public comment on August 6, 2021, but no later than February 16, 2022.

ADDRESSES: Written comments must be submitted electronically, following the instructions provided on the website. All comments submitted will be posted on the website and available to the public.

Remote public hearings via video or telephone conference are scheduled on the proposed amendments as follows:

- Appellate Rules on January 14, 2022 and January 28, 2022;
- Bankruptcy Rules on January 7, 2022 and January 28, 2022;
- Civil Rules on January 6, 2022 and February 4, 2022;
- Criminal Rules on November 8, 2021 and January 11, 2022; and
- Evidence Rules on January 21, 2022.

Those wishing to testify must contact the Secretary of the Committee on Rules of Practice and Procedure by email at: *RulesCommittee_Secretary@ao.uscourts.gov,* at least 30 days before the hearing.

FOR FURTHER INFORMATION CONTACT: Scott Myers, Esq., Acting Chief Counsel, Rules Committee Staff, Administrative Office of the U.S. Courts, Thurgood Marshall Federal Judiciary Building, One Columbus Circle NE, Suite 7–300, Washington, DC 20544, Phone (202) 502–1820, *RulesCommittee_Secretary@ao.uscourts.gov.*

SUPPLEMENTARY INFORMATION: The Advisory Committees on Appellate, Bankruptcy, Civil, Criminal, and Evidence Rules have proposed amendments to the following rules:

Appellate Rules: 2 and 4.

Bankruptcy Rules: Restyled Rules Parts III–VI; Rules 3002.1, 3011, and 8003; new Rule 9038; Official Forms 101, 309E1, 309E2, and 417A; and new Official Forms 410C13–1N, 410C13–1R, 410C13–10C, 410C13–10NC, and 410C13–10R.

Civil Rules: 15, 72, and new Rule 87.

Criminal Rules: New Rule 62.

Evidence Rules: 106, 615, and 702.

The text of the proposed rules and the accompanying committee notes, along with the related forms, will be posted by August 6, 2021, on the Judiciary's website at: *http://www.uscourts.gov/rules-policies/proposed-amendments-published-public-comment.*

(Authority: 28 U.S.C. 2073.)

Dated: July 27, 2021.

Shelly L. Cox,

Management Analyst, Rules Committee Staff.

[FR Doc. 2021–16319 Filed 7–29–21; 8:45 am]

BILLING CODE 2210–55–P

DEPARTMENT OF JUSTICE

Bureau of Alcohol, Tobacco, Firearms and Explosives

[OMB Number 1140–0024]

Agency Information Collection Activities; Proposed eCollection of eComments Requested; Revision of a Currently Approved Collection; Report of Firearms Transactions—Demand 2—ATF Form 5300.5

AGENCY: Bureau of Alcohol, Tobacco, Firearms and Explosives, Department of Justice.

ACTION: 60-Day notice.

SUMMARY: The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Department of Justice (DOJ), will submit the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995. The proposed information collection OMB 1140–0024 (Report of Firearms Transactions—Demand 2—ATF Form 5300.5) is being renamed (Demand 2 Program: Report of Firearms Transactions—ATF Form 5300.5), to clearly identify the firearms transactions affected by this collection. There is also an increase in the total annual respondents, responses, and burden hours. The proposed (IC) is also being published to obtain comments from the public and affected agencies.

DATES: Comments are encouraged and will be accepted for 60 days until September 28, 2021.

FOR FURTHER INFORMATION CONTACT: If you have additional comments, regarding the estimated public burden or associated response time, suggestions, or need a copy of the proposed information collection instrument with instructions, or additional information, please contact: Neil Troppman, Law Enforcement Support Branch, National Tracing Center Division either by mail at 244 Needy Road, Martinsburg, WV 25405, by email at *neil.troppman@atf.gov,* or by telephone at 304–260–3643.

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

—Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

—Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

—Evaluate whether and if so how the quality, utility, and clarity of the information to be collected can be enhanced; and

—Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses.

Overview of this information collection:

1. *Type of Information Collection (check justification or form 83):* Revision of a currently approved collection.

2. *The Title of the Form/Collection:* Report of Firearms Transactions—Demand 2.

3. *The agency form number, if any, and the applicable component of the Department sponsoring the collection:*

Form number (if applicable): ATF Form 5300.5.

Component: Bureau of Alcohol, Tobacco, Firearms and Explosives, U.S. Department of Justice.

4. *Affected public who will be asked or required to respond, as well as a brief abstract:*

Primary: Business or other for profit.

Other (if applicable): None.

Abstract: The Demand 2 Program requires Federal Firearm Licensees (FFLs) with 25 or more traces with a time to crime of three years or less in a calendar year, to submit an annual Report of Firearms Transactions—Demand 2—ATF Form 5300.5, followed by quarterly reports of used firearms acquired by the FFL.

5. *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* An estimated 628 respondents will use the form approximately four times annually, and it will take each respondent approximately 30 minutes to complete their responses.

6. *An estimate of the total public burden (in hours) associated with the collection:* The estimated annual public burden associated with this collection is 1,256 hours, which is equal to 628 (# of respondents) * 4 (# of responses per respondent) * .5 (30 minutes).

7. *An Explanation of the Change in Estimates:* Due to an increase in the

number of FFLs subject to the reporting requirements of the Demand 2 program, the total respondents, responses, and burden hours for this collection have increased by 233, 932, and 466 respectively, since the last renewal in 2018.

If additional information is required contact: Melody Braswell, Department Clearance Officer, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Two Constitution Square, 145 N Street NE, 3E.405A, Washington, DC 20530.

Dated: July 27, 2021.

Melody Braswell,

Department Clearance Officer for PRA, U.S. Department of Justice.

[FR Doc. 2021–16317 Filed 7–29–21; 8:45 am]

BILLING CODE 4410–FY–P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 007–2021]

Privacy Act of 1974; Systems of Records

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

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A–108, notice is hereby given that the Justice Management Division (JMD), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records titled Security Monitoring and Analytics Service Records, JUSTICE/JMD–026. JMD proposes to establish this system of records to provide external federal agency subscribers with the technical capability to protect their data from malicious or accidental threats using DOJ-managed systems.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by August 30, 2021.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments: By mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, 145 N St. NE, Suite 8W.300, Washington, DC 20530; by facsimile at 202–307–0693; or by email at *privacy.compliance@usdoj.gov.* To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

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 agency information and information systems. *See, e.g.,* 44 U.S.C. 3554 (2018). Executive Order No. 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 ''Sharing Quality Services'' across agencies. The Economy Act of 1932; 31 U.S.C. 1535, authorizes agencies to enter into agreements to obtain supplies or services from another agency.

Consistent with these authorities, the 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 IT service offerings to other federal agencies wishing to leverage DOJ's cybersecurity services, referred to as ''external federal agency subscribers.'' SMAS has a suite of technology products, which consists of a range of commercial off-the-shelf (COTS) software that provide insight into the subscribers' operating environment. SMAS capabilities include, but are not limited to, asset discovery, vulnerability assessment, Network Intrusion Detection System (NIDS), Endpoint Detection and Response (EDR), and Security Information and Event Management (SIEM) event correlation and log management. SMAS also offers User Behavior Analytics (UBA) and User Activity Monitoring (UAM) tools to correlate security events, as part of the service offering. SMAS enables the identification and evaluation of suspicious, unauthorized, or anomalous activity that may indicate malicious behavior and activity. DOJ provides this information directly to external federal agency subscribers for review and further evaluation. JMD monitors user activities and captures and stores files that might be related to suspicious, unauthorized, or anomalous activities. JMD ensures that possible security events or incidents are accurately identified, analyzed, guarded against, investigated, and shared with the external federal agency subscriber via secure means of communication (*e.g.,* encrypted email).

JMD established the system of records, Security Monitoring and Analytics Service Records, JUSTICE/JMD–026, to cover records maintained by JMD while utilizing SMAS for its external federal agency subscribers. Specifically, JMD tracks external federal agency subscriber's IT, information system, and/or network activity, including any access by users to any IT, information systems, and/or networks, whether authorized or unauthorized. Consistent with these requirements, JMD must ensure that it maintains accurate audit and activity records of the observable occurrences on external federal agency subscriber information systems and networks (also referred to as ''events'') that are significant and relevant to the security of the external federal agency subscriber's information and information systems. These audit and activity records may include, but are not limited to, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. These records assist DOJ and external federal agency subscribers with protecting subscribers' data and ensuring the secure operation of IT, information systems, and networks.

Additionally, monitored events—whether detected utilizing information systems maintaining audit and activity records, reported to the Department or external federal agency subscriber by information system users, or reported to the Department or the external federal agency subscriber by the cybersecurity research community or members of the general public conducting good faith vulnerability discovery activities—may constitute occurrences that (1) actually or imminently jeopardize, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitute a violation or imminent threat of violation of law, security