NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2025 Emerging Security Risks Survey Supplemental Information

July 2, 2025

The security risks listed below are accompanied by a risk statement and a hypothetical risk scenario (s). The provided hypothetical risk scenario is only one example and is not meant to exclude other possible valid risk scenarios. Use these details to assist in completing the 2025 Emerging Security Risks and CIP Standards Roadmap - Survey of Industry.

Security Risks

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Supply Chain	Advanced Persistent Threat Actors (APTs) or cybercriminals could counterfeit or insert back-doored components into bulk-power system equipment, compromise software applications or software update channels, potentially compromising Confidentiality, Integrity, Availability (CIA) of Bulk Power System (BPS) elements resulting in widespread impacts to the grid.	Scenario 1) A manufacturer country embeds rogue hardware in replacement relays or other critical electric grid equipment; once installed, a remotely accessible backdoor allows an adversary to disable trips during a July heatwave, causing cascading outages across a reliability coordinator's footprint. Scenario 2) SolarWinds-style compromise inserts malware into Energy Management System (EMS) or component patch; The signed update spreads and the adversary then pivots into Operational Technology (OT) environments eventually coordinating an attack in conjunction with extreme weather events or with war time actions., SolarWinds-style compromise inserts malware into EMS; the signed update spreads and the adversary then pivots into OT environments eventually coordinating an attack in conjunction with extreme weather events or with war time actions.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Ransomware / Malware	Adversary malware infects Information Technology (IT) and OT systems by encrypting or simply wiping data.	Ransomware variant crosses IT-OT boundary through overly permissive firewall rules and encrypts several entity OT devices. A ransomware note is displayed on impacted Human Machine Interfaces (HMI).
Insufficient Low Impact Security	Low impact security controls mandated by NERC Critical Infrastructure Protection (CIP) standards may be insufficient to protect against emerging threats.	Grid assets without Multifactor Authentication (MFA) in place are compromised via valid account credential reuse after being stolen through a phishing campaign allowing an attacker to install a keylogger on an engineering workstation.
Cloud Environment Compromise	OT/IT workloads in public clouds can expose entities to security misconfigurations and attacks arising from shared-tenant environments leading to data loss or unavailability of necessary critical workloads.	Misconfigurations of identity and access management (IAM) policies in a cloud service provider (CSP) allows an attacker to spawn virtual machines (VM) inside an Operational Technology (OT) virtual network (vNet), exfiltrate critical system data, and then execute a Distributed Denial of Service (DDoS) attack against a widely used distributed energy resource (DER)-control application programming interface (API) tripping offline 1500 MW solar.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Compromise of Category 2 Generator Owner (GO) and Generator Operator (GOP) Inverter Based Resource (IBR) facilities	Cyber compromises targeting sub-BES facilities (i.e., falling below NERC CIP standards applicability) constitute risk to grid reliability as coordinated attacks on CAT 2 GO / GOP could negatively impact grid operations.	Poorly secured IBR facilities could be attacked in a coordinated manner staged from one facility to another through a flat stretched network penetrating unpatched firewalls leading to attackers shutting down inverters or maliciously manipulating frequency and voltage signals.
Insider Threats	Intentional - Maliciously motivated employees illegitimately exploit privileged access or knowledge to IT or OT data, systems, or networks resulting in negative operational impacts or data exfiltration. Negligence – Exposes an organization to a threat through carelessness. Negligent insiders are generally familiar with security and/or IT policies but choose to ignore them, creating risk for the organization. (DHS) Accidental – Mistakenly causes an unintended risk to an organization (DHS).	Example of an “intentional” insider threat includes a disgruntled contractor uploads malware containing a logic bomb to several programmable logic controllers (PLC) across a Transmission Operator footprint. A timed failure of many devices during peak summer demand forces emergency load shed. Examples of a "negligent" insider threat includes allowing someone to “piggyback” through a secure entrance point, misplacing or losing a portable storage device containing sensitive information, and ignoring messages to install new updates and security patches. Examples of an "accidental" insider threat includes mistyping an email address and accidentally sending a sensitive business document to a competitor, unknowingly or inadvertently clicking on a hyperlink, opening an attachment in a phishing email that contains a virus, or improperly disposing of sensitive documents.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
End-of-Life Systems	Aging and vendor unsupported operating systems, software, and / or hardware devices remain unpatched in OT environments.	A malware worm exploiting a vulnerable or overly promiscuous server message block (SMB) protocol firewall rule on an outdated Microsoft Windows HMI spreads to primary and backup Supervisory Control and Data Acquisition (SCADA) servers; operators lose control and visibility leading to outages.
Network Based Attacks	Low skill distributed denial of service (DDoS) cyberattacks are increasing and placing reliable operations of the grid at risk.	A DDoS attack disables both primary and back-up control center communications that utilize public networks causing a loss of visibility for a large generation company interrupting grid operations for several hours.
Insecure Protocols	Insecure legacy protocols without native security features create vulnerabilities that could lead to cyber compromise that negatively impact grid operations.	A threat actor takes advantage of the insecure distributed network protocol 3 (DNP3) protocol used in the electric grid, which lacks security protections, performs a man-in-the-middle attack, and is able to intercept valid signals and send malicious commands to disable remote terminal units (RTU) in the field.
Phishing & Social Engineering	Deceptive tactics allow harvesting of legitimate account credentials or bypassing physical security controls.	Spoofed vendor email entices a technician to download malicious files which install a Remote Access Trojan (RAT) on a substation HMI.
Insufficient Cybersecurity Workforce	A lack of qualified personnel could make energy sector entities vulnerable to increasingly sophisticated cyberattacks, which may include ransomware, phishing, and malware.	Grid Asset Owners and Operators (AOO) across the industry are unable to appropriately staff their OT security teams as they compete for talent with other industries, leading to a less secure system state.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Physical Attacks on Infrastructure	Theft, ballistic damage, vandalism, and intrusion (tampering) all pose physical security risks to grid assets which could impact reliability. The current challenges around the manufacture of transformers or similar equipment in a timely manner and resulting supply shortages could aggravate risk by inhibiting system restoration from a natural disaster or man-made attack. The long lead times, combined with limited domestic production, increased load growth, and manufacturing capability, could all impact reliability.	Scenario 1) A Metcalf style coordinated ballistic attack damages several transformers causing distribution-wide outages lasting for several hours. Scenario 2) Vandals cut fiber optic cables (unknown intentional or purely criminal) causing generation unavailability and customer outages. Scenario 3) A spike in copper prices motivates thieves to steal grounding from a substation causing customer outages.
Weaponization of Drones	Physical security attacks facilitated by drones, which could be equipped with explosives could cause disruptions to reliability.	An anarchist group equips several drones with homemade explosives and blows up several large transformers along with other equipment at several substations simultaneously causing regional outages.
Large Load Manipulation	Malicious manipulation of large loads could destabilize the grid.	Scenario 1) Control systems such as Building Management Systems (BMS), Heating, Ventilation, and Air Conditioning (HVAC), or other support systems are compromised which leads to a forced load drop at a data center. Scenario 2) A botnet infects a 100 MW crypto mining farm rapidly toggling miners, causing oscillations that trip a collocated gas plant and cause an outage.
Exploitation of Public Telecommunications	Nation-states compromise telecommunications entities allowing traffic associated with electric grid operators' infrastructure to be intercepted, modified, exfiltrated, or otherwise disrupted.	An adversary compromises internet backbone routers, intercepts traffic (all types, encrypted, unencrypted, or poorly encrypted), exfiltrates data associated with grid operations preparing for a larger future attack and executes a Distributed Denial of Service (DDoS) attack against the internet service provider (ISP) causing grid disruptions across an RC footprint.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Targeting of DER Aggregator (DERA) Control Systems	The cyber compromise of cloud-based DERA management platform via any attack method could enable manipulation of sizable DER generation or manipulation of demand response programs that could result in grid impacts.	A DERA cloud control system is compromised; Malicious control signals are sent to thousands of inverters which causes frequency oscillations triggering a load-shed event or load manipulation signals are sent to demand response program participants causing enrolled smart devices to increase load during demand response events.
Electric Vehicle Supply Equipment (EVSE)	Networked electric vehicle chargers and their physically unsecure nature creates new grid-edge attack surfaces.	Attackers exploit a Linux kernel vulnerability and eventually infect one thousand public charging stations with a Botnet. After using these stations for other malicious intentions, the Botnet owners send commands simultaneously to all the stations to exceed their kilowatt draw thresholds. This causes feeders to overload, protective relays trip, and local instability occurs. (Scenario would require vehicles to be attached)
Unregistered 3rd-Party Operators	Non-NERC registered entities (operating within or outside of the United States) with remote access to generation facilities for monitoring, maintenance, or control capabilities could be targeted via cyber-attacks leading to risk to the grid.	Scenario 1) A breach at a wind generator OEM enables an attacker with remote access capability to US grid assets to push a malicious firmware update to multiple wind generators allowing for a future grid impacting attack to take place.
Ineffective Incident Response & Recovery Planning	Disjointed, out of date, or untested Incident Response Plan (IRP) playbooks delay containment, inhibit recovery, and allow attackers to erase forensic attack data.	Simultaneous substation shootings and a DDoS attack on an ISP effects SCADA communications and takes 8 hours to coordinate the response, prolonging local blackouts.
Targeting of Artificial Intelligence (AI) Tools and Capabilities	Targeting of AI through maliciously poisoned AI training inputs may destabilize grid operations for early adopters of AI technologies.	A poisoned dataset causes autonomous voltage monitoring systems to oscillate tap changers in several transformers causing instability and unplanned load shedding.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Regulatory Lag	Regulations inherently lag behind innovation and this uncertainty may delay or influence the adoption of new security technology that could improve defenses.	A large utility cancels a cloud enabled security solution while awaiting guidance in connection with NERC CIP standards; An APT compromises a large entity and dwells in the networks for over 200 days undetected, triggering a timed load-loss event in a peak-demand scenario.
Compromised Application Programming Interface Keys	Insecure or leaked entity API security keys enable unauthorized access and data theft.	An entity's software developer accidentally posts API security keys to GitHub; An attacker obtains the API security key from the public repository and compromises the entity's CSP tenant allowing an attack that shuts down a 50 MW battery installation.
Compromise of Smart Distribution Switches	Smart distribution switches compromised through other interconnected systems allow attackers to disrupt power at the distribution level.	An Advanced Distribution Management System (ADMS) Software as a Service (SaaS) integration is compromised allowing an attacker to manipulate load causing a total loss of monitoring and control in a distribution provider (DP) footprint.
Compromise of Metering Infrastructure	Compromise of advanced distribution infrastructure such as Advanced Metering Infrastructure (AMI) or metering integrated Customer Information Systems (CIS) potentially degrades operations and allows pivoting into OT systems.	A successful phishing campaign targets a customer service agent working from home and steals credentials for logging into a SaaS CIS solution. The attacker remotely disables meters for several major industrial customers leading to voltage and frequency deviations at the Transmission & Distribution (T&D) interface.
Compromise of Synchrophasor Systems and Data Used in Real-time Operations	Manipulated Phasor Measurement Unit (PMU) data misleads a state estimator causing unsafe system conditions.	An unprotected Transmission Operator (TOP) PMU system is compromised, and the PMU data is spoofed sending incorrect Global Positioning System (GPS) timestamps; The RC's state estimator that receives the TOP PMU data miscalculates phase angles which triggers unwarranted remedial-action schemes.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Compromise of Blackstart resources	Insufficiently secured blackstart restoration assets could be compromised and contribute to prolonged outages.	An attacker misconfigures generation remote start settings and tampers with diesel fuel sensors and logging; post-hurricane blackstart operations are delayed for hours.
Compromise of Power-Line Communication	Adversaries may exploit vulnerabilities in PLC systems used to communicate between substations leading to unauthorized access, disruption of protection schemes, or manipulation of substation controls systems resulting in grid instability or widespread outages.	An APT gains access to a poorly secured PLC endpoint via a compromised substation. Using this access the attacker injects false relay commands over PLC link triggering malicious breaker operations resulting in cascading faults and a blackout.
Insecure Usage of Protocol Converters	Converters used to bridge IT or OT networks expose insecure legacy devices without built in security features.	A critical OT network is bridged with an IT network using a serial to IP protocol converter. Lack of consideration of securing the created network bridge allows an attacker to maliciously communicate with downstream OT devices and alter relay settings degrading system resiliency.
Compromise of Mobile Devices	Vulnerable mobile devices utilized for various purposes (e.g., MFA, mobile badges, email, cloud services (O365), logs & alerts, etc.) could be leveraged to facilitate an attack.	A stolen phone, or e-SIM hijacked device, allows attackers to bypass MFA controls, or bypass Physical Security Perimeter controls via a mobile badge.
Unusable Backups	Asset owner(s) could be unable to operate for extended duration after a successful cyber or physical attack.	Malware encrypts mission critical servers at a Control Center. Backups are unavailable, out of date, or otherwise unusable.
Compromise of Market Systems	Manipulation of Independent System Operator (ISO) / Regional Transmission Organization (RTO) energy market systems, data, bids, or awards disrupting dispatch orders leading to grid instability.	API exploit alters bid data, causing ISO to mis-dispatch units; imbalance forces rolling blackouts and price spikes.

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Quantum Computing	Advancements in quantum computing technology could break modern cryptography which underpins internet communications today allowing adversaries to compromise CIA.	Chinese APTs hack into telecom giants allowing them to steal large amounts of encrypted data which is then unencrypted offline using quantum compute.
Stolen Critical Energy Infrastructure Information or BES Cyber System Information	Exfiltration of communication network architecture, one-line diagrams and model data enabling more precisely targeted attacks.	Spear phishing the lead engineer at an RC allows an attacker to steal one-line drawings and modeling data; months later ballistic attacks target critical buses and infrastructure identified in the stolen data.
Compromise of Geographical Information Systems (GIS)	Compromise of GIS or Outage Management System (OMS) data and integrations could potentially inhibit system recovery after an incident (cyber or extreme weather) and degrade system operators' ability to recover.	A hacker exploits an unpatched vulnerability that allows access into the distribution provider corporate network. Poisoned data in these systems degrades the DP ability to recover from extreme events.