Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996 (Subtitle E—Congressional Review Act)

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996, 5 U.S.C. 801 *et seq.,* requires the Department to comply with small entity requests for information and advice about compliance with statutes and regulations within the Department's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in **FOR FURTHER INFORMATION CONTACT** section, above. Persons can obtain further information regarding SBREFA on the Small Business Administration's web page at *https://www.sba.gov/advocacy.* This rule is not a major rule as defined by 5 U.S.C. 804 of the Congressional Review Act.

Paperwork Reduction Act

This rule imposes no information collection or recordkeeping requirements.

List of Subjects in 28 CFR Part 16

Administrative practices and procedures, Courts, Freedom of information, Privacy.

Pursuant to the authority vested in the Attorney General by 5 U.S.C. 552a and delegated to me by Attorney General Order 2940–2008, the Department of Justice amends 28 CFR part 16 as follows:

PART 16—PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

■ 1. The authority citation for part 16 continues to read as follows:

Authority: 5 U.S.C. 301, 552, 552a, 553; 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717.

Subpart E—Exemption of Records Systems Under the Privacy Act

■ 2. Add § 16.138 to read as follows:

§ 16.138 Exemption of the Department of Justice Information Technology, Information System, and Network Activity and Access Records, JUSTICE/DOJ–002.

(a) The Department of Justice Information Technology, Information System, and Network Activity and Access Records (JUSTICE/DOJ–002) system of records is exempted from subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1), (e)(4)(G), (H), and (I); and (f) of the Privacy Act of 1974, as amended. The exemptions in this paragraph (a) apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1) or (k)(2). The applicable exemption may be waived by the DOJ in its sole discretion where DOJ determines compliance with the exempted provisions of the Act would not interfere with or adversely affect the purpose of this system of records to ensure that the Department can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and DOJ information systems.

(b) Exemptions from the particular subsections listed in paragraph (a) of this section are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system of records is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures of records concerning the subject would specifically reveal investigative interests in the records by the DOJ or other entities that are recipients of the disclosures. Revealing this information could compromise sensitive information classified in the interest of national security, or interfere with the overall law enforcement process by revealing a pending sensitive cybersecurity investigation. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to impede the investigation, *e.g.,* destroy evidence or alter techniques to evade discovery.

(2) From subsection (d)(1), (2), (3) and (4), (e)(4)(G) and (H), and (f) because these provisions concern individual access to and amendment of records, compliance with which regarding certain law enforcement and classified records could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the DOJ and/or other law enforcement or intelligence agencies. Providing access could compromise information classified to protect national security, or reveal sensitive cybersecurity investigative techniques; provide information that would allow a subject to avoid detection; or constitute a potential danger to the health or safety of law enforcement personnel or confidential sources.

(3) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. The relevance and utility of certain information that may have a nexus to cybersecurity threats may not always be fully evident until and unless it is vetted and matched with other information lawfully maintained by the DOJ or other entities.

(4) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the **Federal Register**. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information. Further, greater specificity of sources of properly classified records could compromise national security.

Dated: October 26, 2021.

Peter A. Winn,

Acting Chief Privacy and Civil Liberties Officer, United States Department of Justice.

[FR Doc. 2021–24315 Filed 11–5–21; 8:45 am]

BILLING CODE 4410–NW–P

DEPARTMENT OF JUSTICE

28 CFR Part 16

[CPCLO Order No. 011–2021]

Privacy Act of 1974; Implementation

AGENCY: Justice Management Division, United States Department of Justice.

ACTION: Final rule.

SUMMARY: The United States Department of Justice (DOJ or Department) is finalizing without changes its Privacy Act exemption regulations for the system of records titled, Security Monitoring and Analytics Service Records, JUSTICE/JMD–026, which were published as a notice of proposed rulemaking (NPRM) on July 30, 3021. Specifically, the Department's regulations will exempt the records maintained in JUSTICE/JMD–026 from one or more provisions of the Privacy Act. The exemptions are necessary to avoid interference with efforts to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of information, information systems, and networks of DOJ and external Federal agency subscribers. The Department received two comments on the NPRM, neither of which impact the Department's decision to proceed with issuing this final rule.

DATES: This final rule is effective December 8, 2021.

FOR FURTHER INFORMATION CONTACT: Nickolous Ward, DOJ Chief Information Security Officer, (202) 514–3101, 145 N Street NE, Washington, DC 20530.

SUPPLEMENTARY INFORMATION: In accordance with the Federal Information Security Modernization Act of 2014, among other authorities, agencies are responsible for complying with information security policies and procedures requiring information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. *See, e.g.,* 44 U.S.C. 3554 (2018). Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017), directs agency heads to show preference in their procurement for shared information technology (IT) services, to the extent permitted by law, including email, cloud, and cybersecurity services. Office of Management and Budget (OMB) Memorandum M–19–16, Centralized Mission Support Capabilities for the Federal Government (April 26, 2019), establishes the framework for implementing the ''Sharing Quality Services'' across agencies. The Economy Act of 1932, as amended, 31 U.S.C. 1535, authorizes agencies to enter into agreements to obtain supplies or services from another agency. Consistent with these authorities, the Justice Management Division (JMD), Office of the Chief Information Officer (OCIO), Cybersecurity Services Staff (CSS), developed the Security Monitoring and Analytics Service (SMAS) system to provide DOJ-managed information technology service offerings to other Federal agencies wishing to leverage DOJ's cybersecurity services, referred to as ''external federal agency subscribers.'' This system provides external Federal agency subscribers with the technical capability to protect their data from malicious or accidental threats using a DOJ-managed system. In the **Federal Register** of July 30, 2021 (86 FR 41089), JMD published a notice of a new system of records titled, ''Security Monitoring and Analytics Service Records,'' JUSTICE/JMD–026, to provide the public notice of the records maintained by DOJ while implementing SMAS.

In this rulemaking, the Department exempts JUSTICE/JMD–026 from certain provisions of the Privacy Act in order to avoid interference with the responsibilities of the Department to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of external Federal agency subscribers' information and information systems. Additionally, the Department exempts JUSTICE/JMD–026 from certain provisions to assist DOJ and external Federal agency subscribers with protecting such data and ensuring the secure operation of information systems.

The Department received two anonymous comments during the notice-and-comment period. One comment expressed general support for the Department's work to address cybersecurity threats to the government through the implementation of JUSTICE/JMD–026. The second comment broadly questioned whether the proposed exemption would impact in any way the public's ability to access information maintained in the system of records or otherwise reduce the level of transparency required to maintain the public's trust in the Department. As noted in the rule, any restrictions on individual access are based on an articulated need to protect sensitive or law enforcement information. The Privacy Act was drafted to allow agencies to appropriately restrict the public's access to records maintained in a system of records when doing so could potentially reveal sensitive or law enforcement information. When working to ensure cybersecurity, the Department must balance the needs of ensuring transparency and public access with a duty to protect sensitive or law enforcement information that may reveal sources and methods or otherwise compromise law enforcement equities. Accordingly, the Department is proceeding with issuing this final rule without change.

In reviewing the proposed rule (86 FR 40972, July 30, 2021) for publication, the Department identified a minor typographical error in the name and number of the identified system of records proposed to be exempted. Additionally, the proposed rule indicated in one place an exemption from subsection (d), and in another place an exemption from subsections (d)(1)–(4). In an effort to reduce potential confusion, the language in the final rule has been modified to consistently identify the system of records as being exempted from subsections (d)(1)–(4). Further, corrections have been inserted in the final rule in multiple places where the proposed rule had used the term ''system,'' although ''system of records'' was clearly intended. Finally, the proposed rule stated that, in determining the relevance and utility of certain exempted information, it would be vetted and matched with other information necessarily and lawfully maintained by the DOJ, external Federal agency subscribers, or other entities. Such information need only be maintained lawfully by the DOJ, external Federal agency subscribers, or other entities for use in the vetting and matching described. The Department has determined that these changes do not significantly alter the efficacy of the notice that was provided to the public. The Department has made the adjustments in the final rule, which is published herein.

Executive Orders 12866 and 13563–Regulatory Review

In accordance with 5 U.S.C. 552a(j) and 552a(k), this regulation is subject to formal rulemaking procedures by giving interested persons an opportunity to participate in the rulemaking process ''through submission of written data, views, or arguments,'' pursuant to 5 U.S.C. 553. This regulation will promulgate certain Privacy Act exemptions for a DOJ system of records titled, ''Security Monitoring and Analytics Service Records,'' JUSTICE/JMD–026. This regulation does not raise novel legal or policy issues, nor does it adversely affect the economy, the budgetary impact of entitlements, grants, user fees, loan programs, or the rights and obligations of recipients thereof in a material way. The Department of Justice has determined that this rule is not a ''significant regulatory action'' under Executive Order 12866, section 3(f), and accordingly this rule has not been reviewed by the Office of Information and Regulatory Affairs within the Office of Management and Budget pursuant to Executive Order 12866.

Regulatory Flexibility Act

This regulation will only impact Privacy Act-protected records, which are personal and generally do not apply to an individual's entrepreneurial capacity, subject to limited exceptions. Accordingly, the Chief Privacy and Civil Liberties Officer, in accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), has reviewed this regulation and by approving it certifies that this regulation will not have a significant economic impact on a substantial number of small entities.

Small Business Regulatory Enforcement Fairness Act of 1996 (Subtitle E—Congressional Review Act)

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996, 5 U.S.C. 801 *et seq.,* requires the Department to comply with small entity requests for information and advice

about compliance with statutes and regulations within the Department's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in **FOR FURTHER INFORMATION CONTACT** section, above. Persons can obtain further information regarding SBREFA on the Small Business Administration's web page at *https://www.sba.gov/advocacy.* This regulation is not a major rule as defined by 5 U.S.C. 804 of the Congressional Review Act.

Executive Order 13132—Federalism

This regulation will not have substantial direct effects on the States, on the relationship between the National Government and the States, or on distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this rule does not have sufficient federalism implications to warrant the preparation of a Federalism Assessment.

Executive Order 12988—Civil Justice Reform

This regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate drafting errors and ambiguity, minimize litigation, provide a clear legal standard for affected conduct, and promote simplification and burden reduction.

Executive Order 13175—Consultation and Coordination With Indian Tribal Governments

This regulation will have no implications for Indian Tribal governments. More specifically, it does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes. Therefore, the consultation requirements of Executive Order 13175 do not apply.

Unfunded Mandates Reform Act of 1995

This regulation will not result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100,000,000, as adjusted for inflation, or more in any one year, and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Congressional Review Act

This rule is not a major rule as defined by 5 U.S.C. 804 of the Congressional Review Act.

Paperwork Reduction Act

This rule imposes no information collection or recordkeeping requirements.

List of Subjects in 28 CFR Part 16

Administrative practices and procedures, Courts, Freedom of information, Privacy.

Pursuant to the authority vested in the Attorney General by 5 U.S.C. 552a and delegated to me by Attorney General Order 2940–2008, the Department of Justice amends 28 CFR part 16 as follows:

PART 16—PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

■ 1. The authority citation for part 16 continues to read as follows:

Authority: 5 U.S.C. 301, 552, 552a, 553; 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717.

Subpart E—Exemption of Records Systems Under the Privacy Act

■ 2. Amend § 16.76 by adding paragraphs (e) and (f) to read as follows:

§ 16.76 Exemption of Justice Management Division.

* * * * *

(e) The following system of records is exempted from 5 U.S.C. 552a(c)(3); (d)(1)–(4); (e)(1), (e)(4)(G), (H), and (I); and (f): Department of Justice Security Monitoring and Analytics Service Records (JUSTICE/JMD–026). The exemptions in this paragraph (e) apply only to the extent that information in this system of records is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Where DOJ determines compliance would not appear to interfere with or adversely affect the purpose of this system of records to ensure that the Department can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems, the applicable exemption may be waived by the DOJ in its sole discretion.

(f) Exemptions from the particular subsections listed in paragraph (e) of this section are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system of records is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures of records concerning the subject would specifically reveal investigative interests in the records by the DOJ, external Federal agency subscribers, or other entities that are recipients of the disclosures. Revealing this information could compromise sensitive information or interfere with the overall law enforcement process by revealing a pending sensitive cybersecurity investigation. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to impede the investigation, *e.g.,* destroy evidence or alter techniques to evade discovery.

(2) From subsection (d)(1), (2), (3) and (4), (e)(4)(G) and (H), and (f) because these provisions concern individual access to and amendment of certain law enforcement and sensitive records, compliance of which could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the DOJ, external Federal agency subscribers, and/or other entities that are recipients of the disclosure. Providing access could compromise sensitive information or reveal sensitive cybersecurity investigative techniques; provide information that would allow a subject to avoid detection; or constitute a potential danger to the health or safety of law enforcement personnel or confidential sources.

(3) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes. The relevance and utility of certain information that may have a nexus to cybersecurity threats may not always be fully evident until and unless it is vetted and matched with other information lawfully maintained by the DOJ, external Federal agency subscribers, or other entities.

(4) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system of records than has been published in the **Federal Register**. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement information.

Dated: October 26, 2021.

Peter A. Winn,

Acting Chief Privacy and Civil Liberties Officer, United States Department of Justice.

[FR Doc. 2021–24316 Filed 11–5–21; 8:45 am]

BILLING CODE 4410–NW–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 100

[Docket Number USCG–2020–0332]

RIN 1625–AA08

Special Local Regulations; Recurring Marine Events Within the Fifth Coast Guard District

AGENCY: Coast Guard, DHS.

ACTION: Final rule.

SUMMARY: The Coast Guard is amending its special local regulations established for recurring marine events that take place within the Fifth Coast Guard District area of responsibility. The Coast Guard has periodically updated this regulation to account for changes in these marine events. Through this final rule, the current list of recurring marine events requiring special local regulations is updated with revisions, additional events, and the removal of events that no longer take place in the Fifth Coast Guard District area of responsibility. When these special local regulations are enforced, certain restrictions are placed on marine traffic in specified areas to promote safety on the water around marine events.

DATES: This rule is effective December 8, 2021.

ADDRESSES: To view documents mentioned in this preamble as being available in the docket, go to *https://www.regulations.gov,* type USCG–2020–0332 in the ''SEARCH'' box and click ''SEARCH.'' Click on Open Docket Folder on the line associated with this rule.

FOR FURTHER INFORMATION CONTACT: If you have questions on this rule, call or email Mr. Ethan Coble, Fifth Coast Guard District Office of Waterways Management, U.S. Coast Guard; telephone (757) 398–7745, email *Ethan.J.Coble@uscg.mil.*

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

APA Administrative Procedure Act
CFR Code of Federal Regulations
COTP Captain of the Port
DHS Department of Homeland Security
FR Federal Register
MFR Memorandum for Record
NPRM Notice of proposed rulemaking
PATCOM Patrol Commander
§ Section
U.S.C. United States Code

II. Background Information and Regulatory History

The Coast Guard regularly updates the regulations for recurring special local regulations within the Fifth Coast Guard District listed in 33 CFR 100.501, and its respective tables. These recurring special local regulations are for marine events that take place either on or over the navigable waters of the Fifth Coast Guard District as defined at 33 CFR 3.25. These regulations were last amended June 13, 2017 (81 FR 81005). Since then, Marine Events within the Fifth US Coast Guard District have been newly created or changed in a way that varies from their description in this regulation. In response, on June 03, 2021, the Coast Guard published a notice of proposed rulemaking (NPRM) titled Special Local Regulations; Recurring Marine Events and within the Fifth Coast Guard District (86 FR 29711). There we stated why we issued the NPRM, and invited comments on our proposed regulatory action related to special local regulations and recurring marine events. The comment period ended on July 6, 2021, and we received no comments.

III. Legal Authority and Need for Rule

The Coast Guard is issuing this rule under authority in 46 U.S.C. 70041. The Secretary has delegated ports and waterways authority, with certain reservations not applicable here, to the Commandant via DHS Delegation No. 00170.1(II)(70), Revision No. 01.2. The Commandant has further delegated these authorities within the Coast Guard as described in 33 CFR 1.05–1 and 6.04–6. The Coast Guard has determined that the events listed in this rule could pose a risk to participants or waterway users if normal vessel traffic were to interfere with the event. Possible hazards include risks of participant injury or death resulting from near or actual contact with non-participant vessels traversing through the regulated areas. In order to protect the safety of all waterway users, including event participants and spectators, this rule establishes special local regulations for the time and location of each marine event. This rule prevents vessels from entering, transiting, mooring or anchoring within areas specifically designated as regulated areas during the periods of enforcement, unless authorized by the Captain of the Port (COTP), or designated Event Patrol Commander.

IV. Discussion of Comments, Changes, and the Rule

As noted above, we received no comments on our NPRM published June 3, 2021. We made no changes to the regulatory text as it was proposed in our NPRM. The following discussion explains the changes made to the CFR by this rule.

A. Changes To Improve Clarity and Reflect Current Coast Guard Marine Event Policies

We have made several stylistic and formatting changes to update 33 CFR 100.501, and associated tables, to provide greater clarity and remove potential ambiguities. We have also made revisions to reflect current Coast Guard marine event policy. The following is a summary of changes from the current regulatory text:

- Plain language edits, such as switching from passive to active voice and more clearly stating the enforcement period for each event.
- Writing regulatory requirements and definitions in the singular rather than the plural, where appropriate.
- Listing definitions and the events by COTP Zone in alphabetical order.
- Reformatting the table entries so they all are similar.
- Separating the special local regulations for each COTP Zone into their own tables.
- Amending the name and location for Sector Virginia to Portsmouth, VA (where the command center is located), and updating the phone number for Sector North Carolina.

Additionally, we consolidated all defined terms into a single paragraph, 33 CFR 100.501(b), and listed them in alphabetical order. Currently the defined terms ''buffer area'', ''race area'', and ''spectator area'' appear in the regulatory requirements paragraph 33 CFR 100.5014(c) rather than with the definitions. These definitions have been moved to the definition section and put into alphabetical order. Regulatory requirements for these areas will remain in the regulatory requirements portion of the regulation.

We changed the defined term of ''buffer area'' to ''buffer zone'' to comport with the more common usage. The definition is revised to reflect that it may sometimes be appropriate to utilize a buffer zone at the event if there is not a spectator area within the regulated area.

We changed the defined term ''Coast Guard Patrol Commander'' to ''Event Patrol Commander or Event PATCOM'' in alignment with updated local policy. The underlying associated definition