Data Privacy Policy Priorities (Appendix)

The following priorities are rooted in NEMA's Data Privacy Policy Principles and are meant to serve as the charge for the organization's advocacy in this area. These principles should be reviewed annually by the Cybersecurity Council and amended as necessary.

Convergence

- NEMA supports the adoption of federal legislation that establishes a comprehensive, nationwide data privacy precedent.
- Entities and organizations that adhere to existing federal data privacy and security requirements should be exempt from any new state law or rulemaking that would make compliance duplicative and burdensome.
- Federal data privacy legislation should build upon existing privacy policies, including those established by the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Federal Information Security Modernization Act.
- Data privacy legislation generally should seek to harmonize definitions with existing statutes to prevent ambiguity and strengthen protection across jurisdictions.
- Data privacy legislation generally should be comprehensive in its scope and clear in intention to prevent loopholes in compliance that could be exploited and, thereby, weaken security.

Due Process

- Enforcement and oversight of federal privacy rules and regulations should be assigned to a regulatory entity with appropriate privacy experience, such as the Federal Trade Commission (electric sector) and the HHS-Office for Civil Rights (healthcare sector), which should establish transparent due process procedures.
- Data privacy audits by enforcement authorities should be attested by using objective evidence, including the use of established, appropriate, and certifiable cybersecurity standards.

Innovation

- A company that collects and uses the personal data of its employees within the context of their role should be exempted from mandates granting rights to erasure or unauthorized editing of that data by the employee or outside authority.
- Since expectations on the use of personal data vary between customers—and could also vary between an individual customer's own preferences among differing products and services—a product or service's data design model and collection defaults should be established by the manufacturer.

Compliance

- Frivolous and subjective litigation could stifle innovation and create a disincentive for business collaboration, a necessary component for cybersecurity and data privacy. Therefore, data privacy statutes should not grant private rights of action to consumers. Rather, enforcement should be assigned to a senior state official or regulatory body, including states Attorneys General and/or the Federal Trade Commission.

- State should provide incentives for companies to voluntarily invest in good cybersecurity and data privacy practices through the creation of "safe harbors."

- Individual rights to personal data should be reasonable, objective, and not create undue burden on a company's operations. There should not be an expectation of a right to non-personal data collected by a company, including operational and anonymized data.

Contact: *Peter Ferrell: Manager, Connectivity and Data Policy: 703-841-3280 | peter.ferrell@nema.org*

Updated January 2022.