

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:

Electronic records and backups are stored on secure servers approved by GSA Office of the Chief Information Security Officer (OCISO) and accessed only by authorized personnel. Paper files are stored in locked rooms or filing cabinets.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrievable by a variety of fields including, without limitation, name of an individual involved in a case, email address, email heading, email subject matter, business or residential address, social security number, phone number, date of birth, contract files, litigation files, or by some combination thereof.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

System records are retained and disposed of according to GSA records maintenance and disposition schedules and the requirements of the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS:

Access is limited to authorized individuals with passwords or keys. Electronic files are maintained behind a firewall, and paper files are stored in locked rooms or filing cabinets.

RECORD ACCESS PROCEDURES:

Individuals wishing to access their own records should contact the system manager at the above address. Procedures for accessing the content of a record in the Case Tracking and eDiscovery System and appeal procedures can also be found at 41 CFR part 105–64.2.

CONTESTING RECORD PROCEDURES:

Individuals wishing to contest the content of any record pertaining to him or her in the system should contact the system manager at the above address. Procedures for contesting the content of a record in the Case Tracking and eDiscovery System and appeal procedures can also be found at 41 CFR part 105–64.4.

NOTIFICATION PROCEDURES:

Individuals wishing to inquire if the system contains information about them

should contact the system manager at the above address. Procedures for receiving notice can also be found at 41 CFR part 105–64.4.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

This notice modifies the previous notice, published at 77 FR 16839, on March 22, 2012.

[FR Doc. 2017–04017 Filed 3–1–17; 8:45 am]

BILLING CODE 6820–34–P

GENERAL SERVICES ADMINISTRATION

[Notice–ID–2016–02; Docket No: 2016–0002; Sequence No. 28]

Privacy Act of 1974; System of Records

AGENCY: Office of the Deputy Chief Information Officer, General Services Administration, GSA.

ACTION: Notice of a new system of records.

SUMMARY: GSA proposes a new government-wide system of records subject to the Privacy Act of 1974.

DATES: The system of records notice is effective upon its publication in today's **Federal Register**, with the exception of the routine uses which are effective April 3, 2017. Comments on the routine uses or other aspects of the system of records notice must be submitted by April 3, 2017.

ADDRESSES: Submit comments identified by “Notice–ID–2016–02, Notice of New System of Records” by any of the following methods:

- *Regulations.gov:* <http://www.regulations.gov>. Submit comments via the Federal eRulemaking portal by searching for Notice–ID–2016–02, Notice of New System of Records. Select the link “Comment Now” that corresponds with “Notice–ID–2016–02, Notice of New System of Records. Follow the instructions provided on the screen. Please include your name, company name (if any), and “Notice–ID–2016–02, Notice of New System of Records” on your attached document.

- *Mail:* General Services Administration, Regulatory Secretariat Division (MVCB), 1800 F Street NW., Washington, DC 20405. ATTN: Ms. Flowers/Notice–ID–2016–02, Notice of New System of Records.

Instructions: Comments received generally will be posted without change to <http://www.regulations.gov>, including any personal and/or business confidential information provided. To

confirm receipt of your comment(s), please check www.regulations.gov, approximately two to three days after submission to verify posting (except allow 30 days for posting of comments submitted by mail).

FOR FURTHER INFORMATION CONTACT: Call or email the GSA Chief Privacy Officer at telephone 202–322–8246, or email gsa.privacyact@gsa.gov.

SUPPLEMENTARY INFORMATION: GSA proposes to establish a new government-wide system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. Pursuant to Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113–101, the Office of Management and Budget (OMB), in collaboration with the Chief Acquisition Officers Council, Department of Health and Human Services (HHS) and GSA, is engaged in a multifaceted effort that aims to reduce reporting burden, standardize processes, and reduce costs for Federal awardees. OMB is providing strategic leadership for the procurement pilot and collaborating with GSA and the Chief Acquisition Officers Council for implementation. The objectives of the Section 5 procurement pilot focus are to:

- Identify recommendations in the National Dialogue for further review
- Develop a central reporting portal prototype and collection tool for FAR required reports, and
- Test the portal by centrally collecting select FAR required reports that are currently reported across the Federal government, beginning with collection of reports required under FAR 22.406–6.

The goal is to allow contractors doing business with the Federal Government to submit FAR required reports to one central location in an efficient and effective manner rather than multiple locations and to each contracting officer (CO).

As part of this collaboration, GSA is developing and will operate the Federal Acquisition Regulation (FAR) Data Collection System. The system allows prime contractors and subcontractors (“submitters”), performing work on federal contract awards to enter and certify various reports required by the FAR. The system is intended to decrease the reporting burden on submitters and prior to full adoption the system will be used in a pilot to measure and demonstrate that burden reduction.

Submitters will use the system to report data on their applicable awards. Each awarding agency will access the data provided pursuant to its award(s) and share it internally as required and

provided by law. Each agency is responsible for the collection and use of data pertaining to the submitters. GSA is the system owner and operator.

OMB and GSA will use ongoing feedback from pilot participants, and modify the pilot reporting tool as necessary; and will analyze the feedback on pilot and other relevant information to determine expansion to other FAR required reports.

Richard Speidel,

Chief Privacy Officer, Office of the Deputy Chief Information Officer, General Services Administration.

SYSTEM NUMBER

GSA/GOVT-10

SYSTEM NAME:

Federal Acquisition Regulation (FAR) Data Collection System.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The General Services Administration's (GSA) Federal Acquisition Service (FAS) owns the FAR Data Collection System, which is housed in secure datacenters in the continental United States. Each agency that makes awards has custody of the records pertaining to its own contracts. Contact the system manager for additional information.

SYSTEM MANAGER:

Integrated Award Environment Assistant Commissioner, Office of Integrated Award Environment, Federal Acquisition Service, General Services Administration, 1800 F Street NW., Washington, DC 20405.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

E-Government Act of 2002 (Pub. L. 107-347) Section 204; Davis-Bacon and Related Acts: 40 U.S.C. 3141-3148 40 U.S.C. 276a; 29 CFR parts 1, 3, 5, 6 and 7; Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113-101.

PURPOSES OF THE SYSTEM:

The system facilitates collection of data that prime contractors and their subcontractors are required to submit. Each agency is responsible for the collection, use and review of data pertaining to its contracts to verify contractor compliance with applicable requirements. The system includes an online portal that allows prime or subcontractors to enter, review and as applicable, certify FAR-required reports. While logged in, a prime or subcontractor is able to enter data and review reports. After a required report has been entered by the prime

contractor or a subcontractor on a contract, the prime contractor certifies that the report is correct and submits it to the contracting officer. Contracting officers and other authorized officials in the awarding agency use the data from the system to review submissions for compliance with contractual terms and conditions for contracts for which they are responsible.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The FAR Data Collection System contains records related to prime contractors who are performing on federal contract awards ("prime contractor"), subcontractors, their employees ("prime or subcontractor employees") and employed by the Federal Government. An owner, agent, or employee of a prime or subcontractor may enter or certify information, as applicable.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records include the name of the person entering, and as applicable, certifying, information on behalf of the prime or subcontractor, their position within the company, phone number, and email address. Categories of records related to employees of prime and subcontractors include, but are not limited to: Name, unique identifier assigned by the prime or subcontractor, work classification (per the Department of Labor's job classifications), regular and overtime hours worked by day/date, total hours worked, fringe benefits, whether paid as hourly rate in cash amounts or as an employer-paid benefit, and federal projects gross earnings. Some prime or subcontractors may be obligated to provide contractor employee information about themselves if they are self-employed. Categories of records related to acquisition personnel include name, position, work phone number, email address and other similar records related to their official responsibilities.

RECORD SOURCE CATEGORIES:

Employee records are created, reviewed and, as appropriate, certified by the prime or subcontractor. Records pertaining to the individual entering and certifying data in the system may be created by the individual, by a contracting officer, or in the case of a subcontractor by the prime contractor or another subcontractor. Records pertaining to federal acquisition personnel using the system may be entered by the individual or by other federal employees at the individual's agency.

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) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

b. To a Member of Congress or his or her staff in response to a request made on behalf of and at the request of the individual who is the subject of the record.

c. To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) GSA or any component thereof, or (b) any employee of GSA in his/her official capacity, or (c) any employee of GSA in his/her individual capacity where DOJ or GSA has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and GSA determines that the records are both relevant and necessary to the litigation.

d. To the National Archives and Records Administration (NARA) for records management purposes.

e. To the Office of Management and Budget (OMB) and the Government Accountability Office (GAO) in accordance with their responsibilities for evaluation or oversight of Federal programs.

f. To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant.

g. To appropriate agencies, entities, and persons when (1) GSA suspects or has confirmed that there has been a breach of the system of records; (2) GSA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, GSA (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 GSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

h. To another Federal agency or Federal entity, when GSA 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:

Electronic records and backups are stored on secure servers approved by GSA Office of the Chief Information Security Officer (OCISO) and accessed only by authorized personnel.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

System records are retrievable by searching against information in the record pertaining to the prime or subcontractor (e.g., the prime or subcontractor's company's name; the name of the individual entering or certifying information on behalf of the prime or subcontractor), the contract, (e.g., the contract number), or the contracting officer; however, each agency can only access and retrieve the records pertaining to contracts being administered by its acquisition personnel.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

System records are retained and disposed of according to each respective agency's records maintenance and disposition schedules including, as applicable, the NARA General Records Schedule 1.1, Financial Management and Reporting Records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in the system are protected from unauthorized access and misuse through a combination of administrative, technical and physical security measures. Administrative measures include but are not limited to policies that limit system access to individuals within an agency with a legitimate business need, and regular review of security procedures and best

practices to enhance security. Technical measures include but are not limited to system design that allows prime contractor and subcontractor employees access only to data for which they are responsible; role-based access controls that allow government employees access only to data regarding contracts awarded by their agency or reporting unit; required use of strong passwords that are frequently changed; and use of encryption for certain data transfers. Physical security measures include but are not limited to the use of data centers which meet government requirements for storage of sensitive data.

RECORD ACCESS PROCEDURES:

Prime and subcontractors enter and review their own data in to the system, and are responsible for indicating that those data are correct. If an individual wishes to access any data or record pertaining to him or her in the system after it has been submitted, that individual should consult the Privacy Act implementation rules of the agency to which the report was submitted. For example, for reports submitted to GSA, procedures for accessing the content of a record can be found at 41 CFR part 105-64.2.

CONTESTING RECORD PROCEDURES:

Prime and subcontractors with access to the FAR Data Collection System can edit their own reports before submitting them. If an individual wishes to contest the content of any record pertaining to him or her in the system after it has been submitted, that individual should consult the Privacy Act implementation rules of the agency to which the report was submitted. For example, for reports submitted to GSA, procedures for contesting the content of a record and appeal procedures can be found at 41 CFR part 105-64.4.

NOTIFICATION PROCEDURES:

Prime and subcontractors with access to the FAR Data Collection System enter and review their own data in the system. If an individual wishes to be notified at his or her request if the system contains a record pertaining to him or her after it has been submitted, that individual should consult the Privacy Act implementation rules of the agency to which the report was submitted. For example, for reports submitted to GSA, procedures for receiving notice can be found at 41 CFR part 105-64.4.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

[FR Doc. 2017-04037 Filed 3-1-17; 8:45 am]

BILLING CODE 6820-34-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[60Day-17-1014: Docket No. CDC-2017-0012]

Proposed Data Collection Submitted for Public Comment and Recommendations

AGENCY: Centers for Disease Control and Prevention (CDC), Department of Health and Human Services (HHS).

ACTION: Notice with comment period.

SUMMARY: The Centers for Disease Control and Prevention (CDC), as part of its continuing efforts to reduce public burden and maximize the utility of government information, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995. This notice invites comment on the updated "CDC WORKSITE HEALTH SCORECARD," an organizational assessment and planning tool designed to help employers identify gaps in their health promotion programs and prioritize high-impact strategies for health promotion at their worksites.

DATES: Written comments must be received on or before May 1, 2017.

ADDRESSES: You may submit comments, identified by Docket No. CDC-2017-0012 by any of the following methods:

- *Federal eRulemaking Portal:* Regulations.gov. Follow the instructions for submitting comments.

- *Mail:* Leroy A. Richardson, Information Collection Review Office, Centers for Disease Control and Prevention, 1600 Clifton Road NE., MS-D74, Atlanta, Georgia 30329.

Instructions: All submissions received must include the agency name and Docket Number. All relevant comments received will be posted without change to Regulations.gov, including any personal information provided. For access to the docket to read background documents or comments received, go to Regulations.gov.

Please note: All public comment should be submitted through the Federal eRulemaking portal (Regulations.gov) or by U.S. mail to the address listed above.

FOR FURTHER INFORMATION CONTACT: To request more information on the proposed project or to obtain a copy of the information collection plan and instruments, contact the Information Collection Review Office, Centers for Disease Control and Prevention, 1600