AABE Cybersecurity Principles

The American Association of Blacks in Energy (AABE) recognizes the need for increased participation in the discussion on energy cybersecurity policy by historically underserved communities. To that end, AABE supports the following energy cybersecurity principles.[1]

- AABE believes that cybersecurity policy for the energy industry should address threats and vulnerabilities to the electric, oil, and natural gas sectors.
- AABE supports cybersecurity strategies that focus on assets critical to the reliable operation of the energy supply chain. Such operations include production, transmission, distribution and delivery of energy to customers.
- AABE believes that industry, government and underserved communities should partner to develop a “culture of security” with strategies and training focused on prevention, detection, response and recovery efforts.
- AABE believes that cybersecurity risk cannot be completely eliminated, but instead must be managed through informed decision making. Such risk is a function of threat (potential source of harm), vulnerability (potential weakness) and potential consequences. Planned mitigation controls should include both emergency actions and measured responses.
- AABE believes that awareness should be raised in underserved communities about cyber-type disruptions that may be caused by unintentional incidents and natural forces (e.g., Hurricane Katrina), intentional cyber-attacks (e.g., Stuxnet worm) and attacks against the cyber-physical interface resulting in long-lasting impacts.
- AABE believes the roles and responsibilities of industry (asset owners who operate the infrastructure), government (law enforcement, intelligence gathering) and other stakeholders involved in securing electric, oil, and natural gas infrastructure should be clear to avoid duplicative or conflicting actions in times of crisis.
- AABE believes that cybersecurity protections, such as security certification programs, should be incorporated into the facility operations and human resource architecture.
- AABE supports partnerships with industry and government to inform and engage underserved communities in cybersecurity mitigation planning.
- AABE believes that consideration and treatment of diverse and underserved communities by public and private entities in response to cyber threats and vulnerabilities should be equitable.

[1] Approved by the AABE Board of Directors (November 2012)

- AABE supports elements of the North American Electric Reliability Corporation (NERC) process to develop cybersecurity standards, where such harmonizes with AABE goals and objectives.