Home Energy Rebates (IRA Sections 50121 and 50122): Required Elements of a Privacy and Security Risk Assessment for State Systems

April 2024

Data collection and data sharing must be secure to protect consumer data in the Home Energy Rebate programs. As a means of meeting the requirements[1] of the U.S. Department of Energy (DOE) Privacy and Security Risk Assessment for Home Energy Rebate programs, a state[2] can document its compliance with its own state-level data security and privacy requirements and show how these protections adequately address the DOE-required elements included below. Compliance with the Federal Information Security Modernization Act (Public Law 113-283, December 18, 2014) is not required for state systems implementing Home Energy Rebate programs.

To ensure states are addressing potential data security and privacy risks, states must conduct a documented Privacy and Security Risk Assessment that includes the following three (3) elements:

1. A rationale for categorizing the system,
2. A method for determining the risk impacts, and
3. Risks associated with data sharing.

To illustrate, a Privacy and Security Risk Assessment meeting these elements typically includes descriptions of the following:

- Types of data to be protected and the sensitivity of each data type
- Sources of risk of data leak or theft
- Risks regarding data corruption, data loss, and loss of confidentiality
- Factors (e.g., likelihood, impact to operation, liability, public confidence, etc.) that are considered and weighed to determine the risk impacts
- Person(s)/entity(ies) that will monitor for these risks, and steps that will be taken to guard against these risks

[1] Home Energy Rebate Programs Requirements and Application Instructions | Department of Energy.

[2] For the purposes of this document, "states" means, collectively or individually, the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, American Samoa, Guam, and the Commonwealth of the Northern Mariana Islands.

It should be noted that a state's Assessment may use terms that vary from the ones used in this document as long as key activities – such as, at a minimum, risk analysis, impact analysis, protective measures/controls, and implementation process – are covered.

Security and privacy protection measures/controls must be reviewed by an independent third party at least once every three years, and states must have documented processes in place to monitor and address privacy and security issues in a timely fashion.

States must ensure that data collected through its Home Energy Rebate programs are not sold.

A copy of the Privacy and Security Risk Assessment of state systems must be provided to DOE at least 60 days prior to program launch, which is generally understood as the first date that the state begins to accept rebate claims.

States that do not have existing data security requirements may consult the following resources in developing them:

- Information from the National Institute of Standards and Technology (NIST) on protecting controlled unclassified information in non-Federal systems and organizations: NIST SP 800-171
- Information from NIST on minimum security requirements for Federal information and information systems: FIPS 200
- Standard for information security management systems: ISO/IEC 27001
- Standard for information security controls: ISO/IEC 27002
- Guidance on managing information security risks: ISO/IEC 27005
- NIST's Risk Management Framework that provides a step-by-step method for analyzing and managing risk: https://csrc.nist.gov/projects/risk-management/fisma-background