD-LEVEL CYBER SECURITY GOVERNANCE

Utilities adopt board-level cyber security oversight and governance committees to ensure visibility and build support.

Cyber Security Gaps:

- Institute regular executive and board communication related to enterprise cyber security (includes OT) risk beyond compliance and audit status
- A standard reporting structure, content and frequency is needed to communicate results

SHIFT FROM REACTIVE TO PROACTIVE CYBER SECURITY PLANNING

Future potential cyber security threats and attack vectors to the utility subsector are included in the strategic and tactical operating plans for utilities.

Cyber Security Gaps:

- Need inclusion of cyber-attack impacts in all utility disaster planning and business recovery scenarios and exercises
- Develop processes that identify vulnerabilities and mitigation practices that reduce the impacts of a changing cyber threat landscape

ASSET LIFECYCLE

Utilize asset lifecycle processes that ensure proper technology and controls are in place to guarantee cyber security is risk-informed and built-in at each stage of the lifecycle.

Cyber Security Gaps:

- Buy-in from each business unit is needed for successful implementation
- Need for industry-wide adoption of the EPRI Technical Assessment Methodology (TAM)
- Cyber security considerations built into the plant asset criticality determination process

INGRAINED CYBER SECURITY CULTURE

Cyber security is a company value, reflected in mission statements.

Cyber Security Gaps:

- Need for a “security first” approach like the “safety first” approach in utility processes, acquisitions and design and operations principles to create an embedded security culture
- Need to embed cybersecurity security priorities into the grid planning, design, operations, and maintenance cycles
- Need for subsector-wide recognition of cyber security as a critical business function in utilities and ownership across utility departments
- Need for increased cyber security knowledge-based training for non-cyber security positions
- Need for role-based IT-OT cyber security cross-training and coordination



DIGITAL TRANSFORMATION

DIGITAL TRANSFORMATION

Drivers

- Data Ubiquity – Increasing velocities, varieties, and volumes of data from new sensors, applications, devices, and systems are leveraged to optimize utility operations and cyber security functions.
- Financial Constraints – Existing and new regulations influence investment decisions as cost recovery mechanisms force hard budget choices for cyber security programs.
- Critical Infrastructure Soft Targets – Competing demands of security versus accessibility and visibility for stakeholders, combined with new business models and customer expectations introduce new vulnerabilities and make utilities prominent cyberattack targets.
- Workforce Constraints – Hiring and retention challenges for skilled cyber security resources are exacerbated by new technologies that require different skills.

Future States and Gaps

HAVE THE RIGHT DATA AT THE RIGHT TIME.

Secure access to high priority cyber security and grid-operational data must occur at high levels of availability and integrity. Other data requires high levels of confidentiality.

Cyber Security Gaps:

- Need for defined data governance and management policies to handle increased data and new data for existing and emerging applications and stakeholders
- Lack of standardized data models for cyber security data to enable advanced data applications
- Need for flexible and scalable data architecture frameworks that support automated and distributed decision-making

MAINTAIN EFFECTIVE CRITICAL INFRASTRUCTURE OPERATIONS THAT MEET CHANGING EXPECTATIONS AT THE LOWEST POSSIBLE COST

Utility processes must be flexible, scalable, and secure to provide trust for regulators and customers.

Cyber Security Gaps::

- Standardized methods, reference architectures, and risk models

for enabling use of new technologies like cloud services.

- Improved cost models to analyze technology and service alternatives.
- Need for new technologies that analyze high volumes and velocities of data to identify intrusions and Advanced Persistent Threats (APTs) faster

SECURITY BY DESIGN (SBD) FOR OT SYSTEMS

Utility OT systems are designed and managed with a digital-first approach with provisioning processes managed through machine-readable definition files, enabling Security by Design approaches to automate security baselines, configuration, and auditing.

Cyber Security Gaps:

- Lack of widespread use of digital technologies such as virtualization, containerization, and microservices in OT systems and devices
- Need for industry-level adoption of modern messaging frameworks, network protocols, and communications technologies to support a first-principles approach to grid operations
- Clear and concise regulatory and compliance requirements that rapidly accommodate new digital technologies and services
- Lack of DevSecOps and Infrastructure as Code principles and supporting technologies in the development and management of OT and IoT devices
- Need for new standards for security configuration languages to support digitally-driven OT system design models

HAVE THE RIGHT WORKFORCE SKILLS AT THE RIGHT TIME

Digital transformation requires new data science skills in addition to traditional OT and IT cyber security knowledge and competencies.

Cyber Security Gaps:

- Need for tools and best practices recommendations to make informed decisions about outsourcing versus internal resource use to support existing and new technologies and processes.
- Need for tools and models to conduct sophisticated cost/benefit analyses on best workforce strategies
- Lack of workforce hiring and retention strategies that reflect remote worker considerations



DECARBONIZATION

DECARBONIZATION

Drivers

- **Public Policy** – Legislation and directives at local, state, and national levels set goals for economy wide greenhouse gas reduction, promote innovations for renewable and low-carbon technologies, and enable transactive markets for distributed energy resources (e.g., FERC 2222).
- **Green Investments** – Driven by financial risks associated with climate change, surging valuations of clean energy businesses, and cost trends for renewables, “green finance” goes mainstream and shifts funding away from fossil fuels to renewable and low-carbon generation technologies.

Consumer Interests – Consumer demands for low cost electricity, reduction in carbon footprints, reliability, and democratization of energy production encourages adoption of distributed energy resources and participation in community choice aggregation programs.

- **Corporate Strategy** – Public policy, investors, and consumer demands drive cross-sector corporate strategies to include goals for reduced or net-zero carbon emissions in their lines of business.

Future States and Gaps

SECURE DEPLOYMENT OF UBIQUITOUS ELECTRIFICATION, EFFICIENCY, AND ENVIRONMENTAL STEWARDSHIP

Carbon reductions will require electrification and efficiency innovations across multiple business sectors and transformations within transactive energy markets.

Cyber Security Gaps:

- Need for a Trust Framework for Interconnected DERs that outlines cyber security requirements for interconnection agreements and certifications
- Need for a new risk analysis and mitigation methods and tools that support identification of vulnerabilities and security requirements for massive numbers of new interconnections and supporting communication networks
- Need for supply chain security across lifecycles for all components and subcomponents of DERs and transactive energy market systems used by all market participants

SECURE TRANSACTIVE ENERGY MARKETS, GRID SERVICES AND DISTRIBUTED DISPATCHABILITY

Distributed energy resources (DERs), utility-scale renewable plants and supporting grid services require interoperability in electricity markets and grid management systems to enable secure and efficient operations and settlements that assure trust.

Cyber Security Gaps:

- Need for trust mechanisms for interconnected DERs to enable frictionless multi-party grid interactions with customer and aggregator connected systems.
- Lack of a cyber security framework for transactive energy markets to identify and mitigate emerging security risks and increasing attack surfaces introduced through DERs and aggregated generation.
- Need data privacy and protection policies and interoperable solutions to protect consumer energy production data, personally identifiable information (PII), sensitive market data acquired and exchanged by multiple parties.
- Incident response coordination is needed to inform how interdependent grid participants must respond to critical cyber incidents.

AFFORDABILITY AND ADAPTABILITY

Energy markets expand and adapt to new stakeholders and energy resource types, building cost-reduction pressures on capital, operational, and maintenance costs for generator-based resources and DERs while ensuring proper security controls are deployed.

Cyber Security Gaps:

- Need a Cloud Security Framework for DERs and traditional generation sources – a reference architecture to enable grid applications to securely adapt to cloud-based platforms.
- Lack of risk and vulnerability mitigation best practices that help ensure utilities can adapt to regulatory environments and dynamic attack vectors.
- Need cyber security cost-benefit analysis and planning tools to address massive DER deployments.
- Need intrinsic Cyber Security for Residential Scale DERs to avoid cost or deployment barriers for prosumer participation in transactive energy markets.

CYBER SECURITY VISION FOR 2030

PATH FORWARD

This white paper describes a set of future states and gaps that must be addressed to achieve an intrinsically secure energy system by 2030. However, for this Vision to be actionable, the subsector will also need to develop and adopt a new ten-year cyber security Roadmap. The next phase of this project will engage with industry stakeholders to identify and develop the actions plans necessary to address the gaps identified and achieve the 2030 Cyber Security Vision.

ACKNOWLEDGMENTS

EPRI would like to thank the attendees of the 2030 Cyber Security Vision Working Group meetings, which consisted of more than 40 individuals representing 20 utilities and industry organizations. The creation of this Vision would not have been possible without their insights and guidance.

EPRI RESOURCES

Project Lead: Galen Rasche, *Senior Program Manager*, Power Delivery and Utilization Sector

Project Co-Lead: Christine Hertzog, *Principle Project Manager*, Power Delivery and Utilization Sector

Foundational Security and Resilience Lead: John Stewart, *Principal Technical Leader*, Power Delivery and Utilization Sector

Value Transformation Lead: Ralph King, *Program Manager*, Power Delivery and Utilization Sector

Digital Transformation Leads:

Christine Hertzog, *Principal Project Manager*, Power Delivery and Utilization Sector

Ben Sooter, *Principal Project Manager*, Power Delivery and Utilization Sector

Decarbonization Leads:

Xavier Francia, *Senior Technical Leader*, Power Delivery and Utilization Sector

Jason Hollern, *Program Manager*, Generation Sector

POINTS OF CONTACTS

Galen Rasche, *Sr. Program Manager*,

650.855.8779, grasche@epri.com

Christine Hertzog, *Principle Project Manager*,

650.314.8111, chertzog@epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

Note

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together... Shaping the Future of Energy™