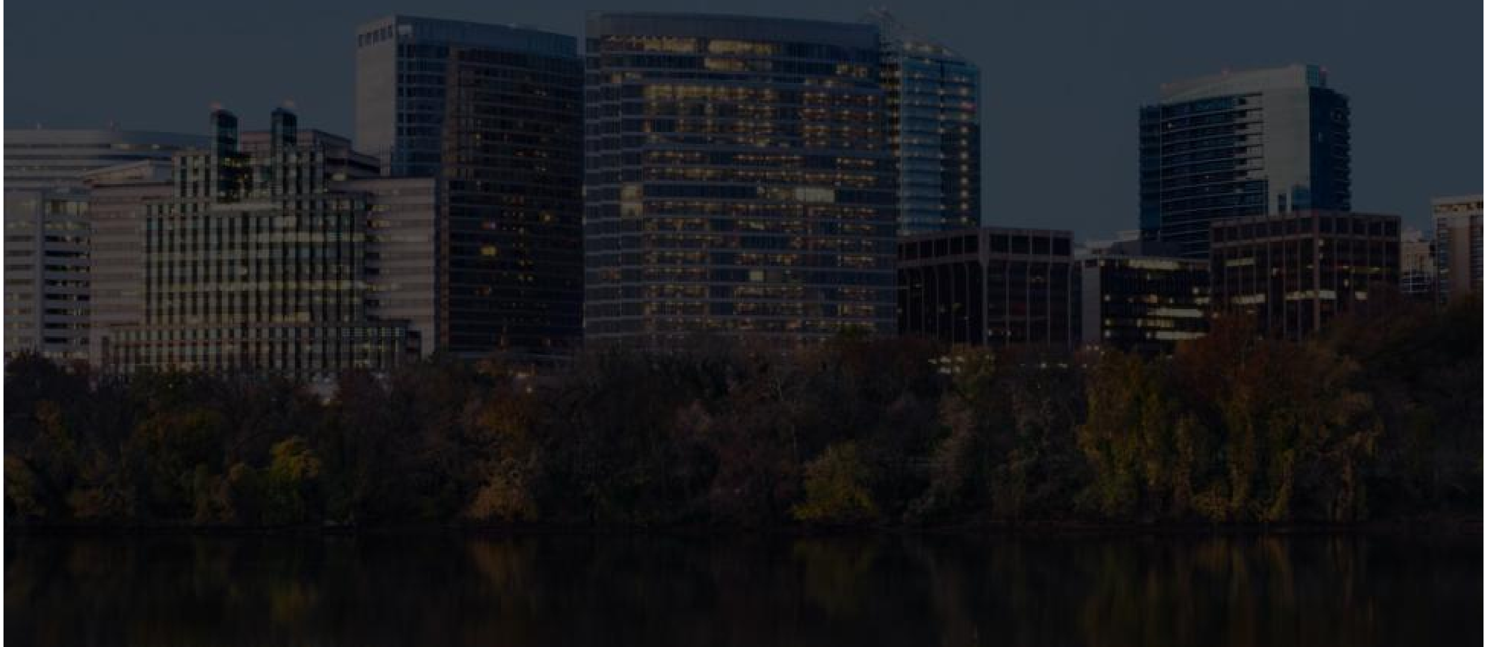

APRIL 18, 2023

TIA BEAD SUCCESS SUMMIT - C/SCRM FREQUENTLY ASKED QUESTIONS (FAQS)

The following Frequently Asked Questions have been developed to provide guidance to State Broadband Offices (Eligible Entities or EEs) in fulfilling their obligations within the BEAD program, specifically in the areas of assessing subgrantees and their alignment with the Cybersecurity and Supply Chain Risk Management baseline requirements enumerated on page 70. Text extracted directly from the NOFO is indicated in this font.

DISCLAIMER: This document is a work intended to evolve along with the BEAD program and input from NTIA and other authorities. This document does not reflect a policy position of TIA or its member companies. We anticipate this document maturing with time and with new information. This document is in the form of a FAQ, but it is not a legal opinion and does not constitute legal advice. This document is subject to change at any time and without notice.

AS AN EE, WHAT AM I REQUIRED TO DO IN MEETING THE NOFO C/SCRM REQUIREMENTS?

The NOFO requires that EEs receive an “attestation” from subgrantees that they meet the NOFO baseline requirements. These requirements include subgrantees providing operational plans that demonstrate that they meet the stated cybersecurity and supply chain security risk management baseline requirements.

Further, EEs have a variety of other responsibilities that relate to the NOFO baseline requirements. Examples include:

- Ensuring that subgrantees are competent (p. 71)
- Ensuring the technical capabilities of the subgrantee (p. 74)
- Ensuring submitted documents demonstrate the subgrantee’s operational capability (p. 75)
- Conduct audits of subgrantees (p. 96 – incorrectly listed as 95 in NOFO)
- Develop monitoring plans for on-going compliance expectations (p. 96 – incorrectly listed as 95 in NOFO)

HOW ARE SUBGRANTEES TO PROVIDE THE ‘ATTESTATION’?

The NOFO is non-specific as to how the attestation is to be provided. It is suggested that EEs define an acceptable format for their subgrantees for consistency in their response. In many cases, and for needs outside of BEAD, a vendor would provide a document called a Supplier Declaration of Conformance (SDoC). An SDoC is a document through which a Page 2 of 2 supplier declares that their product or service meets certain requirements, such as a technical specification or a regulatory requirement. One consideration would be to ask that subgrantees deliver a document that complies with ISO/IEC 17050-1. This standard provides guidance on information that is typically provided within an SDoC. Regardless of the format, it is recommended that EEs archive and store the received attestation(s) for future reference.

WHAT ARE THE C/SCRM BASELINE REQUIREMENTS AND HOW DO I GET THEM?

Section vi. Cybersecurity and Supply Chain Risk Management on page 70 details the C/SCRM requirements. The section opens with:

> The Infrastructure Act directs the Assistant Secretary to specify prudent cybersecurity and supply-chain risk management practices for subgrantees deploying or upgrading broadband networks using BEAD funds. NTIA recognizes the importance of (a) protecting American communications networks and those who use them from domestic and international threat actors, and (b) promoting the natural evolution of cybersecurity and supply-chain risk management practices in a manner that allows flexibility in addressing evolving threats.

Four references are identified as baseline requirements, two each for cybersecurity and supply chain risk management.

The specific references for cyber security are:

- The latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (currently Version 1.1)

  https://doi.org/10.6028/NIST.CSWP.04162018

- The standards and controls set forth in Executive Order 14028: https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

The specific references for Supply Chain Risk Management are:

- NIST publication NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry:

  https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf
- NIST 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. [1]

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

[1]: NIST 800-161 was withdrawn as of May 5, 2022 and replaced with NIST SP 800-161r1.

WHAT SHOULD AN ELIGIBLE ENTITY DO WITH THE OPERATING PLANS ONCE RECEIVED?

The NOFO is non-specific in certain areas of how the BEAD program is to be executed and this is one of them. The NOFO states that delivered risk management plans should ‘reflect’ the 4 referenced requirements. There is no guidance in how to make this determination. Other parts of this document provide additional considerations.

IS THE ELIGIBLE ENTITY RESPONSIBLE FOR REVIEWING SUBGRANTEE OPERATIONAL PLANS FOR SUFFICIENCY?

The NOFO does not directly state that EEs must review subgrantee operating plans for compliance. It does state that EEs must receive an attestation from each subgrantee of their compliance.

However, other sections of the NOFO detail expectations of EEs as to oversight, enforcement and determination of subgrantee operational competence. It will be a challenge to determine whether delivered plans reflect the baseline requirements without a deeper understanding of the baseline requirements. A possible approach would be creating or using available checklists that an EE can leverage to assess delivered risk management plans vs. the identified requirements.

The EE can fill out the checklist, ask the subgrantee to do so, or engage with a consultant to do so.

HOW LONG MUST EE’S MAINTAIN SUBGRANTEE OPERATING PLANS?

The NOFO is non-specific as to the retention period. However, there is a statement within the NOFO that reads:

The Eligible Entity must provide a subgrantee’s plan to NTIA upon NTIA’s request.

There is no qualification in that statement as to time expiration. Accordingly, EEs should likely retain the most recent operating plan for each subgrantee until there is no longer a need to do so and as directed by the NTIA.

The plans may also be needed at a future time considering an EE's responsibility of:

- Ensuring that subgrantees are competent (p. 71)
- Ensuring the technical capabilities of the subgrantee (p. 74)
- Ensuring submitted documents demonstrate the subgrantee's operational capability (p. 75)
- Conduct audits of subgrantees (p. 95)
- Develop monitoring plans for on-going compliance (p. 95

HOW OFTEN DO SUBGRANTEES HAVE TO UPDATE THEIR OPERATING PLANS?

The NOFO is non-specific but states that:

> Plans will be reevaluated and updated on a periodic basis and as events warrant...

The NOFO states that the delivered plans are to be compliant with the baseline requirements at the time of attestation. Plans should at least be updated to the most current versions of the baseline requirements as they become available. As an example, a new version of NIST SP 800-161 has been released since the NOFO was published. It is named "NIST SP 800-161r1" and we think it is prudent that EEs ensure that delivered subgrantee operating plans reflect THAT version of the publication.

Further, the NIST Cyber Security Framework (CSF) is undergoing a major revision presently with an estimated availability date of Winter, 2024.

Another example might be if the subgrantee has been acquired or merged with another organization. In that case, operating procedures may be subject to revision and the Eligible Entity should inquire as to potential changes to the previously submitted operating plans.

Finally, in meeting the expectation that plans be updated "on a periodic basis", the EE may want to state that expectation with selected subgrantees and agree upon a reasonable periodicity, such as annual or perhaps semi-annual.

WHEN DO I NEED TO RECEIVE SUBGRANTEE OPERATING PLANS?

The NOFO states that:

The plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes to the plan, a new version will be submitted to the Eligible Entity within 30 days.

EEs will need to determine whether the delivered operating plans are sufficient for the release of funds, or whether they will need to make an assessment of their sufficiency to the baseline requirements considering their enforcement and oversight responsibilities. Once funds are released, they may be difficult to recover if the subgrantee is subsequently found to be non-compliant.

WHAT HAPPENS IF A SUBGRANTEE IS FOUND TO BE NON-COMPLIANT WITH NOFO BASELINE REQUIREMENTS?

Page 95 has a section titled 4. Enforcement. Within this section, it states:

NTIA shall take enforcement action against Eligible Entities and, if necessary, subgrantees, and Eligible Entities shall take enforcement action against subgrantees, as necessary and appropriate [2] :”

1. “A subgrantee that fails to comply with any requirement under Section 60102 of the Infrastructure Act or this NOFO shall be required to return up to the entire amount of the subgrant to the Eligible Entity, at the discretion of the Eligible Entity or the Assistant Secretary.

Certainly, all involved should have a goal of avoiding this situation. This places the onus on the EE to ensure that subgrantees are selected carefully and that proper diligence is performed on their capabilities and their provided C/SCRM operational plans before funding is allocated.

[2]: The Enforcement section identifies 3 areas of non-compliance, only the first is relevant and listed for the purposes of this discussion.

HOW CAN ELIGIBLE ENTITIES PROVIDE A HIGHER LEVEL OF ASSURANCE THAT SUBGRANTEES TRULY MEET THE BASELINE REQUIREMENTS, REGARDLESS OF THEIR ATTESTATION THAT THEY DO?

Considering the expectations of EEs for providing oversight, enforcement and evaluating subgrantees for competency and meeting the expectations of the NOFO, simply relying upon the subgrantees attestation of compliance (and on-going compliance) may be insufficient.

The NOFO provides additional authority to the EE:

> …an Eligible Entity may propose additional measures it believes necessary to safeguard networks networks and users falling within its jurisdiction for consideration by the Assistant Secretary…

The EE may wish to engage with a professional consultancy to help evaluate the subgrantee's submissions. An additional option would be to place demands on subgrantees as a condition of funding to certify to a cyber and / or supply chain security standard to provide a higher level of assurance of compliance to the baseline requirements. The SCS 9001 Cyber and Supply Chain Security management system developed by the Telecommunications Industry Association is one such example.

WHAT ARE AN EE'S ON-GOING RESPONSIBILITIES?

The NOFO states:

> NTIA, Eligible Entities, and subgrantees each have a critical role to play in ensuring that the BEAD Program is implemented in a manner that ensures transparency, accountability, and oversight sufficient to, among other things:
>
> 1. Minimize the opportunity for waste, fraud, and abuse;
>
> 2. Ensure that recipients of grants under the Program use grant funds to further the overall purpose of the Program in compliance with the requirements of the Infrastructure Act, this NOFO, 2 C.F.R. Part 200, the terms and conditions of the award, and other applicable law; and
>
> 3. Allow the public to understand and monitor grants and subgrants awarded under the Program.

The NOFO further states:

To that end, NTIA and Eligible Entities shall:

1. Conduct such audits of grantees and subgrantees as are necessary and appropriate, including audit requirements described in Section VII.G. Eligible Entities shall report the full results of any audits they conduct to the appropriate Federal Program Officer.

2. Develop monitoring plans, subject to the approval of the Assistant Secretary, which may include site visits or desk reviews, technical assistance, and random sampling of compliance requirements.

3. Impose specific conditions on grant awards designed to mitigate the risk of nonperformance where appropriate.

Clearly, the EE's responsibility extends well beyond the selection of the subgrantee and awarding funds. It is not clear how long an EE is required to provide the on-going expectations of oversight, auditing, reporting, monitoring and enforcement.

FOR ADDITIONAL INFORMATION OR INQUIRIES ON UPDATES, PLEASE CONTACT:

Mike Regan

Email: MRegan@tiaonline.org