Cybersecurity Considerations for State Procurement of Solar Assets

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

NASEO
National Association of State Energy Officials

Cybersecurity Considerations for State Procurement of Solar Assets

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

CATSS Toolkit is designed to provide states with basic education on cybersecurity issues for solar and enable their efforts to support cybersecurity enhancements efforts for solar. Cybersecurity challenges for solar should not be viewed as unique. All electricity generation technologies are, to varying degrees of potential severity and vulnerability, susceptible to cyberattacks and disruption. As interconnected electricity generation technologies, solar systems—and DERs generally—have a unique advantage to ensure that cybersecurity is incorporated by-design and prior to deployment, rather than applied ex post facto. The recommendations provided within the CATSS Toolkit/this tool were developed to meet the expressed needs of State Energy Offices and Public Utility Commissions during the project, and their respective purviews, priorities, and directives to support cyber-secure solar deployment in their states. While many industry and federal partners were included in the CATSS Advisory Group, it must be noted that neither the states' nor other stakeholders' perspectives collected are exhaustive. The Toolkit represents a snapshot of a quickly evolving and complex area, and should not be treated as a definitive guide, but rather a basis for continued discussion and adaptation of public-private partnerships for solar cybersecurity.

This material is based upon work supported by the U.S. Department of Energy (DOE) under award number DE-EE0009004. This report was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

Introduction

State Energy Offices and Public Utility Commissions may have a significant, often unrecognized role to set the cybersecurity parameters for state procurement of solar assets through the development of formal guidelines, or standard language for grants and Requests for Proposals (RFPs). As supply chains are becoming the source of cyberattacks and intrusion more frequently, it is important to consider not only the physical composition of solar assets, but also the country in which they were manufactured and the existence or supply chain standards. Reducing disparate procurement strategies and standardizing cybersecurity practices can help a state more easily implement risk-reduction strategies and support the deployment of technologies and their sources that are certifiably more cyber-secure. Further, aligning minimum, standard state policies and executive orders with federal policies and executive orders may help streamline industry and manufacturer efforts to develop solar PV system components that are more easily verifiable as cyber-secure, which will lead to faster, and ultimately more reliable deployment of solar assets. States should consider engaging with industry experts to help develop this language to support a "common security baseline."[1]

States might also consider actions that enable them to advise consumers on what might be considered "acceptable" standards or designs, without going into the technical complexities. For example, recommendations for software bills of materials (SBOM)[2] might also be developed to avoid the procurement or acquisition of certain devices which may possess cybersecurity risks. A SBOM is a formal record containing the details and supply chain relationships of various components used in building software. For state officials responsible for procurement, or determining parameters for state-funded software, SBOMs are used to inform pre-purchase assurance, negotiate discounts, or plan implementation strategies. The cybersecurity benefits of a SBOM include:

- Identifying and avoiding known vulnerabilities
- Identifying both security and license compliance requirements
- Enabling quantification of the risks inherent in a software package
- Managing mitigations for vulnerabilities

As state designees for distribution of significant funding provided for clean energy technology and generation asset deployment through the U.S. State Energy Program (SEP), Infrastructure Investment and Jobs Act (IIJA), the Inflation Reduction Act (IRA), or other funding, State Energy Offices will need to ensure projects are in compliance with state objectives and federal requirements. Several programs established through the IIJA require a cybersecurity plan for recipients of these funds, which may include procurement standards to help maintain cybersecurity of funded projects.

This tool provides an overview of existing procurement programs and example language that prioritizes cybersecurity. While not always explicitly specific to solar or distributed energy resources (DERs), the following language and references can readily be applied to state solar cybersecurity practices. As this approach may be novel for many states, the information herein should be considered as a model only. The following programs and example language are by no means exhaustive and should be evaluated in accordance with state processes and policies. This tool also identifies Sample Language for Procurement Agreements, Contracts, and Grants (pg. 8), which can serve as lower entry points for state officials interested in pursuing this subject matter more immediately.

Federal Landscape

At the Federal Government level, multiple Executive Orders have been issued in recent years by several Presidents to address cyber threats and vulnerabilities. Executive Order 14028: Improving the Nation's Cybersecurity, outlines federal intent to remove barriers to cyber threat information-sharing, modernize federal government cybersecurity, enhance software supply chain security, and improve detection of cybersecurity vulnerabilities and incidents on federal networks, among other actions.[3] Significantly, the Executive Order included updates for contracting language of the Federal Acquisition Regulation (FAR), which are required for all contracts with federal agencies. This requires all contractors to the federal government to meet updated standards in software design and cybersecurity. The contract condition updates signal an effort by the federal government to improve transparency and minimize cyber-attacks targeting contractors' information technology (IT) and operational technology (OT) systems closely linked to the federal government.

In response to Executive Order 14017: America's Supply Chains, the U.S. Department of Energy (DOE) conducted a supply chain deep dive assessment on Cybersecurity and Digital Components in the Energy Sector, including solar photovoltaic (PV) systems.[4] The report recommended that "...proactive security investments [must] be made to ensure the integrity of the cyber supply chain for firmware on connected devices and the software systems used to connect and manage them. Emerging technologies that support the energy sector should be developed with approaches to illuminate the risk of sub-tier suppliers inlevel"[5] For solar photovoltaics specifically, the report recommended that domestic manufacturing be incentivized through legislative and executive action, as domestically sourced components are at a significantly lower levels of cyber risk and vulnerability. Domestic favorability in state procurement proceedings, with specific considerations for cybersecurity, may help incentivize manufacturers and vendors to design and deploy more cyber-secure assets.

The Federal Energy Management Program (FEMP) energy and cybersecurity integration effort, managed by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) provides information and tools to help agencies enhance the cybersecurity of federal facilities and facilitate the implementation of Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[6] These tools, some of which are explored in greater detail below, can also be utilized by state entities as models and guidance for their own programs. [7]

Procurement Guidance

Thirty-seven states and the District of Columbia have renewable energy requirements or goals, meaning that most of the U.S. population is impacted by these policies. As these jurisdictions take a more active role in managing their renewable energy resources , they have leveraged competitive procurements to do so when purchasing renewable resources. NASEO maintains a general overview of Solar Procurement and Compensation, and provides basic resources on competitive solicitations, power purchase agreements (PPA), and model solar leases. Each of these strategies may serve as appropriate entry points for cybersecurity considerations, so long as the state first defines cybersecurity as an accompanying objective to its' clean energy goals. The rest of this section contains resources pertaining to cybersecurity considerations in procurement guidance.

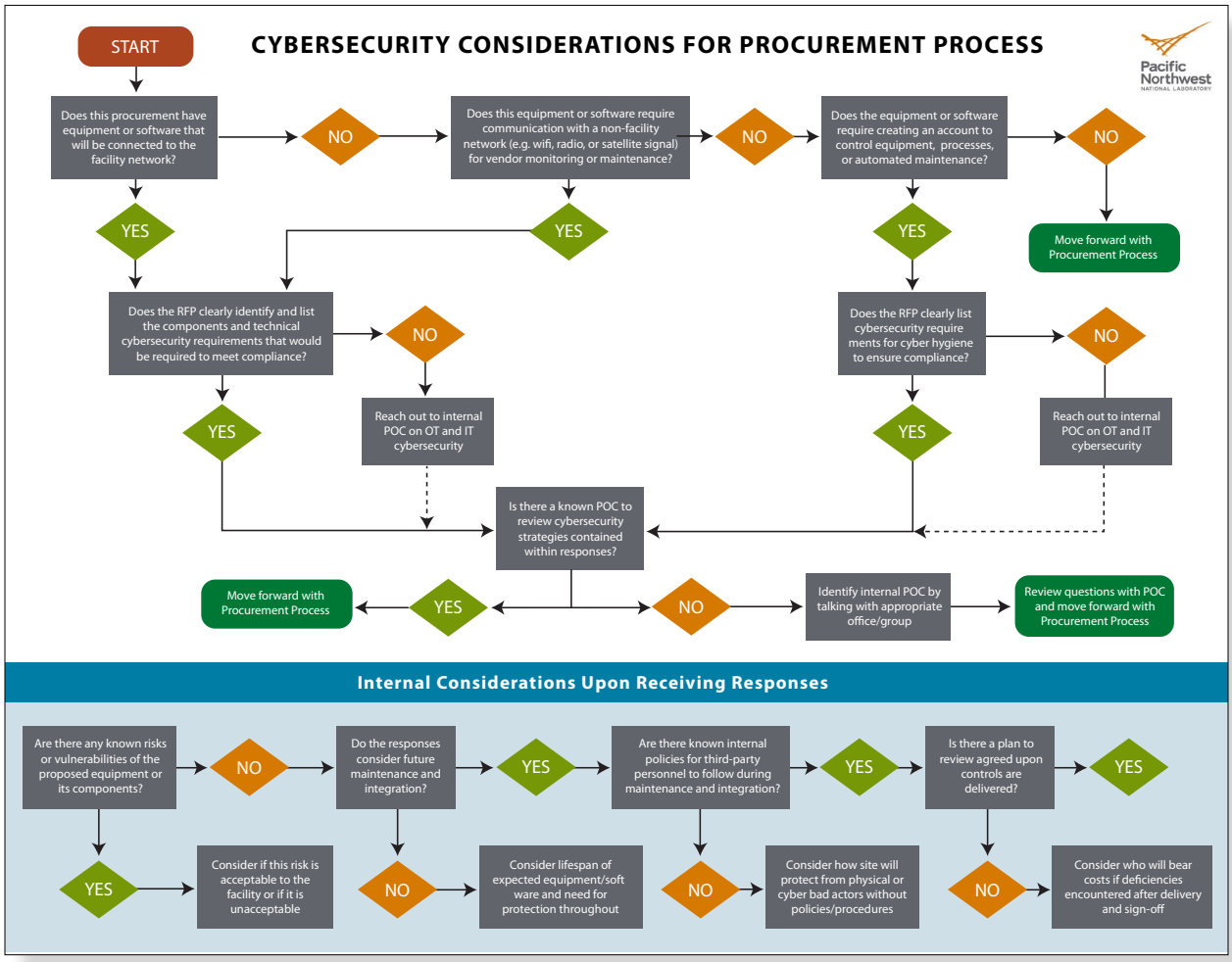
The Pacific Northwest National Laboratory (PNNL) produced a Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities, which notes that a procurement, implementation, and integration plan for energy assets being connected to federal facilities should include the following elements, which may also be considered for state processes:[8]

- At a minimum, the cybersecurity implementation plan must describe how cybersecurity is established between networks, systems, devices, application, or physical components within the proposed solution, and at the necessary external interfaces at the solution boundaries
- A summary of the cyber security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact)
- A summary of the cyber security criteria utilized for vendor and device selection
- A summary of the relevant cyber security standards and/or best practices that will be followed
- A summary of how the project will support emerging smart grid cyber security standards
- Plans should also address the adequacy of their approach for:
    - Ensuring confidentiality, integrity, availability
    - Secure logging, monitoring, alarming, and notification

Cybersecurity Procurement Decision Tree

The Cybersecurity Considerations for Procurement Process decision tree was developed by the U.S. DOE's FEMP to encourage the recognition of cybersecurity during the procurement process for agencies to proactively address cyber vulnerabilities.[9] The decision tree guides all levels of staff through a series of questions to determine whether to confer with cybersecurity professional during the acquisition of equipment, systems, or services. The questions posed in the procurement process decision tree work to determine, for example, if the new device has network connectivity capabilities or requires an account to be created to control equipment, all of which are applicable cybersecurity considerations for solar PV procurement. This tool can be utilized by state entities as guidance for their own programs and solar PV procurement.

The decision tree below outlines questions that States might consider when determining when cybersecurity experts should be consulted in the procurement of equipment.[10]



Cybersecurity Considerations for Performance Contracts

States pursuing solar projects funded through performance contracting vehicles, such as energy savings performance contracts (ESPCs) and utility energy service contracts (UESCs), should be sure that projects and interconnected components do not introduce any new cybersecurity vulnerabilities.[11] This framework offers considerations for integrating cybersecurity planning into performance contracts during each phase of the ESPC or UESC process, as follows:

- Acquisition Planning
- Contractor Selection
- Project Development
- Project Implementation
- Post-Acceptance Performance

States interested in increasing their cybersecurity standards for solar projects funded with these mechanisms may reference this framework, or more formally replicate and expand upon these considerations in state-level projects.

Electricity Industry Cybersecurity Guidance
The Electric Power Research Institute (EPRI) has produced a public, higher-level guidance on cyber security in the supply chain that provides a methodology for integrating cyber security into procurement processes, titled Understanding Vendor Cyber Security Certifications: Generation Cyber Security. It provides readers with a basic understanding of supply chain cybersecurity certifications, and outlines the values and limits of these certifications.

IoT Security Acquisition Guidance
The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (US DHS CISA) maintains an IoT Security Acquisition Guidance, which addresses vulnerabilities and acquisition lifecycles of HVAC systems, EVs, and portable computing devices.[12] This guidance includes recommended security actions stakeholders should consider through each step for IoT procurement but is applicable for other two-way communication technologies and DERs, including solar PV. From a procurement perspective, this guidance might help consumers and purchasers identify common risks associated with solar PV system components and make more cyber-secure choices during solar PV acquisition.

U.S. Environmental Protection Agency Cybersecurity Grant Conditions
The U.S. Environmental Protection Agency (EPA) maintains a set of Cybersecurity Grant Conditions for assistance agreements that recipients and subrecipients including intertribal consortia must adhere to.[13] The conditions ensure grant recipients are using secure information systems, the Environmental Information Exchange Network or EPA's Central Data Exchange, for data storage and exchange and comply with State and Tribal law cybersecurity requirements. There are similar cybersecurity grant conditions in place for states and tribes that have assistance agreements with the EPA.

The Cybersecurity Maturity Model Certification

U.S. Department of Defense (DoD) has established a cybersecurity framework that all contractors must meet to work with DoD. The Cybersecurity Maturity Model Certification (CMMC) is comprised of three increasingly rigorous maturity levels that incorporate Federal Acquisition Regulation (FAR and trusted industry standard, National Institute of Standards and Technology (NIST) 800-171. Obligating a similar security certification threshold for contractors installing solar photovoltaic (PV) on public facilities, including schools and government buildings could be a consideration by States to limit common vulnerabilities.[14]
Sample Language for Procurement Agreements, Contracts, and Grants

State Procurement Officers responsible for procurement of solar assets must comply with state cybersecurity policies or guidance. Such guidance is intended to ensure that public funds used to purchase assets including hardware and software and supporting systems are cyber-secure, and that the state has done it due diligence as the steward of public funds. The National Association of State Procurement Officers (NASPO) has several resources highlighting cybersecurity considerations for acquisition of state assets. These resources may be helpful for State Energy Offices and Public Utility Commissions to review prior to the solicitation and procurement of solar assets. In particular, the NASPO report on Integrating Cybersecurity in to the Acquisition Process outlines processes may be used by State Energy Officials to ensure an integrated and thoughtful approach to procurement which involves all relevant parties, such as State Procurement Officials, Information and Information Security Officials, and legal departments, among others; and considers education, risk management, budgeting, and vendor/third-party compliance processes. NASPO also maintains a library of State Policy and Procedure Templates and Resources and an Authorized Products List to assist states with streamlining their own procurement processes for assets with cybersecurity considerations, which can include solar and related assets.

State Energy Offices and Public Utility Commissions working with State Procurement Officers should consider reviewing pre-developed procurement language and templates to expedite the procurement process and include pre-verified language to ensure that solicitations meet state and the cybersecurity requirements. After reviewing the guidance included above in this document, states should review some of the following resources to find more specific examples and templates that might be included in state procurement language.

Potential Entry points for Cybersecurity Language

While none of the following resources include cybersecurity provisions or language, the mechanisms listed may be suitable for inclusion of cybersecurity language at a state's discretion. For example, if a state defines its cybersecurity goals as being complimentary to and inseparable from its clean energy goals, it can work with relevant parties internal to the state (e.g., State Procurement Officer, Chief Information Officer) to determine criteria and language that could be included in competitive solicitations for physical solar PV systems, and possibly even power-purchase agreements.

- The Solar Foundation and the MA Clean Energy Center have both produced **guidelines on competitive solicitations** for renewable resources, to ensure a fair, competitive, and efficient process.
- **Power Purchase Agreements (PPAs)** are a widespread mechanism for states, municipalities, and private firms to contract renewable energy production for a set time period. To support competitive and fair agreements, NREL released a Checklist for State and Local Governments, and the Interstate Renewable Energy Council released a Toolkit for Local Governments.

Model Resources

The U.S. Department of Homeland Security has produced a resource dedicated to providing cybersecurity procurement language for control systems, including some of the components within the PV solar schema (See: Engineering and Systems Overview). The DHS guidance provides specific procurement language for various system components designed to increase the minimum cybersecurity criteria that a supplier or vendor must meet for the asset to be purchased. This list is extremely thorough, but states should note the more applicable systems and components for which the resource provides procurement language, including but not limited to:

- System Hardening
- Perimeter Protection
- End Devices
- Remote Access
- Physical Security
- Network Settings
- Wireless Technology

Cybersecurity Procurement Language for Energy Delivery Systems provides baseline cybersecurity procurement language that is the consensus opinion of a variety of federal, industry, academic stakeholders.[15] It provides general cybersecurity considerations that apply to many types of products being procured as part of an energy delivery system. The language may be tailored by states based on the specific product being procured and the environment in which it will be integrated or applied. It provides baseline procurement language for the following functions for energy delivery assets:

- Software and Services
- Access Control
- Account Management
- Session Management
- Authentication/Password Policy and Management
- Logging and Auditing
- Communication Restrictions
- Malware Detection and Protection
- Heartbeat Signals
- Reliability and Adherence to Standards

Further, the aforementioned Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities produced by PNNL includes "Key Procurement Recommendations," including conditions that might be amended or supplemented by states prior to insertion in a state procurement contract based on state cybersecurity risk assessments, and agency guidelines.[16] The recommendations include direct excerpts pertaining to security features, instructions for cyber-secure operation and maintenance, authentication and access criteria, equipment communication protocols, and interconnection specifications, among others.

The Guide also provides information on Procurement Lifecycle Cybersecurity and Considerations for Federal Facilities, which may be tailored to the specific policies and regulations pertaining to energy asset management and procurement performed by states.

Enforcement

The Department of Justice (DOJ) created a new Civil Cyber-Fraud Initiative to use the power of the False Claims Act (FCA) to initiate suits against federal contractors that fall short of their regulatory and contractual cybersecurity obligations.[17] The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. Some of key benefits of the initiative include, among others:

- Building broad resilience against cybersecurity intrusions across the government, the public sector and key industry partners.
- Holding contractors and grantees to their commitments to protect government information and infrastructure.
- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly used information technology products and services.
- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.

Conclusion and Next Steps

State Energy Offices and Public Utility Commissions have an opportunity to serve as primary educators and leaders for prioritizing cybersecurity in state procurement and solicitation of solar assets. Because threats to solar assets and DERs will continue to expand, proactive mitigation measures—including establishing cybersecurity parameters for procurement and consulting State Procurement Officers and cybersecurity experts—are crucial steps for states to address current and future cyber vulnerabilities. While States have limited purview over the solar cybersecurity risks that they can directly mitigate, it is important to establish proactive state protocols and public-private partnerships to signal to industry partners and vendors that cybersecurity is a top priority or the state. By referencing existing federal procurement programs and standard cybersecurity language for grants and RFPs, states can enhance the design of their own procurement strategies and standard cybersecurity practices. Such policies and posture may help promote inherent cybersecurity-by-design in manufacturers and vendors whose customer base includes states. To that end, States should consider incorporating cybersecurity provisions into:

- Model state clean energy objectives and goals
- Procurement processes
- Performance contracts
- Competitive RFPs for solar assets and DERs
- Grants to local governments and/or the private sector to implement solar projects
- Power Purchase Agreements

There are abundant opportunities to enhance cybersecurity through state procurement functions, but additional deliberate efforts are needed to clarify discrete procedures and increase state ability to incorporate cybersecurity into their procurement processes.

References

1 Wray et al., "Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure". Solar Energy Industries Association. (June 7, 2021). https://www.seia.org/sites/default/files/2021-10/SEIA%20Comments%20RFI%20on%20Ensuring%20Security%20US%20Critical%20Electric%20Infrastructure%202021.06.07_%20%28003%29.pdf

2 A "software bill of materials" (SBOM) has emerged as a key building block in software security and software supply chain risk management. A SBOM is a nested inventory, a list of ingredients that make up software components. An SBOM-related concept is the Vulnerability Exploitability eXchange (VEX). A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities. https://www.cisa.gov/sbom

3 Executive Order 14028, 86 Federal Register 26633 (May 12, 2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

4 Executive Order 14017, 86 Federal Register 11849 (February 24, 2021), https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

5 U.S. Department of Energy (February 24, 2022). *Cybersecurity and Digital* Components. Supply Chain Deep Dive Assessment U.S. Department of Energy Response to Executive Order 14017, "Americas Supply Chains". https://www.energy.gov/sites/default/files/2022-02/Cybersecurity%20Supply%20Chain%20Report%20-%20Final.pdf

6 Executive Order 13800, 82 Federal Register 22391 (May 11, 2017), https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

7 U.S. Department of Energy. *Federal Energy Management Program*. https://www.energy.gov/eere/femp/federal-energy-management-program

8 Mylrea, Michael, JA Rotondo, Sri Nikhil Gupta Gourisetti (May 2019). *Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities*. Pacific Northwest National Laboratory. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-28661.pdf

9 U.S. Department of Energy. *Cybersecurity Considerations for Procurement*. Federal Energy Management Program. https://www.energy.gov/eere/femp/cybersecurity-considerations-procurement

10 U.S. Department of Energy Pacific Northwest National Laboratory. *Cybersecurity Considerations for Procurement Process*. Federal Energy Management Program. https://www.energy.gov/sites/default/files/2020/07/f76/cyber-procurement-decision-tree.pdf

11 U.S. Department of Energy. *Energy Saving Performance Contracts for Federal Agencies*. Federal Energy Management Program. https://www.energy.gov/eere/femp/energy-savings-performance-contracts-federal-agencies

12 Cybersecurity and Infrastructure Security Agency. *Internet of Things Security Acquisition Guidance*. Information Technology Sector. https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_1.pdf

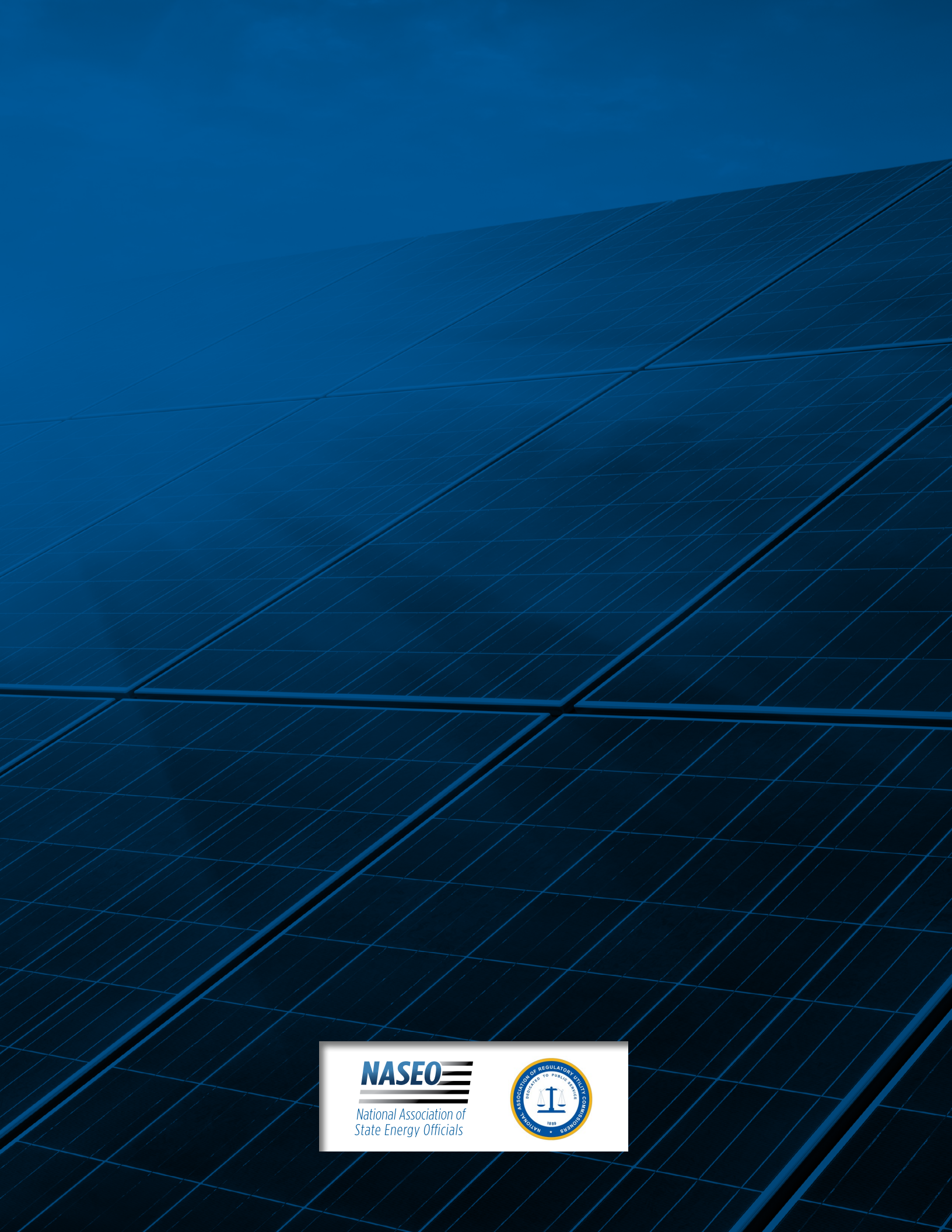
13 Environmental Protection Agency (November 12, 2020). *Cybersecurity Grant Condition for Other Recipients, Including Intertribal Consortia*. https://www.epa.gov/sites/default/files/2015-07/documents/cyber_security_grant_condition_for_other_recipients.pdf

14 https://dodcio.defense.gov/CMMC/about/

15 Energy Sector Control Systems Working Group (April 2014). *Cybersecurity Procurement Language for Energy Delivery Systems*. https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

16 Mylrea, Michael, JA Rotondo, Sri Nikhil Gupta Gourisetti (May 2019). *Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities*. Pacific Northwest National Laboratory. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-28661.pdf

17 U.S. Department of Justice (October 6, 2021). *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.


NASEO
National Association of
State Energy Officials
NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
DEDICATED TO PUBLIC SERVICE
1889