



Billing Code: 4410-AT-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 001-2020]

Privacy Act of 1974; Systems of Records

AGENCY: Office of Community Oriented Policing Services, 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 Office of Community Oriented Policing Services (COPS Office), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records notice titled COPS Management System: NexGen (CMS:NxG), JUSTICE/COPS-003. The COPS Office proposes to establish this system of records to consolidate its various business databases, applications, and web applications under one umbrella to support the grant-making and grant management processes from the pre-award phase, including posting solicitations and administering applications for COPS Office funding, to the post-award phase, including budget modifications and award monitoring activities. Previously, grant-making and grant management was handled by a legacy system covered under the DOJ-003 Correspondence Management Systems (CMS) SORN. Because certain aspects of NexGen are more consistent with a separate system of records, COPS is issuing a new SORN to make that clear.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this System of Records 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 DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

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 20002; by facsimile at 202-307-0693; or by email at *privacy.compliance@usdoj.gov*. To ensure proper handling, please reference the above-listed CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Mark Gowen, Information System Security Officer, COPS Office, 145 N Street NE, Washington, DC 20530; by email at *mark.a.gowen@usdoj.gov*, or by phone at (202) 305-8840.

SUPPLEMENTARY INFORMATION:

The COPS Office advances the practice of community policing in America's state, local, territorial, and tribal law enforcement agencies through information and grant resources. CMS:NxG provides authorized internal users with the capability to effectively run queries on various data elements, review and score applications, select successful applicants for COPS Office funding, generate award documents for successful applicants, sign off on awards, and obligate award funds. CMS:NxG is also used by authorized internal users to update, modify, and maintain files for unsuccessful applicants, and award files for past and current award recipients.

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

Dated: January 6, 2020.

Peter A. Winn,

Acting Chief Privacy and Civil Liberties Officer,

United States Department of Justice.

JUSTICE/COPS-003

SYSTEM NAME AND NUMBER:

COPS Management System: NexGen (CMS:NxG), JUSTICE/COPS-003

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained in two Office of Community Oriented Policing Services (COPS Office) locations: 145 N Street NE Washington, DC 20530, and, on the date of this publication, the DOJ Federal Risk and Authorization Management Program (FedRamp) Certified Azure Government Cloud. Cloud computing service providers may change. For information about the current cloud computing service provider, please contact the COPS Office through its website, <https://www.cops.usdoj.gov>.

SYSTEM MANAGER(S) AND ADDRESSES:

Donte Turner, Acting Chief Information Officer, and Mark Gowen, Information System Security Officer, (202) 305-8840, COPS Office, 145 N Street NE, Washington, DC 20530.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

CMS:NxG is established and maintained pursuant to 5 U.S.C. 301 and 44 U.S.C. 3101. General authority for the COPS Office mission activities include the Violent Crime Control and Law Enforcement Act of 1994 (Pub. L. 103–322), and the Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. 109–162). Specifically, these authorities authorize the COPS Office to provide grants to states,

units of local government, territories, tribal governments, public and private entities to advance community policing.

PURPOSE(S) OF THE SYSTEM:

CMS:NxG consolidates various business databases, applications, and web applications under one umbrella to streamline and expedite the grant-making and grant management processes to effectively advance the COPS Office's community policing mission.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The individuals covered by CMS:NxG are the COPS Office's unsuccessful grant applicants, and past and current award recipients. These include state, local, territorial, and tribal law enforcement agency officials, government officials, tribal officials/representatives, representatives of private and public institutions of higher education, and representatives of for-profit and nonprofit organizations.

CATEGORIES OF RECORDS IN THE SYSTEM:

CMS:NxG maintains files for unsuccessful applicants and award files for past and current award recipients of COPS Office funding, including business and contact information about grant applicants, and the outcomes of grant applications. For audit purposes, the system maintains information regarding the COPS Office programs applied for by applicants, and the final disposition of applications (funded or denied funding). CMS:NxG also maintains information from queries including, but not limited to, the number of applicants that applied for COPS Office programs each fiscal year; the number of applicants funded and denied funding for each fiscal year; the total number of awards authorized for each fiscal year; the total number of awards made by the COPS Office for

each fiscal year; the number of years the same award recipients received funding from the COPS Office; and the dollar amounts of the awards and the associated duration of award obligations.

RECORD SOURCE CATEGORIES:

Individuals with the authority to sign and submit applications for COPS Office funding, on behalf of state, local, territorial, and tribal law enforcement agencies, states, units of local government, Indian tribes, for-profit and nonprofit organizations, private and public institutions of higher education, and individuals authorized to make modifications to existing COPS Office awards.

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), all or a portion of the records or information contained in this system of records may be disclosed as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

A. To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. Any such disclosure under 28 CFR 50.2 would be in connection with a civil or criminal proceeding.

B. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

C. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

D. 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, DOJ (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.

E. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system of records.

F. To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local 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.

G. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, 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 charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

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

I. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

J. 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in CMS:NxG are stored in electronic format in the Justice Management Division (JMD) cloud platform. Records are stored securely in accordance with applicable federal laws, regulations, Department directives, and guidance.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Authorized internal users with the required permissions may retrieve information in CMS:NxG by an individual's name, including the name of the business point-of-contact (POC), law enforcement executive, agency executive (for institutions of higher education, for-profit and nonprofit organizations), government executive, program official, and financial official of the applicant or award recipient agency/organization.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records for successful applicants are destroyed ten years after final action is taken on the award, but longer retention is authorized if required for business use in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) 1.2, item 020, Disposition Authority DAA-GRS-2013-0008-0001. Other records (unsuccessful applications) in CMS:NxG are destroyed three years after final action is taken on the file, but longer retention is authorized if required for business use in accordance with GRS 1.2, item 021 and item 010, Disposition Authority DAA-GRS-2013-0008-0006, and DAA-GRS-2013-0008-0007, respectively.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information in CMS:NxG is safeguarded in accordance with appropriate laws, rules, and policies, including the Department's mandated standards. Records and technical equipment are maintained in buildings with restricted access. Internal access is restricted using traditional two-factor authentication, and external access is restricted using complex passwords. Electronic records are accessed only by authorized personnel with accounts on the COPS Office computer network, and authorized external users with password access to their own account via the COPS Office Agency Portal. Additionally,

direct access to certain information may be restricted depending on a user's role and responsibility within CMS:NxG.

Internet connections are protected by multiple firewalls. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations. Users of individual computers can only gain access to their own data using a valid user identification and password.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the COPS Office, FOIA/PA, 145 N Street NE, Washington, DC 20530 or by email to cops.foia@usdoj.gov. The envelope and letter should be clearly marked "Privacy Act Access Request." The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. The request must 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 either notarized or submitted under penalty of perjury.

Although no specific form is required, you may obtain forms for this purpose from the FOIA/Privacy Act Mail Referral Unit, United States Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530, or on the Department of Justice Web site at <https://www.justice.gov/oip/oip-request.html>.

More information regarding the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 CFR Part 16 Subpart D, "Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974."

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the “RECORD ACCESS PROCEDURES” paragraph, above. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked “Privacy Act Amendment Request.” All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

More information regarding the Department’s procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR 16.46, “Requests for Amendment or Correction of Records.”

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the “RECORD ACCESS PROCEDURES” paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2020-00786 Filed: 1/17/2020 8:45 am; Publication Date: 1/21/2020]