[Users must accept these protections to create a user account.]

**EXAMPLE ONLY—Energy Connector Digital Protections**

We are working in a cloud environment as an enterprise [National Renewable Energy Laboratory] NREL solution for enabling scalability, reliability, and efficiency of mission-driven data science, computing, application development, data management/sharing, and analysis innovation.

All NREL applications follow industry best practices as defined under NIST 800-53, ISO 27001, and PCI SOC type 1 and 2; which are approved by the U.S. Department of Energy (DOE) for housing secure data. DOE has authorized the Alliance [Alliance for Sustainable Energy—managing and operating contractor of NREL] to host secure data and control access using multi-factor authentication (MFA). The site includes encryption for data, where all data must be encrypted at rest as well as in transit. All NREL websites and applications use the same high standards for security and encryption and guard against known Structures Query Language (SQL) exploits automatically.

Based on the nature of the application [the Energy Connector, “Connector”] and the data it will be sorting, we are planning for this application to be deployed in a secure environment. A verified log-in is required to get onto the Tool. Any Personally Identifiable Information (PII) stored on the Tool will only be seen by the intended viewers. All vulnerabilities are remediated before a new system or application goes into production. Projects are required to remediate all Known Exploited Vulnerabilities (KEV) or critical and high vulnerabilities prior to production release. Additionally, regular audits are performed regularly for an additional layer of security against KEVs.

For questions and concerns in regards to digital protections, please contact us [use Contact Us feature on the Connector].