D. Be divided into short sections and sentences; and

E. Use lists and tables whenever possible.

If you feel that we have not met these requirements, send us comments by one of the methods listed in the **ADDRESSES** section. To better help us revise the rule, your comments should be as specific as possible. For example, you should tell us the numbers of the sections or paragraphs that you find unclear, which sections or sentences are too long, or the sections where you feel lists or tables would be useful.

List of Subjects

30 CFR Part 250

Administrative practice and procedure, Continental shelf, Environmental impact statements, Environmental protection, Government contracts, Investigations, Mineral resources, Oil and gas exploration, Penalties, Pipelines, Continental Shelf—mineral resources, Continental Shelf—rights-of-way, Reporting and recordkeeping requirements, Sulfur.

30 CFR Part 290

Administrative practice and procedure.

Steven H. Feldgus,

Deputy Assistant Secretary, Land and Minerals Management.

For the reasons stated in the preamble, the Department of the Interior is proposing to revise 30 CFR parts 250 and 290 as follows:

PART 250—OIL AND GAS AND SULPHUR OPERATIONS IN THE OUTER CONTINENTAL SHELF

■ 1. The authority citation for part 250 continues to read as follows:

Authority: 30 U.S.C. 1751, 31 U.S.C. 9701, 33 U.S.C. 1321(j)(1)(C), 43 U.S.C. 1334.

Subpart N—Outer Continental Shelf Civil Penalties

■ 2. Amend § 250.1409 by:
■ a. Revising paragraph (b) introductory text;
■ b. Redesignating paragraph (d) as paragraph (e);
■ c. Adding new paragraph (d); and
■ d. Revising paragraph (e).

The revisions and additions read as follows:

§ 250.1409 What are my appeal rights?

* * * * *

(b) In order to file an appeal, you must perform one of the following actions within the 60-day appeal period to have your appeal heard:

* * * * *

(d) Satisfying the bonding requirement in paragraph (b) of this section is a jurisdictional precondition for a civil penalty appeal. If you have timely filed a request with BOEM pursuant to paragraph (b)(2) of this section to use your lease-specific/area-wide bond on file as the bond for the penalty amount, the IBLA's jurisdiction over the appeal is preserved while BOEM's decision on your request is pending. Should BOEM deny your request or require additional security pursuant to paragraph (c) of this section, you have 30 days to satisfy paragraph (b)(1) of this section or post the required additional security, as applicable, and jurisdiction is preserved during that 30-day period. If you fail to satisfy these bonding requirements, the IBLA will lose jurisdiction and must dismiss your appeal.

(e) If you do not either pay the penalty or fully satisfy the appeal requirements, the Department may take one or more of the following actions:

(1) Collect the amount you were assessed, plus interest, late payment charges, and other fees as provided by law, from the date you received the Reviewing Officer's final decision until the date we receive payment;

(2) Initiate additional enforcement, including, if appropriate, cancellation of the lease, right-of-way, license, permit, or approval, or the forfeiture of a bond under this part; or

(3) Bar you from doing further business with the Federal Government according to Executive Orders 12549 and 12689, and section 2455 of the Federal Acquisition Streamlining Act of 1994, 31 U.S.C. 6101. The Department of the Interior's regulations implementing these authorities are found at 43 CFR part 12, subpart D.

PART 290—APPEAL PROCEDURES

■ 3. The authority citation for part 290 continues to read as follows:

Authority: 5 U.S.C. 305; 43 U.S.C. 1334.

Subpart A—Bureau of Safety and Environmental Enforcement Appeal Procedures

■ 4. Amend § 290.4 by:
■ a. Removing the text ''and'' at the end of paragraph (a);
■ b. Removing the text ''.'' at the end of the sentence and adding the text ''; and'' at the end of the paragraph (b) introductory text; and
■ c. Adding paragraph (c).

The revisions and additions read as follows:

§ 290.4 How do I file an appeal?

* * * * *

(c) If you are appealing a civil penalty assessment, either notification of payment of the penalty or documentation demonstrating satisfaction of the requirements in 30 CFR 250.1409(b). You cannot extend the 60-day period for satisfying this requirement, except as specifically provided in 30 CFR 250.1409(d).

[FR Doc. 2023–27079 Filed 12–12–23; 8:45 am]

BILLING CODE 4310–VH–P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 117

[Docket ID: DoD–2023–OS–0061]

RIN 0790–AL52

National Industrial Security Program Operating Manual (NISPOM); Amendment

AGENCY: Office of the Under Secretary of Defense for Intelligence & Security, Department of Defense (DoD).

ACTION: Proposed rule.

SUMMARY: DoD is proposing amendments to the National Industrial Security Program Operating Manual (NISPOM) based on public comments received on a final rule published on December 21, 2020. The proposed amendments address implementation guidance and costs for the Security Executive Agent Directive (SEAD) 3, clarifications on procedures for the protection and reproduction of classified information, controlled unclassified information (CUI), National Interest Determination (NID) requirements for cleared contractors operating under a Special Security Agreement for Foreign Ownership, Control or Influence, and eligibility determinations for personnel security clearance processes and requirements.

DATES: Comments must be received on or before February 12, 2024.

ADDRESSES: You may submit comments, identified by docket number and/or Regulatory Identifier Number (RIN) and title, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name and

docket number or RIN for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Allyson Renzella, 703–697–9209.

SUPPLEMENTARY INFORMATION:

Background

The NISPOM establishes requirements for the protection of classified information disclosed to or developed by contractors, licensees, grantees, or certificate holders to prevent unauthorized disclosure. The National Industrial Security Program (NISP) is established by Executive Order (E.O.) 12829 ''National Industrial Security Program (NISP)'' (available at *https://www.archives.gov/files/isoo/policy-documents/eo-12829-with-eo-13691-amendments.pdf*) provides a single integrated, cohesive industrial security program to protect classified information to preserve our Nation's economic and technological interests. Under the NISP, the USG establishes requirements for the protection of classified information to be safeguarded in a manner equivalent to its protection within the executive branch of USG, where practicable. For industry, those requirements are included in the NISPOM. When bound by contract, license, or grant, industry must comply with the NISPOM and any Cognizant Security Agency (CSA)-specific supplementary guidance for unique CSA mission requirements. As the Executive Agent of the NISP, the Secretary of Defense is responsible for overall implementation of the program. The Department of Defense (DoD) issues and maintains the NISPOM with the concurrence of the other four NISP CSAs and in consultation with other affected Federal agencies.

DoD codified the NISPOM in a final rule on December 21, 2020 (85 FR 83300–83364) *National Industrial Security Program Operating Manual (NISPOM)* to add 32 CFR part 117 to the Code of Federal Regulations (CFR). The rule was effective on February 24, 2021. In addition to adding the NISPOM to the CFR, the final rule incorporated requirements of Security Executive Agent Directive (SEAD) 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.* SEAD 3 requires reporting by all contractor cleared personnel who have been granted eligibility for access to classified information. The final rule provided a single nation-wide implementation plan to include SEAD 3 reporting by all contractor cleared personnel to report specific activities that may adversely impact their continued national security eligibility, such as reporting of foreign travel and foreign contacts. NISP CSAs are required to conduct an analysis of such reported activities to determine whether they pose a potential threat to national security and take appropriate action. Finally, the rule also implemented the provisions of Section 842 of Public Law 155–232, which removed the requirement for a covered National Technology and Industrial Base (NTIB) entity operating under a special security agreement pursuant to the NISP to obtain a national interest determination as a condition for access to proscribed information. The 60-day public comment period ended on February 19, 2021.

On August 19, 2021, DoD published a technical amendment to the December final rule (at 86 FR 46597–46599) to extend until August 24, 2022, the implementation date for those contractors under DoD security cognizance to report and obtain pre-approval of unofficial foreign travel to the DoD. The technical amendment was effective on August 19, 2021 and was done to allow DoD to make modifications to its information technology (IT) systems. The technical amendment addressed comments from regulated parties on the burdensome nature of submitting individual foreign travel reports for those contractors under DoD security cognizance. The technical amendment allowed DoD more time to make the necessary changes to the IT system for multiple foreign travel reports in a single submission.

This proposed rule addresses the comments received on the final rule published in December 2020 and further amends the 32 CFR 117 to make the following changes as discussed below.

Discussion of Comments and Changes

The December 21, 2020 final rule received nine sets of public comments from five individuals who provided 11 comments, two companies that provided 41 comments, an industry representative organization that provided 28 comments, and a law firm that provided four comments, for a total of 84 comments.

Clarification on Procedures

The vast majority of the comments related to a request for clarification on procedures for those contractors under DoD security cognizance. Many of the comments did not result in a change to the rule because they related to procedures that a NISP CSA would provide to supplement unique CSA mission requirements. For contractors under DoD security cognizance, DoD provides unique CSA mission guidance via industrial security letters (ISLs) when applicable. ISLs are published on the Defense Counterintelligence and Security Agency (DCSA) website (*https://www.dcsa.mil/*) and will address the comments received and re-issue previous NISPOM ISLs, as needed. Previous ISLs were tied to the content of the NISPOM when it was a DoD manual. Some of the guidance contained in prior ISLs has been incorporated into the rule and is no longer needed. Those ISLs that are still needed in order to provide further guidance to those contractors under DoD security cognizance will be re-issued in accordance with the rule.

Comments Related to SEAD 3 Implementation

Many comments were received on § 117.8, relating to implementation of SEAD 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position,* published by the Office of the Director of National Intelligence. Commenters were concerned with the lack of guidance on how information systems will be used to report foreign travel and when foreign travel reporting should be accomplished by contractors. Also, commenters requested more details as to who approves foreign travel requests: the contractor security staff, the government customer, or CSA. DoD also received comments from regulated parties stating it would be burdensome for contractors under DoD security cognizance to submit individual foreign travel reports. Regulated parties recommended DoD modify its information technology (IT) system so a contractor may submit multiple or batched foreign travel reports in a single submission. As discussed earlier, to allow time for the completion of modifications to DoD's IT system, DoD published an amendment on August 19, 2021, to extend until August 24, 2022, the implementation date for contractors under DoD security cognizance to report and obtain pre-approval of unofficial foreign travel to DoD. The IT system was modified prior to the August 2022 implementation date and can now receive multiple foreign travel reports at a time.

Additionally, one commenter opined the cost to contractors to implement SEAD 3 was underestimated—both in

the time it will take to report and the number of reports that will be generated. We agree with this assessment and the corrected numbers can be found in the cost analysis section of the preamble. Further, commenters asked how the CSA will analyze the reported data and if the analysis will be shared with the contractor or the cleared employee going on foreign travel. For those contractors under DoD cognizance, guidance was provided via an ISL (*https://www.dcsa.mil/Portals/128/Documents/CTP/tools/ISL2021-02_SEAD-3.pdf*) to provide supplementary procedures and inform industry how compliance with SEAD 3 will be accomplished for unique DoD mission needs.

Controlled Unclassified Information

DoD received seven comments on CUI as it relates to the paragraphs on security reviews (§ 117.7), training (§ 117.12), and safeguarding CUI (§ 117.15). DoD did not make any changes to the rule as compliance with CUI is outside the scope of the NISP. For the purposes of this rule, if a contractor has a classified contract that also includes provisions for CUI, then, under certain circumstances, CUI assessments may be conducted by the CSA in conjunction with NISP USG reviews. The contractor must follow the requirements as stated in their contract concerning the safeguarding of CUI.

Security Reviews

DoD received several comments on § 117.7, to include that a facility security officer (FSO) should be a U.S. citizen with no exceptions; and the text was updated accordingly in 117.7(b). The text clarifies that the only exception for U.S. citizenship may apply to the Senior Management Official or Insider Threat Program Senior Official if the entity has a limited entity eligibility determination due to foreign ownership, control, or influence. Two commenters observed that § 117.7(h)(1)(i) did not include the frequency of security review cycles. DoD is accepting this change and has modified § 117.7(h)(1)(i) to reflect security reviews will only occur once every 12 months unless special circumstances exist, to include addressing security vulnerabilities found during a previous security review. Another commenter expressed concern the final rule allowed a CSA to conduct unannounced reviews at its discretion without any specific guidelines. Based on this comment, DoD has proposed to update § 117.7(h)(1)(ii)(A) to clarify unannounced security reviews will be conducted only if there is a possibility of the imminent loss or compromise of classified information.

Eligibility Determinations

DoD received several comments on eligibility determinations in § 117.10, to include a request for clarification on the system of record for personnel security clearances, clarification of requirements for current investigations, reinvestigation, and continuous evaluation requirements, definition of what is considered a break in access and break in employment, and the process for requesting and granting an extension if a temporary eligibility determination goes beyond a year. DoD is not proposing any changes based on these comments as clarification to contractors under DoD cognizance will be provided when applicable via ISLs.

National Interest Determination (NID) Requirements

DoD received comments on the changes to the NID requirements for a covered National Technology and Industrial Base (NTIB) entity based on section 842 of Public Law 115–232 included in § 117.11. Commenters asked for clarification on which specific entities fall under section 842 of Public Law 115–232 and recommended that NIDs be eliminated completely. The final NISPOM rule reflects language taken directly from section 842 of Public Law 115–232, which includes eliminating a NID requirement for U.S.-cleared companies owned by Australia, Canada, and the United Kingdom. DoD is not making any changes based on these comments as DoD is unable to eliminate NIDs, since the provisions for NID requirements are driven by 32 CFR part 2004, *National Industrial Security Program,* and not this rule. There has been no change to the NID requirements in 32 CFR part 2004 outside of section 842 Public Law 115–232.

Safeguarding

Eight comments were received on safeguarding, § 117.15, to include four on open storage areas and another four on intrusion detection systems (IDS). Commenters also requested more guidance on open storage area requirements included in the previous NISPOM DoD Manual, to include procedures for leaving an open storage area unattended during business hours, whether self-approval authority can still be delegated to FSOs by a CSA, procedures to ensure the structural integrity of the space, and whether open bin and open shelf storage is still permitted. DoD is proposing updated text in § 117.15(a) and (c) to address several of these comments (*e.g.,* procedures for leaving an open storage area unattended during business hours and delegation of approval authority to FSOs if agreed to by the CSA, respectively) and as a result added a definition for ''pedestrian door locks'' from the added text on security checks. DoD is also proposing updated text in paragraph 117.15(d) to provide more clarity on required investigative response to alarms for IDS. More guidance on safeguarding for those contractors under DoD cognizance will be provided via forthcoming ISLs, as appropriate. DoD is also proposing additional text to § 117.15(e) regarding information management systems to more accurately reflect the terminology for classified information systems, and as a result added the term ''authorization to operate'' to the definitions section in § 117.3. Finally, DoD is proposing additional text to § 117.15(e)(6) to provide more clarity on the requirements for the reproduction of classified information, to include accountability, control, and marking requirements of the reproduced classified information, and procedures for waste products resulting from the reproduction.

A commenter questioned the accuracy of the text in § 117.17(a)(3) which stated that if an entity eligibility determination could not be completed in time to qualify the prospective subcontractor for participation in a procurement action, that the CSA will continue the entity eligibility determination processing for future contract consideration. After review of this text, DoD has concluded this text provides guidance to CSAs, rather than contractors and is proposing it for deletion.

Joint Personnel Adjudication System

Finally, the reference to the Joint Personnel Adjudication System is proposed for deletion from the list of approved information collections as part of the Paperwork Reduction Act section because it has been discontinued and replaced by the Defense Information System for Security. The text in § 117.5(d) has also been proposed for updating to reflect only the Defense Information System for Security is used for the initiation, investigation, and adjudication of information relevant to DoD security clearances and employment suitability determinations.

Expected Impact of the Proposed Rule and Changes Being Proposed Based on Public Comment

The proposed rule changes seek to provide clarification on safeguarding terminology and correct identified paragraph numbering errors, as well as

address comments from regulated parties seeking more detail or guidance on existing requirements from the final rule published December 21, 2020. The proposed changes are mostly insignificant in that by themselves, these proposed changes create no additional requirements to current NISP policy. For example, a paragraph on subcontracting was removed because it was deemed to be guidance for the government, rather than contractors (*i.e.,* the regulated parties). Also, the references to the Joint Personnel Adjudication System as the system of record for personnel security clearance processing were removed and replaced with the current system of record, Defense Information System for Security. These changes create no additional burden or cost to contractors; but rather seek to provide updated, accurate information. The proposed changes also seek to clarify terminology in relation to safeguarding requirements, which were initially incorporated into the final rule published December 21, 2020 to be in line with 32 CFR part 2001. These changes are not expected to result in any changes to cost estimates or burden on the regulated parties, but rather provide a more consistent, uniform means to comply with existing NISP requirements across the federal government.

Costs

As stated under the Discussion of Comments and Changes section, DoD received one comment that the cost for implementing SEAD 3 was underestimated in the original rule. DoD agrees with the commenter and the cost estimates have been updated accordingly.

We are including here the summary of information on the baseline cost from the original rule for reference. DCSA began the cost analysis for the baseline costs for fiscal year 2017 by randomly selecting active NISP contractor facilities that have existing DoD approval for classified storage at their own physical locations and having those facilities submit security costs. The randomly selected contractor facilities also have an active facility security clearance and a permanent Commercial and Government Entity (CAGE) Code. In addition to the randomly selected cleared facilities having approved classified storage, DCSA categorizes these contractor facilities for the survey based on the size, scope, and complexity of each contractor's security program.

The general methodology used to estimate security costs incurred by contractor cleared facilities with approved storage of classified information is based on the costs incurred by respondent contractors for the protection of classified information. The methodology captures the most significant portion of industry's costs, which is labor. Security labor in the survey is defined as personnel whose positions exist to support operations and staff in the implementation of government security requirements for the protection of classified information. Guards who are required as supplemental controls are included in security labor. The respondent contractors are requested to compile their cleared facility's current annual security labor cost in burdened, current year dollars with the most recent data being from the 2017 survey. The labor cost, when identified as an estimated percent of each contractor's total security costs, enables the respondent contractors to calculate their total security costs.

Information collected is compiled to create an aggregate estimated cost of NISP classification-related activities. Only the aggregate data is reported. The full enterprise industrial security total baseline cost in the December 21, 2020, rule was estimated to not exceed $1.486 billion for fiscal year 2017. Based on the data collected from the survey, we can be 95% confident the true 2017 total NISP security cost for contractor facilities with approved classified storage is less than $1.486 billion.

Public Cost Analysis of the Changes to the Baseline From This Rule

1. *Cost Analysis.* Throughout, labor rates are adjusted upward by 100% to account for overhead and benefits. The following areas, 1.a and 1.b, were re-evaluated for cost based on the public comment.

a. Train all cleared employees on requirements to submit foreign travel reports. We determined that the estimate of cleared contractor personnel who would be required to be trained should also include TOP SECRET cleared employees rather than just SECRET cleared employees as indicated in the original rule. The FSO at each entity (small or large) must ensure that its cleared employees are trained on the requirements. Such training by the FSO is estimated to take one hour in 2021 and a half an hour in each of the following years up to the 20th year. Using the published Office of Personnel Management GS salary schedule for FY20, the estimated labor rate for an FSO of a small business entity firm is the equivalent of a GS11 step 5 and for an FSO of a large business entity is the equivalent of a GS13, step 5. These assumptions imply total costs of $0.99 million in 2021 as year one; and, $0.49 million each year from year two through the 20th year. These estimates have not changed from the original baseline.

b. We determined that the estimate of cleared contractor personnel who would be required to submit foreign travel reports should also include TOP SECRET cleared employees rather than just SECRET cleared employees as indicated in the original rule. As a result, the estimated cost has increased from $16.81 to $19.25 million. The following provides details on the estimated increase. All cleared employees, rather than only SECRET cleared employees, must submit foreign travel reports, and receive any pre-travel threat briefings or post travel briefings from the FSO based on the threat according to this rule, SEAD 3, and CSA-provided guidance for unique mission requirements. It is estimated that the number of foreign travel reports submitted annually will increase from 483,681 as estimated in the original rule to 813,054 to comply with the amendment. That estimate is based on analysis of calendar year 2019 unofficial foreign travel reported by DoD civilians and military in the DoD Aircraft and Personnel Automated Clearance System (APACS), a web-based tool for the creation, submission, and approval of aircraft diplomatic clearances and personnel travel clearances (*i.e.,* Country, Theater, and Special Area, as applicable with individual DoD Foreign Clearance Guide (FCG), *https://www.fcg.pentagon.mil* country pages) designed to aid USG travelers on official government and unofficial (*e.g.,* leave) travel. For calendar year 2019, there were 126,131 travelers and 113,214 travel requests submitted into APACS. APACS requirements are published on the DoD FCG, *https://www.fcg.pentagon.mil.* Thus, an annual estimate of .89 expected foreign travel trips by traveler (113,214 divided by 126,131). In the small business analysis, there was a total of 18,242 cleared employees in the 658 small entities sampled and 63,598 cleared employees in the remaining 356 non-small businesses. Of the total cleared employees in the small business analysis (as reported in the National Industrial Security System), approximately 22.3% were at small entities, and 77.7% were at non-small businesses. Known number of new travelers expected to be affected by this proposed rule will increase from the initial estimate of 543,462 to 905,818 cleared contractor personnel, an increase of 362,356 to include TOP

SECRET cleared contractor personnel under DoD security cognizance and the estimated trips at .89 per traveler is (905,818 × .89 = 813,054 estimated trips). Assuming the ratio for those employees reporting foreign travel into APACS is the same as cleared employees would report, of the estimated 813,054 foreign trips by cleared employees, it can be estimated that approximately 181,262 (22.3% of 813,054) will be taken by contractors at small entities, and 631,792 (77.7% of 813,054) by contractors at non-small businesses. It is estimated that it will take a half an hour for a cleared employee to report foreign travel in 2021 and in each of the following years up to year 20 to report foreign travel and receive any pre-travel or post-travel briefings. The estimated average labor rate for a cleared employee to report foreign travel is the equivalent of a GS11 step 5. These assumptions imply costs increasing from $16.81 to $19.25 million in each year one through 20.

2. *Projected Public Costs.* Based on the re-evaluation of the cost of training cleared employees on foreign travel reporting and submissions, the estimated public costs are present value costs of $267.4 million, which includes the additional foreign travel reporting cost.

3. *Updated Baseline Cost.* With this increase for the foreign travel reporting, DoD's updated enterprise industrial security baseline cost is estimated not to exceed $1.753 billion ($1.486 billion plus $267.4 million).

Regulatory Analysis

Executive Order 12866, ''Regulatory Planning and Review'' and Executive Order 13563, ''Improving Regulation and Regulatory Review''

Executive Orders 12866 and 13563 direct agencies to assess all 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, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. It has been determined that this rule is a significant regulatory action. Accordingly, the rule has been reviewed by the Office of Management and Budget (OMB) under the requirements of these Executive Orders.

Congressional Review Act

This rule is not a ''major rule'' as defined by 5 U.S.C. 804(2).

Public Law 96–354, ''Regulatory Flexibility Act'' (5 U.S.C. Chapter 6)

The Under Secretary of Defense for Intelligence and Security, pursuant to a delegation of authority from the Secretary of Defense, certifies that this rule will not, if promulgated, have a significant economic impact on a substantial number of small business entities in accordance with the Regulatory Flexibility Act (5 U.S.C. 601) requirements since a contractor cleared legal entity may, in entering into contracts requiring access to classified information, negotiate for security costs determined to be properly chargeable by a Government Contracting Activity.

Public Law 96–511, ''Paperwork Reduction Act'' (44 U.S.C. Chapter 35)

Notwithstanding any other provision of law, no person is required to respond to, nor is subject to a penalty for failure to comply with, a collection of information, subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA), unless that collection of information displays a currently valid Office of Management and Budget (OMB) Control Number. This proposed rule involves collections previously approved by OMB under the following control numbers.

- OMB Control Number: 0704–0194, DD Form 441, Department of Defense Security Agreement
- OMB Control Number: 0704–0571, National Industrial Security System
- OMB Control Number: 0704–0567, DoD Contract Security Classification Specification
- OMB Control Number: 0704–0573, Defense Information System for Security (DISS)
- OMB Control Number: 0704–0579, Certificate Pertaining to Foreign Interests, SF 328
- OMB Control Number: 3150–0047, 10 CFR part 95, Facility Security Clearance and Safeguarding of National Security Information and Restricted Data
- OMB Control Number: 1910–1800, Security

DoD believes the total burden hours associated with these collections are not expected to change based on the amendments proposed in this rule. Information on the current version of these collections, including all supporting materials, can be obtained at *https://www.reginfo.gov/public/do/PRAMain* and typing in the OMB control number.

Section 202, Public Law 104–4, ''Unfunded Mandates Reform Act''

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) (2 U.S.C. 1532) requires agencies to assess anticipated costs and benefits before issuing any rule whose mandates require spending in any one year of $100 million in 1995 dollars, updated annually for inflation. This rule will not mandate any requirements for State, local, or tribal governments, nor will it affect private sector costs.

Executive Order 13132, ''Federalism''

E.O. 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications. This rule will not have a substantial effect on State and local governments.

Executive Order 13175, ''Consultation and Coordination With Indian Tribal Governments''

Executive Order 13175 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct compliance costs on one or more Indian tribes, preempts tribal law, or affects the distribution of power and responsibilities between the federal government and Indian tribes. This rule will not have a substantial effect on Indian tribal governments.

List of Subjects in 32 CFR Part 117

Classified information; Government contracts; USG contracts, National Industrial Security Program (NISP); Prime contractor, Subcontractor.

Accordingly, the Department of Defense proposes to amend 32 CFR part 117 as follows:

PART 117—NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM)

■ 1. The authority citation for part 117 continues to read as follows:

Authority: 32 CFR part 2004; E.O. 10865; E.O. 12333; E.O. 12829; E.O. 12866; E.O. 12968; E.O. 13526; E.O. 13563; E.O. 13587; E.O. 13691; Public Law 108–458; Title 42 U.S.C. 2011 *et seq.;* Title 50 U.S.C. Chapter 44; Title 50 U.S.C. 3501 *et seq.*

■ 2. Amend § 117.3 in paragraph (b) by adding in alphabetical order the definitions of ''Authorization to operate'' and ''Pedestrian door locks'' to read as follows:

§ 117.3 Acronyms and definitions.

* * * * *

(b) * * *

Authorization to operate means an approval granted by an authorizing official for a system to process classified information.

* * * * *

Pedestrian door locks means a series of GSA-approved (FF–L–2890C) preassembled locks designed, tested, and approved for security, fire safety, life safety, and accessibility when installed on doors located in the occupants anticipated path of travel to a means of egress to evacuate the facility in a fire emergency.

* * * * *

■ 3. Amend § 117.5 by revising paragraph (d) to read as follows:

§ 117.5 Information collections.

* * * * *

(d) *DoD collection.* ''DoD Security Agreement,'' is assigned OMB Control Number: 0704–0194. ''National Industrial Security System,'' a CSA information collection, is assigned OMB Control Number: 0704–0571, and is a DoD information collection used to conduct its monitoring and oversight of contractors. Department of Defense ''Contract Security Classification Specification,'' (available at: *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0254.pdf* and *https://www.dcsa.mil/is/nccs/),* is assigned OMB Control Number: 0704–0567 and used by both DoD and agencies which have an industrial security agreement with DoD. ''Defense Information System for Security,'' is assigned OMB Control Number: 0704–0573. Defense Information System for Security is a DoD automated system for personnel security, providing a common, comprehensive medium to record, document, and identify personnel security actions within DoD including submitting adverse information, verification of security clearance status, requesting investigations, and supporting continuous evaluation activities. It requires personal data collection to facilitate the initiation, investigation and adjudication of information relevant to DoD security clearances and employment suitability determinations for active duty military, civilian employees and contractors seeking such credentials.

* * * * *

■ 4. Amend § 117.7 by:

■ a. Revising paragraph (b) introductory text;

■ b. In paragraph (f) introductory text, removing the words ''official reviews'' and adding in their place the words ''security reviews'';

■ c. In paragraph (f)(2), adding the words ''for review'' after the word ''Providing''; and

■ d. Revising paragraphs (h)(1)(i) and (h)(1)(ii)(A).

The revisions read as follows:

§ 117.7 Procedures.

* * * * *

(b) *Contractor Security Officials.* Contractors will appoint security officials who are U.S. citizens, unless the provisions of § 117.11(e)(1)(iii) apply for the SMO and ITPSO.

* * * * *

(h) * * *

(1) * * *

(i) *Review cycle.* The CSA will determine the scope and frequency of security reviews, which may be increased or decreased consistent with risk management principles. Security reviews may be conducted not more often than once every 12 months unless special circumstances exist, to include addressing security vulnerabilities found during a previous security review.

(ii) * * *

(A) The CSA will generally provide notice to the contractor of a forthcoming review, but may also conduct unannounced reviews at its discretion, *e.g.,* if there is possible imminent loss or compromise of classified information. The CSA security review may subject contractor employees and all areas and receptacles under the control of the contractor to examination.

* * * * *

■ 5. Amend § 117.8 by revising paragraphs (a)(2)(ii), (c)(7)(iii)(B), and (c)(14) to read as follows:

§ 117.8 Reporting requirements.

(a) * * *

(2) * * *

(ii) Provide requested information to enable the CSA to ascertain whether classified information is adequately protected in accordance with this rule.

* * * * *

(c) * * *

(7) * * *

(iii) * * *

(B) Whether they have been excluded from access to classified information in accordance with § 117.7(c)(2).

* * * * *

(14) *Reporting by subcontractor.* Subcontractors will also notify their prime contractors if they make any reports to their CSA that affect the status of the entity eligibility determination (*e.g.,* FCL), may indicate an employee poses as an insider threat, affect the proper safeguarding of classified information, or indicate classified information has been lost or compromised.

* * * * *

■ 6. Amend § 117.9 by:

■ a. Revising paragraph (f); and

■ b. Redesignating paragraphs (h)(i) and (h)(ii) as paragraphs (h)(1) and (h)(2).

The revision reads as follows:

§ 117.9 Entity eligibility determination for access to classified information.

* * * * *

(f) *Exclusion procedures.* If a CSA determines that certain KMP can be excluded from access to classified information, the contractor will follow the procedures in accordance with § 117.7(c)(2).

* * * * *

■ 7. Amend § 117.11 by:

■ a. In paragraph (d)(2)(iii)(B)(*4*), removing the words ''SCI, RD, or COMSEC'' and adding in their place the words ''proscribed information''; and

■ b. Revising paragraph (h)(4).

The revision reads as follows:

§ 117.11 Foreign Ownership, Control, or Influence (FOCI).

* * * * *

(h) * * *

(4) *Facilities location plan.* When a contractor is potentially collocated with or in close proximity to its foreign parent or an affiliate, the contractor will provide a facilities location plan that identifies the physical locations of the contractor and its foreign parent(s) or affiliate(s) respectively. The facilities location plan will assist the CSA in determining if the contractor is collocated or if the close proximity can be allowed under the FOCI mitigation plan. A U.S. entity generally cannot be collocated with the foreign parent or affiliate, *i.e.,* at the same address or in the same location.

* * * * *

§ 117.12 [Amended]

■ 8. Amend § 117.12 in paragraph (k) by removing the words ''every 12 months'' and adding in their place the words ''at least annually''.

■ 9. Amend § 117.15 by:

■ a. Revising paragraph (a) introductory text;

■ b. Redesignating paragraphs (a)(2) and (a)(3) as paragraphs (a)(3) and (a)(4);

■ c. Adding new paragraph (a)(2);

■ d. In the newly redesignated paragraph (a)(3), revising the heading;

■ e. In the newly redesignated paragraph (a)(4), redesignating paragraphs (ii), (iii), and (iv) as paragraphs (iii), (iv), and (v);

■ f. In the newly redesignated paragraph (a)(4), adding a new paragraph (ii);

■ g. In the newly redesignated paragraph (a)(4)(iv)(B), adding the word ''effects'' after the word ''personal'';
■ h. Revising paragraph (c) introductory text;
■ i. Revising paragraph (d)(3)(i)(A);
■ j. Revising paragraph (e)(1)(ii) and paragraph (e)(2) introductory text;
■ k. Adding a new paragraph (e)(2)(viii); and
■ l. Revising paragraph (e)(6).

The revisions and additions read as follows:

§ 117.15 Safeguarding classified information.

(a) *General safeguarding.* Contractors will be responsible for safeguarding classified information in their custody or under their control, with approval for such storage of classified information by the applicable CSA. Individuals are responsible for safeguarding classified information entrusted to them. Contractors will provide the extent of protection to classified information in accordance with the provisions of this rule.

* * * * *

(2) *Restricted areas.* When it is necessary to control access to classified material and an open storage area is not available, a restricted area may be established. A restricted area will normally become necessary when it is impractical or impossible to protect classified material because of its size, quantity, or other unusual characteristic. The restricted area shall have a clearly defined perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate need-to-know for the information within the restricted area. All classified material will be secured during non-working hours in approved repositories, in accordance with the provisions of this rule, or secured using other methods approved by the CSA.

(3) *Security checks.* * * *

(4) * * *

(ii) During working hours when an open storage area is unattended, admittance to the area must be controlled by locked entrances and exits secured by GSA-approved pedestrian door locking hardware (FF–L–2890C), ''Federal Specification Lock Extension,'' or CSA approved deadbolts or emergency exit hardware on any secondary doors.

* * * * *

(c) *Storage.* Contractors will store classified information and material in General Services Administration (GSA)-approved security containers, vaults built to Federal Standard 832, or an open storage area constructed in accordance with 32 CFR 2001.53. The CSA may grant self-approval to the FSO for open storage area approvals, provided the FSO meets specified qualification criteria as determined by the CSA. In the instance that an open storage area has a false ceiling or raised floor, contractors shall develop and implement procedures to ensure their structural integrity in accordance with CSA provided guidance. Nothing in 32 CFR part 2001, should be construed to contradict or inhibit compliance with local laws or building codes, but the contractor will notify the applicable CSA if there are any conflicting issues that would inhibit compliance. Contractors will store classified material in accordance with the specific sections of 32 CFR 2001.43:

* * * * *

(d) * * *

(3) * * *

(i) * * *

(A) If after a thorough inspection of the facility perimeter with no damage to the facility visible, the alarm system resets and remains in the secure condition, then entrance into the area is not required and an initial response team may consist of uncleared personnel.

* * * * *

(e) * * *

(1) * * *

(ii) An information management system to protect and control the classified information in their possession regardless of media, to include information processed and stored on information systems with an authorization to operate by an applicable CSA, otherwise referred to as an authorized information system.

(2) *Top secret information.* Unless otherwise directed by the applicable CSA, the contractor will establish the following additional controls:

* * * * *

(viii) When TOP SECRET information and material is generated or stored on authorized information systems, contractors will establish controls for TOP SECRET information and material to validate procedures are in place to address accountability, need to know, and retention, *e.g.,* demonstrating that TOP SECRET material stored in an electronic format on an authorized information system does not need to be individually numbered in series. These controls are in addition to the information management system and must be applied, unless otherwise directed by the applicable CSA, regardless of the media of the TOP SECRET information, to include information processed and stored on authorized information systems.

* * * * *

(6) *Reproduction of classified information.* Contractors will reproduce paper copies, electronic files, and other material containing classified information only when necessary for accomplishing operational needs or for complying with contractual requirements. Use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

(i) Unless restricted by the GCA on behalf of the originating agency, TOP SECRET, SECRET, and CONFIDENTIAL information may be reproduced, including by emailing, scanning, and copying, to the extent operational needs require on authorized systems and equipment approved at the level of the classified material and in support of a contractual requirement.

(ii) Contractors shall establish procedures that facilitate oversight and control of the reproduction of classified information and the use of equipment for such reproduction, including controls that ensure:

(A) Reproduction is kept to a minimum consistent with contractual requirements.

(B) Contractor personnel reproducing classified information are knowledgeable of the procedures for classified reproduction and aware of the risks involved with the specific reproduction equipment being used and the appropriate countermeasures they are required to take.

(C) Reproduction limitations the GCA places on documents and special controls applicable to special categories of information are fully and carefully observed.

(D) Reproduced material is placed under the same accountability and control requirements as applied to the original material. Extracts of documents will be marked according to content and may be treated as working papers if appropriate.

(E) Reproduced material is conspicuously identified as classified at the applicable level and copies of classified material are reviewed after the reproduction process to ensure that the required markings exist.

(F) Waste products generated during reproduction are protected and destroyed as required.

* * * * *

■ 9. Amend § 117.17 by:
■ a. Revising paragraphs (a)(3) introductory text;
■ b. Removing paragraphs (a)(3)(i) through (iii); and

■ c. Redesignating paragraphs (a)(3)(iv) introductory text and (a)(3)(iv)(A) and (B) as paragraphs (a)(4) introductory text and (a)(4)(i) and (ii).

The revisions read as follows:

§ 117.17 Subcontracting.

(a) * * *

(1) * * *

(2) * * *

(3) *Lead time for entity eligibility determination when awarding to an uncleared subcontractor.* Requesting contractors will allow sufficient lead time in connection with the award of a classified subcontract to enable an uncleared bidder to be processed for the necessary entity eligibility determination.

* * * * *

§ 117.19 [Amended]

■ 10. Amend § 117.19 in paragraph (b)(5)(iv) by adding the words ''(*e.g.,* a security aspects letter)'' at the end of the paragraph.

Dated: December 6, 2023.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2023–27171 Filed 12–12–23; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 100

[Docket Number USCG–2023–0903]

RIN 1625–AA08

Special Local Regulations; Sector Ohio Valley Annual and Recurring Special Local Regulations

AGENCY: Coast Guard, Department of Homeland Security (DHS).

ACTION: Notice of proposed rulemaking.

SUMMARY: The Coast Guard proposes amending and updating its special local regulations for recurring marine parades, regattas, and other events that take place in the Coast Guard Sector Ohio Valley area of responsibility (AOR). This proposed rulemaking would update the current list of recurring special local regulations with revisions, additions, and removals of events that no longer take place in the Sector Ohio Valley AOR. We invite your comments on this proposed rulemaking.

DATES: Comments and related material must be received by the Coast Guard on or before January 12, 2024.

ADDRESSES: You may submit comments identified by docket number USCG–2023–0903 using the Federal Decision-Making Portal at *https://www.regulations.gov.* See the ''Public Participation and Request for Comments'' portion of the **SUPPLEMENTARY INFORMATION**. This notice of proposed rulemaking with its plain-language, 100-word-or-less proposed rule summary will be available in this same docket.

FOR FURTHER INFORMATION CONTACT: If you have questions about this proposed rulemaking, call or email Petty Officer Bryan Crane, Sector Ohio Valley, U.S. Coast Guard; telephone (502) 779–5334, email *SECOHV-WWM@uscg.mil.*

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

CFR Code of Federal Regulations
DHS Department of Homeland Security
FR Federal Register
NPRM Notice of proposed rulemaking
§ Section
U.S.C. United States Code

II. Background, Purpose, and Legal Basis

The Captain of the Port Sector Ohio Valley (COTP) proposes to update the current list of recurring special local regulations for events occurring within the Sector Ohio Valley area of responsibility within the Coast Guard's Eighth District. The list of events we seek to update is in Title 33 of the Code of Federal Regulations (CFR) section 100.801, Table 1 to § 100.801.

The Coast Guard will consider comments submitted on this proposed rule in determining if any additional revisions are needed to this regulatory section. Additionally, the public would be informed of these recurring events through local means and planned by the local communities.

The current list of annual and recurring special local regulations occurring in Sector Ohio Valley's AOR is published in 33 CFR 100.801, Table 1 titled ''Ohio Valley Annual and Reoccurring Marine Events.'' The most recent list was published on April 4, 2023 (87 FR 6026).

The Coast Guard's authority for establishing a special local regulation is contained in 46 U.S.C. 70041(a). The Coast Guard proposes to amend and update the special local regulations in 33 CFR 100.801, Table 1, to include the most up to date list of recurring special local regulations for events held on or around the navigable waters within Sector Ohio Valley's AOR. These events would include marine parades, boat races, swim events, and other marine related events. The current list under 33 CFR 100.801, Table 1, requires amendment to provide new information on existing special local regulations, add new special local regulations expected to recur annually or biannually, and to remove special local regulations that no longer occur. Issuing individual regulations for each new special local regulation, amendment, or removal of an existing special local regulation creates unnecessary administrative costs and burdens. This single proposed rulemaking will considerably reduce administrative overhead. It also provide the public with notice through publication in the **Federal Register** of all recurring special local regulations in the AOR.

III. Discussion of Proposed Rule

Part 100 of 33 CFR contains regulations describing regattas and marine parades conducted on U.S. navigable waters in order to ensure the safety of life in the regulated areas. Section 100.801 provides the regulations applicable to events taking place in the Eighth Coast Guard District and also provides a table listing each event and special local regulations. This section requires amendment from time to time to properly reflect the recurring special local regulations. This proposed rule would update section 100.801, Table 1 titled ''Ohio Valley Annual and Reoccurring Marine Events.''

This proposed rule would add 4 new recurring special local regulations to Table 1 of section 100.801 for Sector Ohio Valley, as follows:

Date	Event/sponsor	Sector Ohio Valley location (city, state)	Regulated area
2 Days—Saturday and Sunday before Memorial Day.	Powerboat Nationals—Point Marion	Point Marion, PA	Monongahela River, Miles 89–91 (Pennsylvania).
1 Day—One Weekend in June	Race on the Oyo	Racine, OH to Point Pleasant, WV.	Ohio River (Mile 242–265) Ohio.