Digital Assurance Checklist for Homeowners and Installers

Managing Behind-the-Meter Energy Assets

CYBER HYGIENE CHECKLIST FOR INSTALLERS

As frontline professionals in deploying behind-the-meter generation and distributed energy management assets, installers play a vital role in ensuring these systems are not only functional but also secure. While manufacturers provide the hardware and software, installers are often the first—and sometimes only—line of defense when it comes to configuring devices securely and educating customers. Simple steps like changing default credentials, verifying secure network connections, and disabling unnecessary remote access can significantly reduce cyber risk. This checklist outlines key actions installers should take during setup and commissioning of distributed energy resources (DERs) to help protect both the system and the homeowner from potential cybersecurity threats. These recommendations are resource-agnostic, focused on general best practices for behind-the-meter systems, but specific considerations for different types of recommendations should be identified.

Pre-Installation

1. **Asset Inventory and Assign Asset Ownership**
   - ☐ Maintain a detailed inventory of all components and software versions (variable generation or storage systems, energy management devices, power delivery equipment, and gateways). Assign ownership for maintenance of each asset.
2. **Secure the Installer's Tools and Laptops**
   - ☐ Use antivirus, strong passwords, and encrypted storage on devices used for configuration.
   - ☐ Use a dedicated mobile device for commissioning. Avoid using personal phones or tablets for system setup to reduce cross-contamination risks.
3. **Align with State-Specific Requirements**
   - ☐ Some states may have requirements for communications or cybersecurity. Check the applicability of these requirements to the specific site and ensure that the site complies with required standards.
4. **Physical Access and Safety**
   - ☐ Treat your equipment like an appliance that needs to be secured. Don't let unauthorized persons (strangers, unvetted technicians) plug into or tamper with the equipment.

During Installation

5. **Segment DER Devices on a Separate Network**
   - ☐ Place DER systems on a separate virtual local area network (VLAN) or network segment apart from corporate information technology (IT) or home networks.[1] Use firewalls or gateway devices to create an *Electronic Security Perimeter* (in line with NERC CIP-005). Only allow required communications (e.g. power telemetry) and block all unnecessary inbound/outbound traffic.
   - ☐ Do not request passwords for a homeowner's primary Wi-Fi network.

6. **Secure Remote Access**
   - ☐ Avoid enabling remote access to DER equipment unless absolutely needed for monitoring or support. If remote access is required, do not use unsecured protocols or public IP access. Instead, use a virtual private network (VPN) or private network and enforce multi-factor authentication (MFA) for logins.[2]
   - ☐ Configure remote access for least privilege (access only what is necessary) and disable any unused remote access accounts

7. **Ensure Firmware is Up-to-Date at Installation**
   - ☐ Check for and apply the latest firmware updates before commissioning the system.
   - ☐ Verify digital signatures on firmware. Check that firmware or software updates come from trusted sources and are digitally signed.

8. **Rename Devices with Non-Identifiable Labels**
   - ☐ Avoid using customer names or addresses in device names or Service Set Identifiers (SSIDs).
   - ☐ Use a consistent naming convention across installations for easier support and auditing.

9. **Verify Secure Communication Protocols**
   - ☐ Ensure HTTPS is enabled for all web-based interfaces.
   - ☐ Use VPNs or encrypted tunnels for remote monitoring access.
   - ☐ Disable unencrypted protocols like HTTP, Telnet, or FTP.

10. **Ensure Physical Security of Devices**
    - ☐ Physically secure all DER equipment (e.g., lock external enclosures).
    - ☐ Install tamper-evident seals or surveillance for critical equipment if possible.

11. **Change All Default Credentials Before Handover**
    - ☐ Update default usernames and passwords on inverters, gateways, and monitoring platforms. Avoid reusing credentials (SSIDs and passwords) across multiple sites.

12. **Disable Unused Services and Ports**
    - ☐ Turn off remote access, Bluetooth, or open ports that aren't necessary for operation.
    - ☐ Disable manufacturer debug or developer modes if accessible.
    - ☐ Confirm that only essential services are running before leaving the site.

13. **Educate the Homeowner on Best Practices**

[1] https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology
[2] https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

- ☐ Briefly explain the importance of updates, password changes, and app security.
- ☐ Leave behind a simple, visual guide for homeowners on how to maintain cyber hygiene.
- ☐ Encourage homeowners to contact support if they notice unusual behavior.

Post-Installation

14. Log and Document System Configuration

- ☐ Record device models, firmware versions, IP addresses, and credentials (securely stored).
- ☐ Record device models, firmware versions, IP/MAC addresses, and network settings.
- ☐ Securely store credentials and configuration logs in an encrypted format.
- ☐ Maintain a backup of the configuration for troubleshooting or future upgrades.

15. Install Monitoring and Anomaly Detection

- ☐ Implement an intrusion detection system (IDS) to log abnormalities within networks.
- ☐ Ensure that alerts/alarms from DER monitoring platforms (e.g. sudden drop in output, unauthorized access attempts) are reported and reviewed.[3]

16. Log Out of All Installer Portals Before Leaving Site

- ☐ Ensure no admin sessions remain open on local devices or mobile apps.
- ☐ Clear browser caches and saved credentials on installer devices.

17. Disable any Setup Hotspots on DER Equipment

- If a private Wi-Fi, Bluetooth, or other personal network was used to configure and initialize the asset, disable and turn it off.

18. Firmware Updates & Patching

- ☐ Ensure the latest firmware/software updates are applied to DER devices before commissioning and schedule regular updates (e.g. quarterly or per vendor alerts).
- ☐ Enable automatic updates where available or plan manual updates during maintenance windows.

19. Report Vulnerabilities to Vendors

- ☐ If a security flaw is discovered, document it clearly with steps to reproduce.
- ☐ Submit the issue through the vendor's responsible disclosure process.
- ☐ Follow up to ensure the issue is acknowledged and addressed.

ADDITIONAL RESOURCES FOR INSTALLERS

- CISA Cybersecurity Training & Exercises
- NARUC Cybersecurity Baselines for Electric Distribution Systems and DER
- EPRI Security Architecture for the DER Integration Network
- NIST Cybersecurity for Smart Inverters Guidelines
- DOE SETO Cybersecurity Resources
- NASEO Cybersecurity Advisory Team for State Solar (CATSS)
- Security Recommendations for IBRs/DERs
- SEIA Cybersecurity Resources

[3] https://malcolm.fyi/

CYBER HYGIENE CHECKLIST FOR HOMEOWNERS

As residential behind-the-meter generation and distributed energy management assets become more common in homes, they also become potential targets for cyber threats. While manufacturers build in many safety features, homeowners play a critical role in keeping these systems secure. Just like locking your front door, taking a few simple steps—like updating passwords or securing your Wi-Fi—can help protect your energy system from unauthorized access or misuse. These actions don't require technical expertise, but they do require awareness and follow-through. By taking responsibility for basic cybersecurity practices, homeowners can ensure their systems remain safe, reliable, and resilient.

This guide uses a tiered approach to help homeowners improve their cybersecurity in a way that matches their comfort level and technical ability. You are not expected to understand every advanced feature or make every change. Instead, the focus is on giving you practical steps that protect your home without overwhelming you. There are four tiers included. Tiers 1& 2 include beginner items that are recommended for all users, while Tiers 3 & 4 are intended for advanced users who wish to maximize the defensive postures for their home networks.

Checklist Levels

Both Beginner and Advanced checklists have a set of minimum recommendations with an additional list of stretch goals. As suggested in the framing, performing the Tier 1 items is a minimum viable product that would drastically reduce risk for average homeowners, but for those that want more they can achieve the Tier 2 stretch goals. For tech savvy homeowners, Advanced items would help them mitigate even more cyber risk, once again following the core items with a set of Advanced Stretch goals if they want to push towards enterprise grade security for their residential home environment.

Tier 1: Beginner Essentials	For homeowners with little to no technical background who need straightforward, confidence-building steps. This tier focuses on the simplest actions that any homeowner can complete independently to establish a basic level of digital security.
Tier 2: Beginner Stretch Goals	For homeowners who are comfortable navigating device settings or apps and are willing to spend a bit more time learning. These steps go slightly beyond the essentials but remain appropriate for users without specialized knowledge.
Tier 3: Advanced Recommendations	For homeowners with moderate technical experience—those familiar with home networking basics or who routinely manage their own smart-home devices. This tier is intended for users ready to adopt more proactive, system-level practices that require deeper understanding
Tier 4: Advanced Stretch Goals	For highly engaged or tech-savvy homeowners who want the highest degree of control and visibility. These items typically require more time, troubleshooting skills, and confidence working with network or device configurations.

Tier 1 – Beginner Essentials

These are the must-do steps for any homeowner with behind-the-meter resources.

They are simple, high-impact actions that every homeowner can complete, regardless of the type of router they have. Completing Tier 1 dramatically reduces the risk of unauthorized access, protects your personal devices, and helps ensure that your residential distributed energy resources (DERs) operate safely and reliably. Completing Tier 1 removes low-effort attack paths, reducing the likelihood of compromise.

1. **Change the Wi-Fi Name (Service Set Identifiers - SSID)**
   What to do: Use a neutral name (e.g., GreenHall_WiFi, PineNet, etc.) that does not reveal your identity or router type. Do not use the default name (e.g., NETGEAR123 or SpectrumWiFi), nor use personal info (address, last name, etc.)
   Why: Default names often reveal the router brand/model, which helps attackers know what vulnerabilities to use. Personal names (e.g., SmithFamilyWifi) reveal who lives there.

2. **Create a Strong Wi-Fi Passphrase**
   What to do: Use a long phrase (16+ characters), not a single word. **NOTE:** Did you know adding just 4-6 characters increases the difficulty by thousands or millions of times. Examples include: 'sunset-lights-river-chair', 'jumping2horsesAcrossFields!' Avoid personal information like birthdays, pets, short words, company names, or reusing passwords from elsewhere.
   Why: Every extra character makes the password exponentially harder to guess. Long phrases are easy to remember but extremely hard to crack. Short or reused passwords are the most common cause of home network breaches.

3. **Change the Router's Admin Password**
   What to do: Change the login password for the router's control panel.
   Why: Default admin passwords (like "admin/admin") are publicly known. Someone who gets into your router controls everything, including all DER devices. Changing the Wi-Fi password alone does not protect the router's admin panel.

4. **Turn Off WPS (Wi-Fi Protected Setup)**
   What to do: Disable WPS buttons or PIN access. This feature lets people connect by pressing a button or using a PIN. It is known to be insecure on many routers.
   Why: WPS PIN attacks are easy and fast for attackers to exploit. Eliminating WPS closes a major shortcut into your network.

5. **Enable Automatic Updates**
   What to do: Turn on auto-updates for router and DER devices. Cyber risks evolve quickly, and patches matter.
   Why: Many attacks target outdated firmware. Automatic updates ensure security patches are applied without you needing to remember.

6. **Educate Your Household**
   What to do: Make sure everyone knows not to share system passwords. Teach basic cybersecurity habits like recognizing phishing emails. Keep a record of all connected devices, and login credentials (stored securely, such as with a password manager). Contact your installer or utility if you notice anything suspicious or need help with updates.
   Why: You are the first line of defense and attackers are always looking to socially engineer passwords and information out of you in order to get access to your environment.

Tier 2 – Beginner Stretch Goals

These are beginner-friendly items but may be new to some users.

These items are still beginner-friendly, but many require slightly more comfort navigating a router's settings menu if these options exist. They offer additional protection, but the essentials always come first. Homeowners are encouraged to try them when ready, but there is no pressure—your network is already significantly safer once Tier 2 is complete.

1. **Create a Guest or Internet of Things (IoT) Wi-Fi Network**
   What to do: Create a separate Wi-Fi for smart devices and distributed energy resource (DER) equipment.
   Why: This keeps your laptops/phones safe if a smart device gets hacked. It prevents movement by the attacker from simple IoT devices to important personal devices.

2. **Disable Remote Administration**
   What to do: Turn off anything labeled "Remote Access" or "Remote Management".
   Why: This prevents attackers on the internet from reaching your router's control panel. Most households never need to enable remote access at all.

3. **Ensure WiFi Protected Access (WPA) version 3 is Enabled.**
   What to do: Use WPA3 when possible, otherwise WPA2.
   Why: WPA3 is the newest and strongest encryption for Wi-Fi communications. Avoid WEP/WPA/"Open" networks--they are insecure and can be cracked in minutes.

4. **Hide the Service Set Identifiers – SSID (Do not broadcast the Wi-Fi Name)**
   What to do: Stop broadcasting your Wi-Fi Name (See #1 in Tier 1 – Essentials)
   Why: This makes your network less visible to casual scanning. This is not a full security measure but reduces opportunistic attacks. NOTE: You will need to type your Wi-Fi name manually on devices, when you click on 'Hidden Network' when connecting the device.

5. **Plan for Outages or Incidents**
   What to do: Ask your installer to show you how to safely disconnect or power down your residential DER in case of an emergency (for example, if there's a suspected cyber incident or the equipment behaves erratically). Having a manual shutdown procedure is important. Keep a contact list of who to call – your installer, the device manufacturer support, and your utility – if you suspect a cybersecurity issue or equipment malfunction. Timely communication can help contain any problems.
   Why: Controlling the loss of service but also the recovery of your service is important to ensure any impact is minimized. Keeping DER resources at your property online and active is our shared goal.

Tier 3 – Advanced Recommendations

These items are for users who are comfortable with networking setup and administration.

These steps are intended for homeowners who feel confident exploring deeper router settings or who have prior experience with networks, home labs, or smart home systems. They offer stronger defenses for homes with many connected devices, including distributed energy resources (DER). Completing Tier 3 is optional but recommended for anyone who wants a more resilient and controlled home network.

1. **Network Segmentation (Separate Networks)**
   What to do: Use multiple Service Set Identifiers (SSIDs) or virtual local area networks (VLANs) to separate device types. Expands Item #1 from Tier 2 – Beginner Stretch Goals, but includes home network, guest network, IoT network, etc.
   Why: A hacked internet-of-things (IoT) or DER device cannot reach personal devices, and vice versa when network segmentation is used. This reduces the impact from malware, misconfigurations, or compromised vendor cloud accounts.

2. **MAC Filtering (Optional but Helpful)**
   What to do: Configure Router to only allow specific devices on the Local area network. Pull up the MAC address of the device and add it to the MAC address list in the router. This allows only pre-approved devices to join.
   Why: Skilled attackers can spoof MACs, but MAC filtering still reduces casual intrusion.

3. **Device Isolation / Access Point (AP) Isolation**
   What to do: Turn on options that prevent devices from talking to each other.
   Why: IoT devices rarely need to talk to each other. This limits any infection to a single device instead of the whole VLAN/network.

4. **Domain Name Service (DNS) Filtering**
   What to do: Set DNS to Quad9 (9.9.9.9) / Cloudflare (1.1.1.3) / OpenDNS (208.67.222.123) / other secure filtering addresses. Secure DNS providers reduce phishing and malware exposure.
   Why: DNS filtering automatically blocks known malicious websites and command-and-control servers. It protects every device instantly by preventing resolution of known bad domains.

5. **Assign Static IPs to DER Devices**
   What to do: Reserve fixed IP addresses for DER devices.
   Why: This makes it easier to apply firewall rules and monitor device behavior.

6. **Advanced Firewall Rules**
   What to do: Disable UPnP, block inbound traffic, restrict DER devices to outbound-only, and block IoT-to-personal-device traffic.
   Why: This stops devices from opening ports without your knowledge. It prevents remote hackers from entering your network and helps ensure DER devices talk only to their legitimate cloud services.

7. **Multi-SSID by Band (2.4 vs. 5 GHz)**
   What to do: Put DER/IoT on 2.4 GHz. Keep personal devices on 5 GHz or Wi-Fi 6. Assign different bandwidth, priorities, or VLANs per SSID (often called profiles in a router configuration).
   Why: This improves stability for DER devices and keeps performance high for personal devices.

8. **Disable Legacy Network Services**

What to do: Turn off services in the router such as Telnet, SMBv1, FTP, or SNMP.
Why: These are common attack vectors used by attackers if present on your router.

Tier 4 – Advanced Stretch Goals

These steps are specialized and may not apply to all equipment.

These features are more specialized and may only be available on higher-end routers or custom firmware. They provide enterprise-level protection for those who want maximum security and visibility. These are not required for safe operation of distributed energy resource (DER) devices, but they are excellent for enthusiasts, power users, and installers who want to "harden" a home network.

1. **Enable Router Logging**
   What to do: Turn on logs for connection attempts, new devices, firewall alerts. Recommended actions to log: firewall events, admin login attempts, new device connections, blocks connections, and system events like firmware updates.
   Why: Early warning system for suspicious activity. Helps diagnose problems with DER devices.

2. **Export Logs to external Storage (Syslog)**
   What to do: Sends logs to another device like a universal serial bus (USB) or a network attached storage (NAS) device.
   Why: Prevents loss of records when router reboots. Enables long-term monitoring and incident analysis.

3. **Role-Based Access Control (RBAC)**
   What to do: Create multiple router accounts with limited permissions. Roles may include Admin (full control), Standard User (Wi-Fi Settings Only), Guest Manager (Guest Network Only), etc.
   Why: Prevents accidental changes by family members or contractors. Reduces the impact if one account is compromised.

4. **"Glass Break" Emergency Admin Account**
   What to do: Create a backup admin account with sealed passwords stored safely (offline in a closet or safe).
   Why: Protects you if the main admin account is locked or corrupted. Ensures you never lose access to your network.

5. **Remote Authentication Dial-In User Service (RADIUS) Authentication (Enterprise Wi-Fi)**
   What to do: Set up Wi-Fi Protected Access (WPA) WPA2/WPA3-Enterprise with user-based login. If you have a local server, consider running FreeRADIUS or a similar service.
   Why: Allows per-user Wi-Fi credentials. Provides stronger authentication than a shared password. **NOTE:** Most internet-of-things (IoT) or DER devices do not support enterprise Wi-Fi.

6. **Deep Packet Inspection (DPI), Intrusion Detection System (IDS), and Intrusion Protection System (IPS)**
   What to do: Turn on threat detection/prevention if supported. Useful items include unexpected outbound connections, excessive repeated Domain Name Service (DNS) lookups, and attempts to contact known malicious IPs.
   Why: Identifies usual behavior from compromised devices. Blocks known attack signatures automatically.

7. **Advanced Routing & Policy Rules (extending Item #5 from Tier 3 – Advanced)**

What to do: Allow DER devices only to vendor cloud addresses. Restrict IoT virtual local area networks (VLANs) from talking to local area network (LAN) devices. Apply time-based rules for certain devices. Recommend rules include adding egress filtering so IoT devices cannot call unknown servers and restricting DER devices to known vendor cloud IPs, use policy routing to isolate networks.
Why: Gives granular control over network behavior. Limits attack surfaces by restricting unnecessary communication paths.

8. **Deploy Custom Router Firmware**
   What to do: Use a router that allows custom firmware that can disable or turn off features. Firmware like OpenWRT, pfSense, OPNsense, UniFi, MikroTik RouterOS, etc.
   Why: Enables true enterprise-grade controls and monitoring. Provides updates long after consumer routers stop receiving support.

ADDITIONAL RESOURCES FOR HOMEOWNERS

- 7 Tips to Keep Your Smart Home Safer and More Private (NIST)
- CISA Recommendations for Individuals and Families
- CISA Home Network Security
- Best Practices for Keeping Your Home Network Secure (NSA)
- NARUC Cybersecurity Baselines for Electric Distribution Systems and DER
- NASEO Cybersecurity Advisory Team for State Solar (CATSS)
- DOE SETO Cybersecurity Resources
- Home Router Cybersecurity Tips (InfoSec)