US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/23/2026

OPDIV:

NIH

Name:

Electronic Government Ordering System

PIA Unique Identifier:

P-9874415-175971

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

No changes have occurred since the last privacy impact assessment (PIA) was done.

Describe the purpose of the system.

The electronic government ordering system (e-GOS) is the NIH Information Technology (IT) Acquisition and Assessment Center (NITAAC) procurement system providing a mechanism to meet the government wide acquisition contract (GWAC) fair opportunity requirements of Federal Acquisition Regulation (FAR) Part 16 allowing government agencies to procure IT and services and goods. e-GOS currently supports three (3) GWACs including the Chief Information Officer - Solutions and Partners 3 (CIO-SP3), CIO-SP3 Small Business, and CIO- Commodities and Solutions (CS). This system houses all relevant procurement data related to federal government procurements, as well as all contract holder data for companies that were awarded the GWAC.

Describe the type of information the system will collect, maintain (store), or share.

e-GOS collects the following information: business phone numbers, business location, procurement and contract information for both government and businesses, and business proprietary information. Though sensitive in nature, this information is not personally identifiable.

e-GOS collects the following personally identifiable information (PII): Name, email address, phone number and organizational affiliation, login credentials (emails and passwords), contracts and related documents for securing contracts, and Business Proprietary Information. Name, email address, phone number and organizational affiliation is used for information distribution purposes.

NIH employees log into the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique email addresses and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.
Non-NIH employees log into the system using their username, password & multi-factor authentication.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The e-GOS is the NITAAC procurement system providing a mechanism to meet the GWAC fair opportunity requirements of FAR Part 16 allowing government agencies to procure IT and services and goods. e-GOS currently supports three (3) GWACs including the CIO-SP3, CIO-SP3 Small Business, and CIO- CS. This system houses all relevant procurement data related to federal government procurements, as well as all contract holder data for companies that were awarded the GWAC.

e-GOS collects the following information: business phone numbers, business location, procurement and contract information for both government and businesses, and business proprietary information.

e-GOS collects the following PII: Name, email address, phone number and organizational affiliation, login credentials (emails and passwords), contracts and related documents for securing contracts, and Business Proprietary Information. Name, email address, phone number and organizational affiliation is used for information distribution purposes.

NIH employees log into the system using the NIH IAM Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique email addresses and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources. Non-NIH employees log into the system using their username, password & multifactor authentication.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
E-Mail Address
Phone Numbers
Passwords, usernames, multi-factor authenticiation

Contracts and related documents for securing contracts
Business Proprietary Information
Organizational affiliation

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The contact information is used for the purpose of contacting that individual with respect to a contract. PII within the contracts and proprietary information is used for daily acquisition functions. Email and passwords are used by external partners to log into the system.

Describe the secondary uses for which the PII will be used.

NA

Identify legal authorities governing information use and disclosure specific to the system and program.

Public Service Health Act, 42 U.S.C. §§ 282 and 284.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-90-1802, HHS Correspondence, Customer Service, and Contact List Records

09-25-0217 NIH Business System (NBS)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Hardcopy
Email
Online
Government Sources
Within OpDiv
Other HHS OpDiv
Non-Governmental Sources
Commercial Data Broker
Private Sector

Identify the OMB information collection approval number and expiration date

The system does not solicit for PII and is exempt from the paper reduction act.

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Individuals are notified when they register. At that time, it is explained that personal information will be collected. Individuals have the right to consent or not utilize the service.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There isn't a method for opting out. Individuals must provide their PII if they would like to participate in the program. However, at any time, individuals may request being removed from the program and use of e-GOS or may chose to not provide their PII in the first place but then they cannot participate.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

If a major change occurs, NITAAC administrators will reach out to individuals and ask for their consent to use their PII along with options to provide their preferences.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

In the event that an individual's PII has been inappropriately obtained, used, or disclosed, the individual may contact the NITAAC program to have the information removed. In the event that the PII is inaccurate individuals may contact the NITAAC program to have the information changed or potentially utilize self service options.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Individuals control their accounts so NITAAC does not have a process in place for periodic reviews. Individuals are responsible for updates or changes to account related information. Periodic audits are conducted utilizing CloudWatch, CloudTrail, and GuardDuty to ensure the data's integrity, availability, accuracy and relevancy. The system produces reports for review by the Office of Information Technology (OIT) Security and System Administrators..

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job. A NIH IAM Systems account login is required to gain access to the stored PII data. Specific login credentials are required to access the stored PII data.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Periodic training (one training for Federal Customers, and four trainings for General Customers) is provided to instruct users on new features and functionality along with the importance of keeping the data secure and the best practices to avoid exposing PII to unauthorized individuals.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

5-102, Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. Official Record Held in the Office of Record.
Description: Many records included in this item are maintained by accountable officers to account for the availability and status of public funds, and are retained to enable GAO, Office of Inspector General, or other authority audit.
Financial transaction records include those created in the course of procuring goods and services, paying bills, collecting debts, and accounting for all finance activity, per the following definitions.
Disposition Instructions: The data is destroyed 6 years after agreement, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is requested and authorized if required for business use.
Disposition Authority: Disposition Authority Agency (DAA)-General Records Schedules (GRS)-2013-0003-000.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative controls. Include policies, training, and an annual re-certification process to make sure user roles have not changed.

Technical controls: Include the capability to identify users and differentiate among user roles. Based on the least privilege principle, e-GOS allows only the accesses and permissions needed to perform specific functions. User roles are linked to Personal Identity Verification (PIV) smartcard authentication. Strict password requirements include expiration after a set period of time, a minimum length, a combination of uppercase, lowercase, and special characters. In addition, accounts are locked after a set number of incorrect attempts.

Physical controls: The system is entirely hosted within the Amazon Web Services (AWS) East/West region cloud environment. The system infrastructure components are maintained in Federal Risk and Authorization Management Program certified environments, and physical security controls are inherited under the AWS shared responsibility model.

Identify the publicly-available URL:

https://cio.egos.nih.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Other technologies that do not collect PII:

Google Analytics

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null