Billing Code: 4410-02-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 010-2017]

Privacy Act of 1974; System of Records

AGENCY: United States Department of Justice, Federal Bureau of Investigation.

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 Federal Bureau of Investigation (FBI), a component within the United States Department of Justice (Department or DOJ), proposes to establish a new system of records titled, "FBI Online Collaboration Systems," JUSTICE/FBI-004. This system of records will cover all FBI online collaboration systems that facilitate online collaboration between the FBI and its criminal justice, intelligence, national security, emergency management, public safety, and private sector partners, as well as to support internal collaboration for and external collaboration among such partners in the United States and approved countries worldwide. Expanding available collaboration tools of the FBI and its partners enables the FBI to carry out its national security and criminal justice missions. Elsewhere in this Federal Register, DOJ is concurrently issuing a Notice of Proposed Rulemaking to exempt JUSITCE/DOJ-004 from certain provisions of the Privacy Act.

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 [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The public, OMB, and Congress are invited to submit any comments: by mail to the Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, National Place Building, 1331 Pennsylvania Avenue, NW., Suite 1000, Washington, DC 20530-0001; 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: Katherine M. Bond, Assistant General Counsel, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001; telephone (202) 324-3000.

SUPPLEMENTARY INFORMATION: In an effort to carry out its national security and criminal law enforcement responsibilities, and to more robustly collaborate with its partners in the criminal justice system, intelligence communities, emergency management personnel and first responders, military personnel, governmental agencies associated with critical infrastructure protection of the United States, and private sector entities that provide critical information regarding criminal justice and national security matters to the FBI and law enforcement, the FBI has created online collaboration systems to provide user-driven, real-time, collaboration and communication tools designed to facilitate the exchange of information within, between, and among partners more expeditiously. The FBI's online collaboration systems will promote communication and information sharing for federal, state, local, tribal, territorial, foreign, and international

criminal justice agencies; emergency management personnel and first responders; as well as military and other government personnel involved in criminal justice and national security matters, by allowing the FBI and its partners to communicate with experts, create and join communities of common interest, create blogs to present ideas and receive feedback, share files with colleagues, exchange ideas through online forums, enhance situational awareness, and facilitate incident management. The online collaboration systems will also allow individuals and private sector entities to easily and quickly submit information to and collaborate with the FBI and other law enforcement and intelligence agencies regarding criminal justice and national security matters. By providing online communication platforms such as JusticeConnect and collaboration tools such as Special Interest Groups and Virtual Command Centers, and providing and maintaining a secure communications network, the FBI will increase collaboration and cooperation between and among its partners.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and the Congress on this new system of records.

Dated: November 28, 2017.

Peter A. Winn,

Acting Chief Privacy and Civil Liberties Officer,

United States Department of Justice.

SYSTEM NAME AND NUMBER:

FBI Online Collaboration Systems, JUSTICE/FBI-004.

SECURITY CLASSIFICATION:

This system contains Unclassified information.

SYSTEM LOCATION:

Records may be maintained at all locations at which the FBI operates or at which FBI operations are supported, including: J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001; FBI Academy and FBI Laboratory, Quantico, VA 22135; FBI Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Road, Clarksburg, WV 26306; FBI Records Management Division, 170 Marcel Drive, Winchester, VA 22602-4843; and FBI field offices, legal attaches, information technology centers, and other components listed on the FBI's Internet Web site, *https://www.fbi.gov*. Some or all system information may also be duplicated at other locations where the FBI has granted direct access for support of FBI missions, for purposes of system backup, emergency preparedness, and/or continuity of operations.

SYSTEMS MANAGER(S):

Director, Federal Bureau of Investigation, J. Edgar Hoover FBI Building, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. Chapter 33; 42 U.S.C. 3771; 28 U.S.C. 534; 44 U.S.C. 3101, 3301; 5 U.S.C. 301; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551–3558 *et seq.*; 28 CFR 0.85; and 28 CFR part 20.

PURPOSE(S) OF THE SYSTEM:

The purpose of the FBI's Online Collaboration Systems is to facilitate and support internal and external collaboration for and among the FBI, federal, state, local, tribal, territorial, foreign, and international criminal justice agencies, emergency management personnel and first responders, private sector entities, and United States military and other government personnel involved in criminal justice and national security matters in the United States and approved countries worldwide. Expanding the available collaboration tools of the FBI and its partners enables the FBI to carry out its national security and criminal justice missions by providing a real-time online environment for criminal justice agencies, the FBI, and its partners to exchange information internally and externally.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The following categories of individuals are covered by this system:

A. Individuals who are employees, contractors, detailees, assignees, or interns of the FBI, criminal justice agencies, intelligence agencies, the military, other governmental agencies associated with infrastructure protection of the United States, emergency management agencies or first responders organizations, foreign or international law enforcement agencies, and private sector entities, who are

authorized to communicate with or on behalf of the FBI via an FBI online collaboration system;

B. Individuals identified in data maintained in FBI or criminal justice or intelligence agencies' files; or whose information is obtained by the FBI or its partners by authority of law or agreement from other federal, state, local, tribal, territorial, or foreign government, or international agencies to further authorized information sharing purposes carrying out criminal justice, national security, emergency management, or public safety purposes, including the FBI's mission to protect and defend the United States against terrorist and foreign intelligence threats. These individuals may consist of the following: convicted offenders, subjects, suspects, wanted persons, victims, witnesses, missing persons, complainants, informants, sources, bystanders, law enforcement personnel, intelligence personnel, other responders, private sector liaison contacts, administrative personnel, consultants, relatives, and associates who may be relevant to investigation or intelligence operations;

C. Individuals who are identified in publicly available information, commercial databases, or private entity records and who are associated, related, or have a nexus to the criminal justice system or the FBI's missions; and

D. System users or other individuals accessing this system whose information is collected and maintained for this system's user auditing and security purposes.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may include biographical information about individuals who are employees, contractors, detailees, assignees, or interns of the FBI, criminal justice agencies, or other FBI partners as outlined above who are authorized to access an FBI online collaboration system. Biographical information may include name, phone number, email address, organization, photographs, citizenship, designation as a law enforcement officer with arresting powers, user login identification, and other information users choose to share within the collaboration system.

Records are unclassified and may contain information collected by the FBI, criminal justice or intelligence agencies, or other FBI partners for the performance of their legally authorized, required functions; investigative and/or intelligence information provided by the FBI or criminal justice agencies; or publicly available information or information from commercial databases about individuals who are associated, related, or have a nexus to the criminal justice system or the FBI's missions. These records may include biographical information (such as name, alias, race, sex, date of birth, place of birth, social security number, passport number, driver's license number, other unique personal identifier, addresses, telephone numbers, physical descriptions, and photographs); biometric information (such as fingerprints); financial information (such as bank account numbers); locations, actions, and activities; associates and affiliations; employment and business information; citizenship; visa and immigration information; travel information; and criminal and investigative history, and other data that may assist the FBI, criminal justice agencies, and other FBI partners in fulfilling their criminal justice, national security, emergency management, or public safety objectives.

Records may also contain information collected and compiled to maintain an audit trail of the activity of authorized users of the system, such as user name and user login identification.

RECORD SOURCE CATEGORIES:

Information is provided by Federal, state, local, tribal, territorial, and foreign government agencies; international agencies; agencies of the U.S. foreign intelligence community and military community; publicly available information, such as broadcast and print media; commercial databases; and individuals, corporations, and organizations.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b), the records or information in this system may be disclosed as a routine use, under 5 U.S.C. 552a(b)(3), in accordance with the blanket routine uses established for FBI record systems. See Blanket Routine Uses (BRU) Applicable to More Than One FBI Privacy Act System of Records, Justice/FBI–BRU, published at 66 FR 33558 (June 22, 2001) and amended at 70 FR 7513 (February 14, 2005) and 82 FR 24147 (May 25, 2017) or as may be updated in the future. In addition, as routine uses specific to this system, the FBI may disclose relevant records to the following persons or entities and under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which the information was collected:

A. To authorized users of an FBI online collaboration system, as necessary, to facilitate and support internal and external collaboration for and among the

FBI and its partners for the performance of their legally authorized, required functions.

B. To any person, organization, or governmental entity in order to notify them of a potential terrorist threat for the purpose of guarding against or responding to such threat.

C. To a governmental entity lawfully engaged in collecting law enforcement, emergency management, public safety, or national security information, or intelligence for such purposes when determined to be relevant by the FBI/DOJ.

D. To any agency of a foreign government or international agency or entity where the FBI determines that the information is relevant to the recipient's responsibilities, dissemination serves the best interests of the U.S. Government, and where the purpose in making the disclosure is compatible with the purpose for which the information was collected.

E. To any non-governmental entity, including commercial entities, or nonprofit organizations, that are joint participants with or provide support to the FBI and disclosure is consistent with the FBI's law enforcement, national security, or intelligence missions.

F. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, foreign, or international) where the FBI determines that the information is relevant to the recipient entity's law enforcement responsibilities.

G. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—civil, criminal, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity, that is charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

H. To any entity or individual where there is reason to believe the recipient is or could become the target of a particular criminal activity, conspiracy, or other threat, to the extent the information is relevant to the protection of life, health, or property. Information may similarly be disclosed to other recipients who have interests to which the threat may also be relevant, or who may be able to assist in protecting against or responding to the threat.

I. To persons or entities where there is a need for assistance in locating missing persons, and where there are reasonable grounds to conclude from available information that disclosure would further the best interests of the individual being sought.

J. To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, local, tribal, or territorial government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the

former employee regarding a matter within that person's former area of responsibility.

K. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

L. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

M. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Computerized records are stored electronically on hard disk, removable storage devices, or other digital media in areas safe from access by unauthorized persons or exposure to environmental hazards. Some information may also be maintained in hard copy or other form.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by personal identifiers or key word searches.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration (NARA). Different types of information may be subject to different FBI and NARA-approved records' schedules, which are available at *https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0065*.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

System records are maintained in limited access space in FBI controlled facilities and offices. Computerized data is password protected and requires two-factor authentication for access. Remote access through the Internet is provided via the encrypted communications protocol Hypertext Transfer Protocol with Transport Layer Security (HTTPS). All FBI personnel are required to pass an extensive background investigation. The information is accessed only by authorized DOJ personnel or by non-DOJ personnel properly authorized to access the system. The system employs role-based access and authentication controls and enforcement mechanisms so that each user can

access only the information and system locations appropriate for their role. Authorized system users will be subject to adequate physical security controls and built-in system controls to protect against unauthorized personnel gaining access to the equipment and/or the information stored in it. All authorized users are required to agree to Rules of Behavior and Terms of Use limiting use of the information in the system to official purposes. System audit logs are created and monitored to detect any misuse of the system.

RECORD ACCESS PROCEDURES:

The Attorney General has exempted this system of records from the notification, access, amendment, and contest procedures of the Privacy Act. These exemptions apply only to the extent that the information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j) or (k). Where compliance would not appear to interfere with or adversely affect the purposes of the system, or the overall law enforcement/intelligence process, the applicable exemption (in whole or in part) may be waived by the FBI in its sole discretion.

All requests for access should follow the guidance provided on the FBI's website at *https://www.fbi.gov/services/records-management/foipa*. A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 170 Marcel Drive, Winchester, VA 22602-4843; facsimile: 540-868-4995/6/7; electronically: *https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records*. The request should include a general

description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity, which can be located at the above link. In the initial request, the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

CONTESTING RECORD PROCEDURES:

The Attorney General has exempted this system of records from the notification, access, amendment, and contest procedures of the Privacy Act. These exemptions apply only to the extent that the information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where compliance would not appear to interfere with or adversely affect the purposes of the system, or the overall law enforcement/intelligence process, the applicable exemption (in whole or in part) may be waived by the DOJ in its sole discretion.

Individuals desiring to contest or amend information maintained in the system should direct their requests according to the **RECORD ACCESS PROCEDURES** paragraph above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. The envelope and letter should be clearly marked "Privacy Act Amendment Request" and

comply with 28 CFR 16.46 (Request for Amendment or Correction of Records). Some information may be exempt from contesting record procedures as described in the **EXEMPTIONS PROMULGATED FOR THE SYSTEM** paragraph, below. An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

NOTIFICATION PROCEDURES:

Same as **RECORD ACCESS PROCEDURES** paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5) and (8); (f); and (g) of the Privacy Act. The exemptions will be applied only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Rules are being promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and are published in this Federal Register. In addition, the FBI will continue in effect and assert all exemptions claimed under 5 U.S.C. 552a(j) or (k) (or other applicable authority) by an originating agency from which the FBI obtains records, where one or more reasons underlying an original exemption remain valid. Where compliance with an exempted provision does not appear to interfere with or adversely affect interests of the United States or other system stakeholders, the FBI in its sole discretion may waive an exemption in whole or in part; exercise of this discretionary waiver prerogative in a particular matter shall not create any entitlement to or expectation of waiver in that matter

or any other matter. As a condition of discretionary waiver, the FBI in its sole discretion may impose any restrictions deemed advisable by the FBI (including, but not limited to, restrictions on the location, manner, or scope of notice, access, or amendment).

HISTORY:

None.

[FR Doc. 2017-25994 Filed: 12/1/2017 8:45 am; Publication Date: 12/4/2017]