Title

# 0009

11/08/2023

by **Mike Regan** in **Kansas BEAD Volume 2 Public comment**

id. 44646029

1310 N Courthouse Rd.
Arlington, Virginia
22201
United States
candrews@tiaonline.org

## Original Submission

11/08/2023

| | |
|---|---|
| Please provide your first and last name | Mike<br>Regan |
| Please provide an email that we can contact you through | mregan@tiaonline.org |
| Please provide your address (not required) | |
| Are you filing a comment on behalf of an organization? | Yes |
| Which organization are filing on behalf of? | Telecommunications Industry Association |
| Please indicate which sections of volume 2 you are responding to: | Requirement 19: Certification of Compliance |
| Please provide your response to Requirement 19: Certification of Compliance | The Telecommunications Industry Association ("TIA") appreciates the opportunity to submit these comments regarding volume 2 of Kansas' Initial Proposal, as required under the National Telecommunications and Information Administration's ("NTIA") Broadband Equity Access and Deployment ("BEAD") program. TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used by the owners and operators of communications networks across all technology platforms. TIA is both a standards development organization ("SDO") and an advocate for the ICT industry. As such, TIA and our members are working towards the shared goal of connecting every American with high-speed, resilient, secure, and reliable broadband networks. To that end, TIA has developed the first-ever ICT industry |

standard for supply chain risk management and cyber security – SCS 9001TM. Utilizing the SCS 9001 standard can:

Empower the state/EE with a comprehensive and systematic approach to evaluate the responses received from potential sub-grantees.

Provide clear guidance to each prospective sub-grantee on the expected elements when outlining their C/SCRM plans.

Enable the state/EE to showcase their compliance with the requirements outlined in the NOFO to the NTIA.

Access to broadband services has never been more central to American life, and the investments under the BEAD program offers a historic opportunity to connect Americans in unserved and underserved communities. Companies providing broadband service using BEAD funding must deploy networks that provide consumers with the high speeds needed to thrive in our society, with resiliency and security built into them. It is no secret that we are in an era of increasing cyber attacks on the ICT industry, both from sophisticated non-state and government adversaries. This rising threat comes with growing costs for industry and governments – A recent industry report found that a single data breach can cost a company just shy of $10 million on average in 2022. Additionally, innovation across all sectors increasingly rely on open-source platforms to enable rapid prototyping and deployment, interoperability, and cost savings. Open-source code is also often co-created by multiple developers with a range of expertise and without security oversight or standardization. In 2022, more than 80% of analyzed open-source code contained at least one vulnerability, with more than 50% having high-risk vulnerabilities.

NTIA understood these concerns when drafting their NoFO for the BEAD program last year and, for the first time, required subgrantees to adopt plans focused on Cybersecurity and Supply Chain Risk Management (“SCRM”) in order to receive BEAD funding. States and federal territories, as Eligible Entities (“EEs”), will have to require subgrantees to attest that these plans are operational and public by the time an award is granted. Requiring subgrantees to have operational cyber and SCRM plans is essential to ensuring that networks are built with resiliency. Still, given the multitude of jurisdictions that will be building networks across the country with BEAD funding, TIA urges states to consider a standardized approach to ensuring BEAD cyber and SCRM requirements are met.

In the NoFO’s section on Cybersecurity and SCRM, NTIA seeks to impose baseline security requirements for subgrantees and allows EEs to adopt additional rules as they see fit. The NoFO requires all subgrantees to establish cyber and SCRM plans which, among other requirements, must map to the provisions of four existing government documents: the National Institute of Standards and Technology’s (“NIST”) Framework for Improving Critical Infrastructure Cybersecurity, the standards and controls from Executive Order 14028, NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, and NIST 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Taken together, these documents constitute over 400 pages of guidance that subgrantees must adhere to in order to receive BEAD funding. Although comprehensive, these four documents do not provide a clear and concise methodology for organizing and evaluating a sub-grantee's SCRM plan. TIA's SCS 9001TM Supply Chain Security Management System, aligns very well with NTIA's intent and the requirements outlined in the four referenced documents and will allow for precise measuring and certifying of performance.

In addition to requiring guidance from existing federal cyber and SCRM documents, the NoFO requires the subgrantee's cyber and SCRM plans to be reevaluated "on a periodic basis" and ensure that the plans meet the latest version of the federal security documents listed in the NoFO. This requirement means that EEs will be required to review and audit subgrantees for compliance with existing federal requirements cited by the NoFO on a routine basis. As each EE will most likely have multiple sub-grantees and several prospective sub-grantees vying for an award, having a single methodology to evaluate alignment versus the standard and compare responses will be of great value. Building a SCRM checklist of specific requirements, captured from the four referenced documents, into the Final Proposal will enable each potential sub-grantee to make a clear and concise response and allow the EE to compare and contrast responses more easily.

Over fifty EEs will have to implement cyber and SCRM requirements for BEAD funding that align with these four federal documents, as well as determine how compliance will be audited. As such, we strongly believe that a standard set of guidance on security will simplify EEs' requirements under the BEAD NoFO and promote the construction of secure networks in jurisdictions across the country. Cyber threats do not discriminate based on state lines, and all EEs would benefit from ensuring that networks built in their localities using BEAD funding are built to the best industry-led standard regarding security. Additionally, utilizing standardized security requirements will ensure that an EE has robust competition during the application process, as potential subgrantees will benefit from a universal methodology to follow when applying for BEAD funding to build networks in potentially dozens of statewide requests.

As an SDO that has developed hundreds of standards for building networks, TIA has focused on using standards to add transparency to the ICT supply chain and standardize ICT security. That led us to create SCS 9001 – The ICT industry's first standard focused on the ICT supply chain. SCS 9001 is a certifiable standard developed by the ICT industry. SCS 9001 is a cyber and supply chain security management standard developed by members of the ICT industry for the ICT industry. SCS 9001 was developed to provide assurance of the proper operational hygiene of network operators and vendors in delivering products and services that are inherently more secure. Additionally, there is precedence for governments requiring certification to standards -- after consultation with the U.S. Departments of Commerce and the State Department, Costa Rica released security guidelines requiring certification to SCS 9001 for their new 5G network builds.

SCS 9001 contains 116 high-level requirements with most being multi-part.

When fully considered, there are over 750 individual requirements. Further, SCS 9001 contains 60 controls and also specifies seven measurements for those organizations electing to participate in TIA's Industry Benchmarking program.

SCS 9001 was developed to help evaluate and provide higher assurance that vendors:

operate their businesses with integrity, transparency, and trust,

conduct all aspects of operations with a high level of security consideration,

develop products and services with security built in from conception and considered throughout the entire product lifecycle and

have made requisite investments to support products through their entire lifecycle, including the ability to quickly identify, mitigate and resolve vulnerabilities found post-deployment.

Most importantly, SCS 9001 is a standard that already works to operationalize existing government initiatives, including the four documents cited by the NoFO. By certifying to SCS 9001, subgrantees can demonstrate that they've taken steps to operationalize their cyber and SCRM plans in line with NTIA's intent to ensure projects funded by BEAD are deployed in a transparent, accountable, and, above all, secure manner. SCS 9001 certification scales in relation to an entity's size and operational complexity, meaning certification would work for large internet service providers ("ISPs") and smaller, more regional ISPs. A subgrantee's certification would also meet the NoFO's requirements to demonstrate the "technical capabilities of the subgrantee" while fulfilling an EE's requirement of "ensuring that subgrantees are competent" as they will have already completed certification for cyber and SCRM baseline requirements within SCS 9001. EEs could also utilize SCS 9001's routine audits as part of an entity's certification that could be used as a basis for a state's need to "conduct audits of subgrantees" to show that cyber and SCRM plans remain up to date and operationalized.

TIA believes that a subgrantee's certification to SCS 9001 will satisfy the security requirements of the BEAD NoFO while aiding potential subgrantees by offering clarity for how these requirements can be met statewide and nationwide. SCS 9001 furthers the idea that security must be built in by design rather than bolted on as an afterthought, and a subgrantee that has met the comprehensive requirements of the standard will have met the needs of most if not every, state administering BEAD programs. Similarly, mapping the security requirements for BEAD funding to SCS 9001 allows EEs to manage the NoFO's auditing obligations more uniformly as the SCS 9001 certification process includes routine audits which would satisfy a state's need to "conduct audits of subgrantees" cyber and SCRM plans as opposed to solely relying on a self-attestation.

TIA appreciates this opportunity to provide feedback on volume 2 of Kansas' Initial Proposal, and we look forward to continuing to work towards the shared goal of connecting every American with trusted, high-speed networks. We believe this goal would be best served by taking a uniform, industry-led approach to security that will result in Americans being connected with secure and trusted networks. We welcome any questions or further opportunities to discuss the work of TIA and our members and how to ensure the BEAD program is a lasting success.

Please do not hesitate to contact me with any questions.

Sincerely,

Mike Regan

Vice President of Business Performance

---

By submitting the Public Comment Form (the "Form") and any supporting evidence, you attest that all information furnished is true and accurate to the best of your knowledge and that any attachments are free of malware or viruses. You also acknowledge that falsifying any information could result in legal action against you and will bar you from submitting public comments to this web site in the future. You authorize the Kansas Office of Broadband Development, Kansas Department of Commerce (KOBD) to contact you if further information is needed. You expressly acknowledge and

Mike Regan

consent to some personal information, including your name, address, phone, e-mail, organization you represent, and comments, being posted for public view on the Kansas Department of Commerce web site at www.kansascommerce.gov. The KOBD will use its best efforts to redact any personal identifiable information outside of the above that is not considered in the public domain. By typing your name and date and by submitting the Form, you acknowledge, authorize, and consent to this Public Comment Privacy & Acknowledgments.