IMPLEMENTING THE NEW CYBERSECURITY AND SUPPLY CHAIN RISK MANAGEMENT REQUIREMENTS FOR THE BEAD PROGRAM

State and Territory Governments Guide to Meeting New Cybersecurity and Supply Chain Risk Management Requirements (C/SCRM) from NTIA Notice of Funding Opportunity (NOFO)

NEW SECURITY REQUIREMENTS

The National Telecommunications and Information Administration (NTIA) has established new and unprecedented Cybersecurity and Supply Chain Risk Management (C/SCRM) requirements in its Notice of Funding Opportunity (NOFO) for subgrantees to be eligible for funding from the Broadband Equity Access Deployment (BEAD) program. Before allocating any BEAD program funds, Eligible Entities (EEs) must review the C/SCRM Plans from prospective subgrantees (e.g., service providers) to ensure they meet the NTIA grant requirements. States and territories that qualify as EEs to apply for grants under the BEAD program will require prospective subgrantee's attestation that the proper plans are in place and make the subgrantee's C/SCRM plan available to NTIA upon request.

CYBERSECURITY AND SUPPLY CHAIN RISK MANAGEMENT REQUIREMENTS CAN BE FOUND IN:

Cybersecurity

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- Standards and controls set forth in U.S. Executive Order 14028

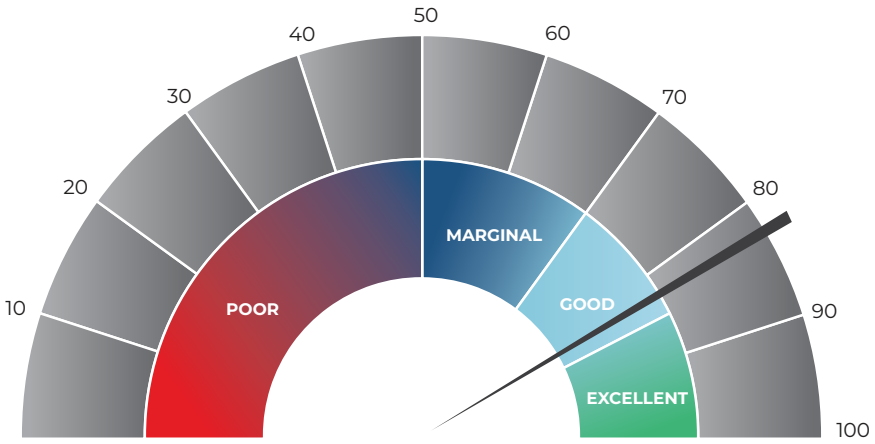
Supply Chain Risk Management

- NIST publication NISTR 8276, Key Practices in Cyber Supply Chain Risk Management Observations from Industry, and related SCRM guidance from NIST
- NIST 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations and specifies the supply chain risk management controls being implemented

ALIGNMENT WITH BEAD SECURITY REQUIREMENTS

The Telecommunications Industry Association (TIA) has completed a detailed analysis of the NOFO C/SCRM requirements and created a comprehensive interactive checklist based on its flagship SCS 9001™ Cyber and Supply Chain Security Standard. This checklist is intended to help the EE's determine whether the C/SCRM operating plans submitted by the subgrantee's reflect the BEAD C/SCRM baseline requirements.

- TIA's new C/SCRM Checklist offers straightforward questions centering on NOFO baseline C/SCRM requirements simplified in 'plain English'
- Answers to the questions are weighted and aggregated to create an overall rating
- A simple gauge is provided for an at-a-glance view of the aggregated checklist score



A GOOD or EXCELLENT rating can provide assurance that the organization's cyber practices reflect the C/SCRM baseline requirements

Access the TIA Checklist

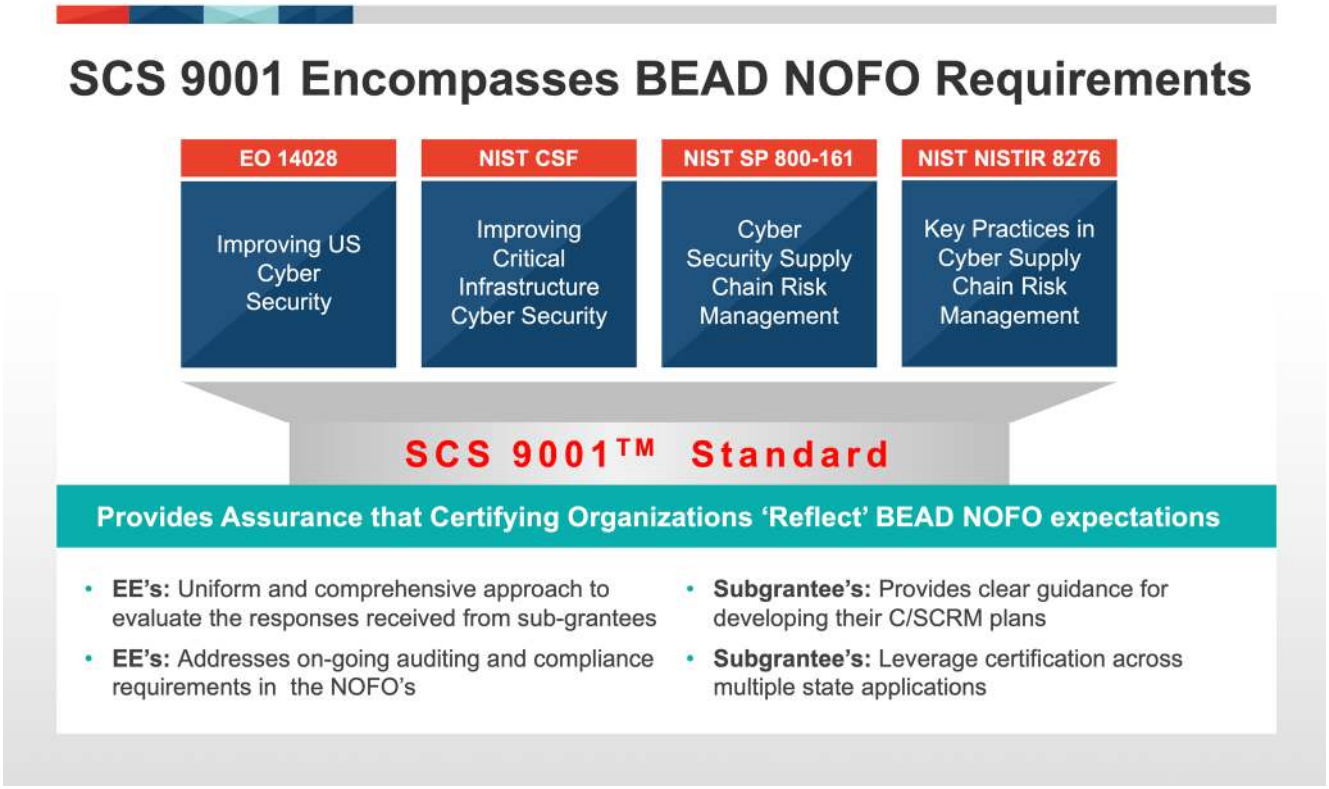
GUIDANCE FOR THE STATES TO ADDRESS C/SCRM REQUIREMENTS

TIA recommends that all EE's incorporate the TIA C/SCRM checklist into their documentation and resources. This will provide a standardized approach for effectively managing the evaluation process when comparing grant application responses. Additionally, it will aid EE's and subgrantees in ensuring compliance with the BEAD C/SCRM NOFO requirements and identifying any areas that require improvement. Specifically, the EE's should include the C/SCRM checklist in:

- The Initial Proposal submitted to NTIA demonstrating how they plan to manage the related requirements.
- The Final Proposal to potential sub-grantees as they look to build specific areas of their states.
- The Resources for potential subgrantees (and their suppliers), guiding them to TIA for related C/SCRM training and support to help them meet the requirements.

SECURING THE ICT SUPPLY CHAIN WITH SCS 9001TM

- In today's digital age, it is crucial for broadband service providers using BEAD funding to establish networks that not only deliver high speeds to consumers but also prioritize resiliency and security. With the increasing prevalence of cyber-attacks on the information and communications technology (ICT) industry, both from non-state actors and government adversaries, the stakes are higher than ever. A recent industry report revealed that a single data breach can cost a company nearly $10 million on average, imposing significant financial burdens on both industry and governments.[1]
- This is a critical time for the ICT industry to act and TIA is leading the charge. With over 80 years of experience developing standards for the ICT industry, TIA and the QuEST Forum committee built the first-ever global Cybersecurity and Supply Chain Security Standard—SCS 9001TM Supply Chain Security Management System. SCS 9001 is a cyber and supply chain security management standard developed by members of 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. SCS 9001 is independently certified and can be used to demonstrate alignment with C/SCRM requirements defined in the BEAD Notice of Funding Opportunity.



GUIDANCE FOR THE SUBGRANTEES TO ADDRESS C/SCRM REQUIREMENTS

TIA recommends that each subgrantee and their suppliers certify to the SCS 9001 standard for assurance that their build plans reflect requirements in the BEAD NOFO. Certifying to SCS 9001 provides the following benefits:

- Provides potential subgrantees with a common methodology to respond to the C/SCRM section in the NOFO.
- Certification to the standard can be leveraged across multiple state applications.
- Helps subgrantees meet the on-going auditing and compliance requirements in the NOFO as the SCS 9001 certification process requires 3-year re-certification and periodic surveillance audits.

ADDITIONAL RESOURCES

- White Paper: SCS 9001 Release 2.0
- Webinar
- C/SCRM Checklist
- SCS 9001 Standard
- Frequently Asked Questions
- Training

REFERENCES

[1] IBM Report US data breaches cost an average of $9.44mn in 2022 Mobile Magazine (mobile-magazine.com)

Access the TIA Checklist

To learn more about SCS 9001 certification contact us at supplychainsecurity@tiaonline.org

BDBR1223