Recommendations for Solar Energy Cybersecurity

CYBERSECURITY CONSIDERATIONS

- There is rapid and continued growth in grid-connected, large-scale solar inverter-based resources (IBR) and behind-the-meter distributed energy resources (DER).
- IBR/DER cybersecurity attacks may impact the energy critical infrastructure sector.
- Combined use of smart-grid technologies, mobile applications, and cloud-based control systems introduces several risks, including:
  - New cyber-attack vectors for the U.S. electric grid
  - Expanded attack surfaces
  - Malicious control of the IBR/DER cyber-physical system through the Internet
  - Logical or physical local ports could offer a foothold into networks (e.g., enterprise, operational, behind-the-meter)
  - Compromised Personally Identifiable Information (PII) or financial information resulting from compromised IBR/DER networks

CYBERSECURITY IMPACTS

IBR/DER vendors, owners, operators, aggregators, grid operators, and government organizations must understand cyber threats targeting IBR/DER can create both localized and widespread impacts:

Local Impacts

- Failure of operations
- Damage to equipment
- Loss of IBR/DER service availability
- Theft of PII and financial information
- Compromise of IBR/DER safety systems

Large-Scale Impacts

- Harvesting of PII and financial information
- Shutdown of IBR/DER networks
- Exposure of upstream and partner IT networks to compromise
- Misconfiguration of IBR/DER grid-support functions leading to dangerous conditions
- Loss of consumer confidence in IBR/DER ecosystem
- Bulk power system reliability impact

OBSERVED WEAKNESSES IN IBR/DER EQUIPMENT

Field Equipment Hardening

- Unencrypted storage allows attackers to steal credentials for use in accessing IBR/DER or partner systems, networks, and cloud services.
- Debugging or other unused ports are not removed or disabled prior to deployment
- Default or generic system accounts using default or generic passwords, enabling malicious activities and preventing accountability.
- Host-Based Intrusion Detection Systems (HIDS) not enabled, logs and alerts not shared upstream to Security Operations Center (SOC).
- Local logs not enabled or integrated with a Security Information and Event Management (SIEM) system.
- System administrators cannot revoke access to shared or local accounts when personnel leave the organization or no longer require access.

Network Protection & Monitoring

- IBR/DER networks do not always support encryption for data-at rest or data-in-transit.
- Network-Based Intrusion Detection Systems (NIDSs) are not installed at key network locations, e.g., IT/OT DMZs, cloud firewall, or DER gateway
- Enterprise systems or IBR/DER networks may not require or enforce proper network segmentation.
- Regular vulnerability scanning and patching of backend/cloud infrastructure is not performed by IBR/DER owners/operators.
- Firmware updates are sent in cleartext or do not include authentication mechanisms

CONTACT:
Jay Johnson | jjohns2@sandia.gov, **Jon Hurtado** | jghurta@sandia.gov,
Bheshaj Krishnappa | bkrishnappa@seia.org, **Larry Collier** | larry.collier@nerc.net,
Dan Goodlett | dan.goodlett@nerc.net

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SEIA Solar Energy Industries Association®

Sandia National Laboratories

NNSA National Nuclear Security Administration

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2023-04512O

SECURITY RECOMMENDATIONS FOR THE IBR/DER ECOSYSTEM

SUPPLY CHAIN & EXTERNAL DEPENDENCIES MANAGEMENT

- Prepare IBR/DER for shipping via a formal process that includes specified paperwork to document the exact state of the IBR/DER when it leaves the facility.
- Perform quality assurance at each manufacturing step to ensure appropriate components are used and malicious hardware is not present.
- Disassemble, inspect, and inventory a sample of equipment arriving from external partners and locations.
- Add security mechanisms to protect cryptographic material during manufacture.
- Track all external libraries and software components for newly discovered vulnerabilities.
- Establish and maintain software (SBOM) and hardware bills of materials (HBOM).
- Create and maintain software golden images to check against tampering.

ASSET, CHANGE, & CONFIGURATION MANAGEMENT

- Create formal processes for uploading configuration baselines to corporate repositories.
- Stage updates for deployment using approval processes that require multiple personnel and a separation-of-duties model.
- Implement secure coding practices including integrity checks of code repositories and versioning control.
- Use digital signatures (code signing) for all updates.
- Use a password-protected bootloader that supports secure boot operations and verifies digital signatures and update package integrity.
- Encrypt all information storage devices within IBR/DERs.
- Disable unnecessary services and ports.

EVENT & INCIDENT RESPONSE, CONTINUITY OF OPERATIONS

- Create a Security Operations Center (SOC) that employs a security information and event management (SIEM) and/or security orchestration, automation, and response (SOAR) technologies.
- Ensure that all alarms, system login notifications, & critical events are prioritized and sent to a centralized logging service.
- Take remediation steps immediately when logs show critical events.
- Ensure roles and responsibilities are clearly documented for incident handling with predefined stakeholder communication plans.
- Ensure business continuity, incident response, and disaster recovery plans are reviewed & tested regularly. Document any lessons learned.
- Forge relationships with FBI field offices and other appropriate government organizations before a cybersecurity incident.

INFORMATION SHARING & COMMUNICATIONS

- Ensure information is classified adequately and access is controlled on a need-to-know basis.
- Encrypt all communications—internal and external to the IBR/DER where possible.
- All networks networks should apply best practices including network segmentation and security systems such as IDS and firewalls.
- Each IBR/DER should establish mutually authenticated connections to the system servers. Prevent communications between multiple IBR/DER devices and sites.
- Install firewalls and Intrusion Detection Systems (IDSs) at key network locations.
- Ensure that secure protocols are enabled whenever supported. Encrypt traffic over the network using a nondeprecated cipher suite.
- IBR/DER vendors and network operators should participate in information sharing programs to exchange pertinent cybersecurity information with the community.

IDENTITY & ACCESS MANAGEMENT

- Require individual system credentials. Do not reuse credentials across different systems.
- Disallow local credential storage physically inside the IBR/DER enclosure. Require updates to any default accounts and passwords upon first use.
- Limit the use of system/maintenance accounts. Shared credentials should be limited to only authorized users.
- Secure and back up critical credentials, keys, or other “secret” items in case of personnel departure or system failure.
- Configure NIST-compliant passwords and use multi-factor authentication to prevent compromised credentials from giving an attacker access.
- Ensure proper defense-in-depth by limiting physical and logical external access to equipment and systems using access control technologies.
- Employ access-control mechanisms & require authentication and authorization for IBR/DER reconfiguration, reprogramming, and firmware updates.

SITUATIONAL AWARENESS

- Employ physical security solutions and access logging for all equipment, manufacturing areas, and office spaces for authorized and unauthorized persons.
- Monitor network events and traffic for malicious anomalies. Consider using network-based and host-based IDSs.
- Protect and position tamper-detection sensors and alarms on IBR/DER sites and enclosures to prevent an attacker from bypassing them; consider installing sensors to detect signs of entry. Improve lock mechanisms to prevent picking or other bypass techniques.
- Install tamper-evident seals on internal covers to detect unauthorized access. Inspect these seals and internal hardware components during regular maintenance.
- Utilize vulnerability and configuration scanning to ensure systems are updated and do not have unauthorized configuration changes. Scan for unintentionally internet-connected IBR/DERs (e.g., Shodan).

WORKFORCE MANAGEMENT

- Ensure critical roles have proper redundancy in personnel.
- Identify any current or future training or recruitment gaps. Fill missing cybersecurity skills.
- Ensure cybersecurity best practices like the NIST Cybersecurity Framework are used for internal assessments, cyber hygiene, patching, supply chain and insider threat mitigations, etc.
- Evaluate competence of personnel with social engineering (e.g., spear phishing) audits and other education-based campaigns.
- Ensure clear roles, responsibilities, and separation of duties for the cybersecurity workforce.
- Ensure clear documentation of critical processes and communicate the document storage location for easy access

THREAT & VULNERABILITY MANAGEMENT

- Establish a patch management program with a process for identifying, prioritizing, acquiring, installing, and verifying the installation of updates.
- Establish a threat profile for the types of attacks that are common on IBR/DER networks and back-end systems to effectively respond.
- Create public Vulnerability Disclosure Policy with a clear disclosure process, vulnerability submission and verification process, and terms for disclosers.
- Use the Common Vulnerability Scoring System (CVSS) to evaluate potential vulnerability impacts and prioritize the response.
- Review IBR/DER scripts and applications to ensure permissions are set to prevent an unprivileged user from executing code as a privileged user.

CYBERSECURITY PROGRAM MANAGEMENT

- Establish a culture of cybersecurity across the IBR/DER vendor and enterprise network operations including non-technical employees.
- Mature a cybersecurity program strategy with priorities and a governance model.
- Maintain clear reporting lines to corporate leadership for addressing high-priority issues.
- Create and maintain the enterprise network architecture with clear isolation between any IT and OT systems.
- Establish response plans, especially for high-priority assets, detailing local law enforcement and federal agency coordination strategies.

RISK MANAGEMENT

- Establish methodology to prioritize cybersecurity improvements based on risk to IBR/DER operations.
- Maintain updated network architecture diagrams to identify critical assets, Internet connections, open ports and supported protocols.
- Establish a process for updating fielded IBR/DER, including additional on-site maintenance activities for critical patches.
- Regularly review and update risk management plans.