proposed action is not subject to Executive Order 13045 because it merely proposes to deny a redesignation request as not meeting Federal requirements. Furthermore, EPA's Policy on Children's Health does not apply to this proposed action.

H. Executive Order 13211: Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use

This proposed action is not subject to Executive Order 13211 because it is not a significant regulatory action under Executive Order 12866.

I. National Technology Transfer and Advancement Act (NTTAA)

This proposed action does not involve technical standards.

J. Executive Order 12898 and Executive Order 14096: Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations and Revitalizing Our Nation's Commitment to Environmental Justice for All

Executive Order 12898 (Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, 59 FR 7629, February 16, 1994) directs Federal agencies to identify and address ''disproportionately high and adverse human health or environmental effects'' of their actions on communities with EJ concerns to the greatest extent practicable and permitted by law. Executive Order 14096 (Revitalizing Our Nation's Commitment to Environmental Justice for All, 88 FR 25251, April 26, 2023) builds on and supplements E.O. 12898 and defines EJ as among other things, the ''just treatment and meaningful involvement of all people regardless of income, race, color, national origin, or Tribal affiliation, or disability in agency decision-making and other Federal activities that affect human health and the environment.''

Neither the Cabinet nor the Louisville Metro Air Pollution Control District evaluated EJ considerations as part of the Cabinet's redesignation request; the CAA and applicable implementing regulations neither prohibit nor require an evaluation. EPA did not perform an EJ analysis and did not consider EJ in this proposed action. Consideration of EJ is not required as part of this proposed action, and there is no information in the record upon which this decision is based that is inconsistent with the stated goal of Executive Order 12898/14096 of achieving EJ for communities with EJ concerns.

List of Subjects in 40 CFR Part 81

Environmental protection, Air pollution control, National parks, Wilderness areas.

Authority: 42 U.S.C. 7401 *et seq.*

Dated: December 23, 2024.

Jeaneanne Gettle,

Acting Regional Administrator, Region 4.

[FR Doc. 2024–31617 Filed 1–2–25; 8:45 am]

BILLING CODE 6560–50–P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 2, 7, 11, 12, and 39

[FAR Case 2019–014, Docket No. FAR–2019–0014, Sequence No. 1]

RIN 9000–AN97

Federal Acquisition Regulation: Strengthening America's Cybersecurity Workforce

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Proposed rule.

SUMMARY: DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to incorporate a framework for describing cybersecurity workforce knowledge and skill requirements used in contracts for information technology support services and cybersecurity support services in line with an Executive Order to enhance the cybersecurity workforce.

DATES: Interested parties should submit written comments to the Regulatory Secretariat Division at the address shown below on or before March 4, 2025 to be considered in the formation of the final rule.

ADDRESSES: Submit comments in response to FAR Case 2019–014 to the Federal eRulemaking portal at *https://www.regulations.gov* by searching for ''FAR Case 2019–014''. Select the link ''Comment Now'' that corresponds with ''FAR Case 2019–014''. Follow the instructions provided on the ''Comment Now'' screen. Please include your name, company name (if any), and ''FAR Case 2019–014'' on your attached document. If your comment cannot be submitted using *https://www.regulations.gov,* call or email the points of contact in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Instructions: Please submit comments only and cite ''FAR Case 2019–014'' in all correspondence related to this case. Comments received generally will be posted without change to *https://www.regulations.gov,* including any personal and/or business confidential information provided. Public comments may be submitted as an individual, as an organization, or anonymously (see frequently asked questions at *https://www.regulations.gov/faq).* To confirm receipt of your comment(s), please check *https://www.regulations.gov,* approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: For clarification of content, contact Ms. Malissa Jones, Procurement Analyst, at 571–882–4687 or by email at *malissa.jones@gsa.gov.* For information pertaining to status, publication schedules, or alternate instructions for submitting comments if *https://www.regulations.gov* cannot be used, contact the Regulatory Secretariat at 202–501–4755 or *GSARegSec@gsa.gov.* Please cite ''FAR Case 2019–014.''

SUPPLEMENTARY INFORMATION:

I. Background

DoD, GSA, and NASA are proposing to revise the FAR to incorporate the NICE Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology (NIST) Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework,* for describing workforce knowledge and skill requirements used in contracts for information technology support services and cybersecurity support services in line with Executive Order (E.O.) 13870, America's Cybersecurity Workforce. E.O. 13870 requires agencies to incorporate the NICE Framework, NIST Special Publication 800–181 into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services. DoD, GSA, and NASA are proposing to revise the FAR to ensure that when acquiring information technology support services or cybersecurity support services, agencies describe the cybersecurity workforce tasks, knowledge, skills, and work roles to align with the NICE Framework.

The NICE Framework is a nationally focused resource that categorizes and describes cybersecurity work. The NICE Framework establishes a common language that defines and categorizes cybersecurity competency areas and work roles, including the knowledge

and skills needed to complete tasks in those roles. It is a fundamental resource in the development and support of a prepared and effective cybersecurity workforce that enables consistent organizational and sector communication for cybersecurity education, training, and workforce development. The NICE Framework is intended to be applied in the public, private, and academic sectors to grow the cybersecurity capability of the U.S. Government, increase integration of the Federal cybersecurity workforce, and strengthen the skills of Federal information technology and cybersecurity practitioners.

II. Discussion and Analysis

DoD, GSA, and NASA are proposing to amend the FAR to define terms that are referenced. As such, this rule proposes to amend FAR 2.101 by adding a definition for ''cybersecurity'' and a definition for the ''NICE Workforce Framework for Cybersecurity (NICE Framework)''. Previously known as the ''National Initiative for Cybersecurity Education,'' NICE is now known only by its acronym.

For the acquisition of information technology support services (*e.g.,* backup and recovery services and technical support) or cybersecurity support services (*e.g.,* threat analysis, vulnerability analysis, and digital forensics), the proposed rule implements the following requirements to ensure agencies include the cybersecurity workforce tasks, knowledge, skills, and work roles to align with the NICE Framework in contracts:

- FAR 7.105 is amended to require that agency acquisition plans for the acquisition of information technology support services or cybersecurity support services describe any cybersecurity workforce tasks, knowledge, skills, and work roles to align with the NICE Framework.
- FAR 11.002 is amended to require that cybersecurity workforce tasks, knowledge, skills, and work roles described in agency requirements documents align with the NICE Framework. Agencies shall also require offers, quotes, and reporting requirements (*e.g.,* contractor deliverables) to align with the NICE Framework.
- FAR 12.202 is amended to require, for the acquisition of commercial products and commercial services, compliance with the direction at FAR 11.002 for incorporating the NICE Framework in requirements documents.
- FAR 39.104 is amended to reference, for information technology support services and cybersecurity support services, the direction at FAR 11.002 for incorporating the NICE Framework in requirements documents.

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold (SAT) and for Commercial Products (Including Commercially Available Off-the-Shelf (COTS) Items) or for Commercial Services

This rule does not create new solicitation provisions or contract clauses or impact any existing provisions or clauses.

IV. Expected Impact of the Rule

A. Requirement

This proposed rule implements requirements for agencies procuring information technology support services and cybersecurity support services to provide—

(1) The cybersecurity workforce tasks, knowledge, skills, and work roles to align with the NICE Framework in their acquisition plans as a security consideration;

(2) A description, in the requirements documents, of the cybersecurity workforce tasks, knowledge, skills, and work roles to align with the NICE Framework; and,

(3) Requirements for offers, quotes, and reporting requirements (*e.g.,* contract deliverables) to align with the NICE Framework.

B. Impact

Government. This rule will require agencies to become familiar with the NICE Framework provided in NIST Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework* in order to describe the cybersecurity workforce tasks, knowledge, skills, and work roles when procuring information technology support services and cybersecurity support services. Agencies are expected to verify that offers, quotes, and reporting requirements (*e.g.,* contract deliverables) align with the NICE Framework. It is expected that this will take place as a part of the Government's existing acquisition process.

Public. This rule does not add any new information collection or additional requirements for contractors. This rule requires contractors to ensure contract deliverables are consistent with the NICE Framework when specified for the acquisition of information technology support services and cybersecurity support services.

Regulatory familiarization. It is expected that contractors providing information technology support services and cybersecurity support services will be required to become familiar with the NICE Framework (NIST Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework*) which is estimated to take 20 hours. Contractors may be required to update their policies and procedures to comply with the NICE Framework requirements for acquisitions of information technology support services and cybersecurity support services. The cost to the public associated with this rule is not expected to be significant because it is limited to the cost of regulatory familiarization and the application of its requirements to offers and quotes for information technology support services and cybersecurity support services.

Based on data from the Federal Procurement Data System (FPDS) for fiscal years (FY) 2021, 2022, and 2023, there was an average of 5,468 unique entities that were awarded contracts for information technology services, of which 64 percent (3,490) are unique small entities. Considering this information, the Government assumes that approximately 50 percent of the unique entities may be awarded a contract for information technology support services or cybersecurity support services. Therefore, it is estimated that 2,734 entities, of which 1,745 are unique small entities, would need to ensure that the contract deliverables submitted to the Government, are consistent with the NICE Framework. The Government has no way to estimate the number of entities awarded non-information technology services awards that contain some information technology support services requirements or cybersecurity support services requirements.

V. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 (as amended by E.O. 14094) and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule is not a significant regulatory action and, therefore, was not subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993.

VI. Regulatory Flexibility Act

DoD, GSA, and NASA do not expect this proposed rule, if finalized, to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601–612. However, an Initial Regulatory Flexibility Analysis (IRFA) has been performed and is as follows:

1. Reasons for the action.

The reason for this proposed rule is to revise the Federal Acquisition Regulation (FAR) to incorporate the NICE Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology (NIST) Special Publication 800–181 for describing workforce knowledge and skill requirements used in contracts for information technology support services and cybersecurity support services in line with Executive Order (E.O.) 13870, America's Cybersecurity Workforce. E.O. 13870 directs agencies to incorporate the NICE Framework lexicon and taxonomy into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services.

2. Objectives of, and legal basis for, the rule.

The objective of this rule is to strengthen the cybersecurity workforce on Federal contracts by incorporating the cybersecurity workforce tasks, knowledge, skills, and work roles into requirements to align with the NICE Framework (NIST SP 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework*).

The rule proposes to amend FAR 7.105 to add the NICE Framework to the list of security considerations analyzed during acquisition planning for information technology support services and cybersecurity support services. The proposed rule also includes amendments to FAR 11.002 to require agencies to provide workforce knowledge and skill requirements and contract deliverables that are consistent with the NICE Framework in their requirements documentation.

The legal basis for the rule is E.O. 13870, America's Cybersecurity Workforce. Promulgation of the FAR is authorized by 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

3. Description of and an estimate of the number of small entities to which the rule will apply.

Based on data from the Federal Procurement Data System (FPDS) for fiscal years (FY) 2021, 2022, and 2023, there was an average of 5,468 unique entities that were awarded contracts for information technology services, of which 64 percent (3,490) are unique small entities. Considering this information, the Government assumes that approximately 50 percent of the unique entities may be awarded a contract for information technology support services or cybersecurity support services. Therefore, it is estimated that 2,734 entities, of which 1,745 are unique small entities, would need to ensure that the contract deliverables submitted to the Government are consistent with the NICE Framework. The Government has no way to estimate the number of entities awarded non-information technology services awards that contain some information technology support services requirements or cybersecurity support services requirements.

4. Description of projected reporting, recordkeeping, and other compliance requirements of the rule.

There are no reporting, recordkeeping, or other compliance requirements in this rule.

5. Relevant Federal rules which may duplicate, overlap, or conflict with the rule.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

6. Description of any significant alternatives to the rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the rule on small entities.

DoD, GSA, and NASA were unable to identify any alternatives that would reduce the burden on small entities and still meet the objectives of E.O. 13870.

The Regulatory Secretariat has submitted a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat. DoD, GSA, and NASA invite comments from small business concerns and other interested parties on the expected impact of this proposed rule on small entities.

DoD, GSA, and NASA will also consider comments from small entities concerning the existing regulations in subparts affected by the rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C 610 (FAR Case 2019–014), in correspondence

VII. Paperwork Reduction Act

This rule does not contain any information collection requirements that require the approval of the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. 3501–3521).

List of Subjects in 48 CFR Parts 2, 7, 11, 12, and 39

Government Procurement.

William F. Clark,

Director, Office of Government-wide Acquisition Policy, Office of Acquisition Policy, Office of Government-wide Policy.

Therefore, DoD, GSA, and NASA propose amending 48 CFR parts 2, 7, 11, 12, and 39 as set forth below:

■ 1. The authority citation for 48 CFR parts 2, 7, 11, 12, and 39 continues to read as follows:

Authority: 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

PART 2—DEFINITIONS OF WORDS AND TERMS

■ 2. Amend section 2.101 by adding in alphabetical order the definitions ''Cybersecurity'' and ''NICE Workforce Framework for Cybersecurity (NICE Framework)''.

2.101 Definitions.

* * * * *

Cybersecurity means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (see National Security Presidential Directive/NSPD–54, Homeland Security Presidential Directive/HSPD–23.)

* * * * *

NICE Workforce Framework for Cybersecurity (NICE Framework) means a common language for describing cybersecurity work which expresses the work as task statements and includes knowledge and skill statements that provide a foundation for learners including students, job seekers, and employees (see National Institute of Standards and Technology Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework).*

PART 7—ACQUISITION PLANNING

■ 3. Amend section 7.105 by revising paragraph (b)(18)(ii) to read as follows.

7.105 Contents of written acquisition plans.

* * * * *

(b) * * *

(18) * * *

(ii)(A) For information technology acquisitions, discuss how agency information security requirements will be met.

(B) For the acquisition of information technology support services or cybersecurity support services, describe any cybersecurity workforce tasks, knowledge, skills, and work roles to align with the NICE Workforce Framework for Cybersecurity (NICE Framework) (National Institute of Standards and Technology Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework*) in effect at the time the solicitation is issued (see 11.002(i)).

PART 11—DESCRIBING AGENCY NEEDS

■ 4. Amend section 11.002 by adding paragraph (i) to read as follows:

11.002 Policy.

* * * * *

(i) Agencies shall procure information technology support services and cybersecurity support services in accordance with section 39.104. Agencies shall—

(1) Ensure any cybersecurity workforce tasks, knowledge, skills, and work roles described in the requirements documents are aligned with the NICE Workforce Framework for Cybersecurity (NICE Framework) (National Institute of Standards and Technology Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework*) in effect at the time the solicitation is issued; and

(2) Require any offers, quotes, and reporting requirements (*e.g.,* contract deliverables) to align with the NICE Framework in effect at the time of the solicitation.

PART 12—ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

■ 5. Amend section 12.202 by adding paragraph (f) to read as follows:

12.202 Market research and description of agency need.

* * * * *

(f) When acquiring information technology support services or cybersecurity support services, requirements documents shall describe any cybersecurity workforce tasks, knowledge, skills, and work roles to align with the NICE Workforce Framework for Cybersecurity (NICE Framework) (see NIST Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework*) in effect at the time the solicitation is issued (see 11.002(i) and 39.104(b)).

PART 39—ACQUISITION OF INFORMATION TECHNOLOGY

■ 6. Revise section 39.104 to read as follows:

39.104 Information technology services.

(a) When acquiring information technology services, solicitations must not describe any minimum experience or educational requirement for proposed contractor personnel unless the contracting officer determines that the needs of the agency—

(1) Cannot be met without that requirement; or

(2) Require the use of other than a performance-based acquisition (see subpart 37.6).

(b) When acquiring information technology support services (*e.g.,* backup and recovery services, technical support) or cybersecurity support services (*e.g.,* threat analysis, vulnerability analysis, digital forensics), which are a subset of information technology services, agencies must—

(1) Ensure any cybersecurity workforce tasks, knowledge, skills, and work role requirements align with the NICE Workforce Framework for Cybersecurity (NICE Framework) (National Institute of Standards and Technology Special Publication 800–181 and additional tools to implement it at *https://www.nist.gov/nice/framework*) in effect at the time the solicitation is issued (see 11.002(i)); and

(2) Ensure any cybersecurity workforce tasks, knowledge, skills, and work role requirements comply with paragraph (a) of this section.

[FR Doc. 2024–30504 Filed 1–2–25; 8:45 am]

BILLING CODE 6820–EP–P