US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/05/2024

OPDIV:

NIH

Name:

Electronic Government Ordering System

PIA Unique Identifier:

P-6930597-956633

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.

Significant System Management Change

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

The eGOS Legacy application has moved into an Amazon Web Services (AWS) cloud environment, with all the existing data and business logic being moved into the eGOS NextGen application.

Describe the purpose of the system.

The purpose of the Electronic Governance Ordering System (eGOS) NextGen is to support the NIH Information Technology Acquisition and Assessment Center (NITAAC) mission of providing a consistent information system platform to administer Government-Wide Acquisition Contracts (GWACs) for information technology procurement. The eGOS NextGen application is an integrated, web-based task and delivery order processing system that automates NITAAC's GWAC Management and ensures Fair Opportunity compliance.

e-GOS NextGen currently supports three (3) GWACs including the Chief Information Officer - Solutions and Partners 3 (CIO-SP3), CIO-SP3 Small Business, CIO-SP4, and CIO-Commodities and

Solutions (CS).

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

The information collected and maintained by eGOS NextGen includes user's contact information including names, email addresses, business phone numbers, business locations (i.e. corporate offices addresses), organizational affiliation as well as procurement and contract related documents for securing contracts and business proprietary information.

Contact information is obtained by the system in order to identify and contact the account holders that are using the e-GOS NextGen system. This information is considered a system of records (SOR) and covered by the following system of records notice (SORN): 09-90-1802, HHS Correspondence, Customer Service, and Contact List Records.

eGOS NextGen houses only relevant procurement data related to federal government procurements, as well as all contract holder data for companies that were awarded a GWAC by NIH, various HHS OpDivs, and other federal entities.

NIH users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (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 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.

For external users, multi-factor authentication (MFA) and federated login will be used. For MFA login, individuals use their email address, password, and request a one time pin that expires after use or after a set duration of time. For external users using federated login, they log into their own organizational systems (NIH or non-NIH) and are then federated into eGOS NextGen. Federated Login uses assigned temporary tokens, or tickets, to obtain access across the network. Actual login credentials are maintained by the affiliated organization and not NIH.

Information handled under the IAM Services PIA is considered a system of records (SOR) and covered by the following system of records notices (SORNs):
09-25-0216, Administration: NIH Enterprise Directory
09-90-0777, Facility and Resource Access Control Records, HH
09-90-1802, HHS Correspondence, Customer Service, and Contact List Records.

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

The purpose of eGOS NextGen is to support the NITAAC mission of providing a consistent information system platform to administer GWACs for information technology procurement. The eGOS NextGen application is an integrated, web-based task and delivery order processing system that automates NITAAC's GWAC Management and ensures Fair Opportunity compliance.

The information collected and maintained by eGOS NextGen includes user's contact information including names, email addresses, business phone numbers, business locations (i.e. corporate offices addresses), organizational affiliation as well as procurement and contract related documents for securing contracts and business proprietary information.

Contact information is obtained by the system in order to identify and contact the account holders that are using the e-GOS NextGen system. This information is considered a system of records (SOR) and covered by the following system of records notice (SORN): 09-90-1802, HHS Correspondence, Customer Service, and Contact List Records.

eGOS NextGen houses only relevant procurement data related to federal government procurements, as well as all contract holder data for companies that were awarded a GWAC by NIH, various HHS OpDivs, and other federal entities.

NIH users log in to this 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 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.

For external users, MFA and federated login will be used. For MFA login, individuals use their email address, password, and request a one time pin that expires after use or after a set duration of time. For external users using federated login, they log into their own organizational systems (NIH or non-NIH) and are then federated into eGOS NextGen. Federated Login uses assigned temporary tokens, or tickets, to obtain access across the network. Actual login credentials are maintained by the affiliated organization and not NIH.

Information handled under the IAM Services PIA is considered a SOR and covered by the following SORNs:
09-25-0216, Administration: NIH Enterprise Directory
09-90-0777, Facility and Resource Access Control Records, HH
09-90-1802, HHS Correspondence, Customer Service, and Contact List Records.

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

Yes

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

y/n - age 18 by June 15 of the current year

Business proprietary information

Organizational affiliation

Usernames and passwords

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

How many individuals' PII is in the system?

500-4,999

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.

N/A - No secondary uses for PII exist.

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

SORN 09-25-0217 NIH Business System (NBS)

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

N/A. PII within the system is that of business partners, vendors, and federal employees.

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.

When an individual registers and each time they log onto the system it is explained via privacy warnings and message of the day banners (MOTDs) 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.

Individuals cannot opt out of providing basic personally identifiable information (PII) such as name, email address and business and/or cell phone number if using the e-GOS NextGen system. This is used to create the e-GOS NextGen account and allow for individuals to be contacted by NITAAC or others using the services. The requirement for opting-in to the collection of PII is for account identification purposes.

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, the e-GOS NextGen administrators will follow-up with individuals via email or direct phone call to 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, disclosed or inaccurate, the individual may contact NITAAC to have the information removed. On the e-GOS NextGen Home page is a link and phone number to contact e-GOS support staff directly to troubleshoot, identify the root cause, resolve said reported issue, and report to the affected parties in the event their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

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 review this information. The NIH IT Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.

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.

Periodic review of accounts are done by NITAAC leadership along with system administrators to to ensure the
continued need for access to a system.

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.

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 use NIH applications must attend security awareness training every year. There are five categories of mandatory annual IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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

Periodic training 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. 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: DAA-2013-0003-0001).

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

The e-GOS NextGen application takes precautions including organizational, technical and physical measures to help safeguard against the accidental or unlawful destruction, loss, alteration and unauthorized disclosure of, or access to, the personal data that is processed or used.

Administrative controls include the requirement for a NIH background check, having a valid need-to-know , and a separation of duties structure which ensures that no single individual role has control of any critical process in its entirety.

Technical controls include provisioning user roles with the appropriate permissions and structure which ensures that no single individual has control of any critical process in its entirety. Data-in-transit communication is secured using Transport Layer Security (TLS) encryption. Whereas, Federal Information Processing Standard Publication (FIPS) 140-2 compliant encryption is in place for data-at-rest.

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:

AWS 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