

PRIVACY IMPACT ASSESSMENT

Once the Privacy Impact Assessment is completed and the signature approval page is signed, please submit an electronic copy and hard copy with original signatures of the PIA to the SBA Senior Advisor to the Chief Privacy Officer in the Information Privacy Office of the OCIO.

Name of System/Application: Goalowner

Program Office: OHCM

A. CONTACT INFORMATION

1) Who is the person completing this document?

Anthony Campbell
IT Specialist
202-205-6418

2) Who is the system owner?

Kevin Mahoney
Chief Human Capital Officer
202-205-6749

3) Who is the system manager for this system or application?

Kelly Robinson
Chief Workforce Relations Division
202-205-7418

4) Who is the IT Security Manager who reviewed this document?

Ja'Nelle DeVore, Chief Information Security Officer, SBA Office of the CIO, (202) 205-7103, JaNelle.DeVore@sba.gov

5) Who is the Senior Advisor who reviewed this document?

Ethel Matthews, Senior Advisor to the Chief Information Officer, SBA Office of the CIO, 202-205-7173, Ethel.Matthews@sba.gov

6) Who is the Reviewing Official?

Paul Christy, Chief Information Officer, SBA Office of the CIO, 202-205-6708, Paul.Christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) Does this system contain any information about individuals? If yes, explain.

The system will contain general employment information on SBA employees as well as specific information on employee performance, organizational performance award data, and competency development.

a. Is the information about individual members of the public?

No

b. Is the information about employees?

Yes

2) What is the purpose of the system/application?

Goalowner Application provides the systematic performance management process by which an SBA employees, as individuals and members of a group, in improving organizational effectiveness in the accomplishment of SBA mission and goals.

Goalowner Application is an automated performance management tool that:

- Links, manages, tracks and reports on both organizational goal and employee performance plans,
- Focuses on Self Monitoring Analysis and Report Technology (SMART) objectives and helps assess employee proficiency on critical competencies,
- Assists in pay and award decisions,
- Helps manage Individual Development Plans (IDP),
- Facilitates Communication,
- Provides for workflow management, cross organizational reporting and historical analysis,
- A suite of services to implement system, initiate culture change, and refine work processes,
- A system designed specifically to meet Federal standards and regulations for performance management consistent with PMA (President's Management Agenda), PTB (Proud-to-Be Goals - A term, coined by Personnel Staff, to represent goals that have specific deadlines.), HCAAF (Human Capital Assessment and Accountability Framework) and PAAT (Performance Appraisal Assessment Tool), and
- A proven system for enacting effective performance management.

3) Is the system in the development process?

No, the system is in its operational phase.

4) How will the technology investment (new or updated) affect existing privacy processes?

Any Changes to Goalowner will not affect existing privacy processes, the same Technical and Access control will be implemented.

5) What legal authority authorizes the purchase or development of this system/application?

- The American Recovery and Reinvestment Act of 2009 (PL 111-5).

- 15 U.S.C. § 634(b) (6), 44 U.S.C. § 3101.
- Privacy Act of 1974, 5 U.S.C. 552a and related statutes (Electronic Communications Privacy Act of 1986; Computer Matching and Privacy Protection Act of 1988).
- Paperwork Reduction Act of 1995; 44 U.S.C. 3501.
- Government Paperwork Elimination Act of 1998.
- Federal Records Act of 1950 and National Archives and Records Administration (NARA) implementing regulating at 36 C.F.R. 1220 and 41 C.S.R. 201-22.
- The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems." OMB Circular A-130 implements a number of Federal laws relating to information resources ID (for example, the Paperwork Reduction Act, the Clinger-Cohen Act; and the Government Performance and Results Act).
- The Federal Information Security Management Act of 2002 (FISMA).
- Additional program definition is detailed in 13 C.F.R., Part 123.

6) Privacy Impact Analysis: What privacy risks were identified and describe how they were mitigated for security and access controls?

a. No documented audit process in place. SBA approved COE's Audit Plan. The plan has been implemented in the most recent set of production audit reports.

b. Hitting the back button on the Web Browser kicks you out of the application. A solution was sent to SBA, however SBA IT security doesn't allow implementation of the link provided that hides the IE browser bar, essentially eliminating the back button.

Implementation of the browser's back button wasn't mitigated.

C. SYSTEM DATA

1) What categories of individuals are covered in the system?

The Goalowner Application will have three categories of users who are identified by the type of functions they perform on the system.

System Administrative users will perform administrative task such as monitoring logs, administering database and Network users.

System Administrators

Technical System Administrator (COE)

Technical System Administrator (Organization)

Hosting Administrator (subset of Technical System Administrator)

Goalowner Application administrator will administrate system and will perform task such as managing active or inactive employees.

Goalowner Application administrator

HR System Administrator

User Account Administrator

Users

User category organized primary and secondary users depending on frequency of system usage.

Primary Users

Employee (Non-Supervisory)

Supervisor (Immediate or multi level as depicted in Figure)

Organization Component Lead

The system contains information on SBA employees.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Performance information is collected from several sources: directly from the employee regarding work accomplishments; directly from the rating officials regarding the performance of their direct reports; directly from organizational unit leads regarding organizational performance; and directly from supervisors regarding competency development of the subordinates.

General employee information is collected from two sources: the NFC Payroll system and Microsoft Outlook.

b. What Federal agencies are providing data for use in the system?

N/A

c. What Tribal, State and local agencies are providing data for use in the system?

N/A

d. From what other third party sources will data be collected?

N/A

e.) What information will be collected from the employee and the public?

The employee will provide performance feedback information on themselves and their individual performance and accomplishments.

3) Accuracy, Timeliness, and Reliability

a. How is data collected from sources other than SBA records verified for accuracy?

Data from Federal Agency records is identified by name and e-mail address, is subject to Privacy Act regulations and documented practices for accuracy. HR System Administrators will run periodic records checks to verify accuracy. Also, Goalowner will generate error reports on information that seems inconsistent with previous data loads.

b. How is data checked for completeness?

Goalowner Application provides field validation and checks for input accuracy, completeness and validity. Character set, length, numerical range, date range, acceptable values, invalid word formats etc

are validated at the entry point. HR Systems Administration will also conduct periodic assessments of the information in the system to determine if the data is complete.

4) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for the types of information collected?

Goalowner Application hosted application transmits or (and) receives data between the presentation server and the client browser. This data includes passwords, employee information, employee performance data and reports. To protect data during transmission, the Goalowner application uses the Secure Sockets Layer (SSL) and its companion protocol, HTTP over Secure Sockets Layer (HTTPS). HTTPS employs SSL to protect data by encrypting it at the source, be it the server or the client, and decrypting it at the Server Vault Facility.

Goalowner Application hosted site for SBA is not accessible for public users. Only HR System Administration within SBA Network can access Goalowner Application SBA Hosted site. The Firewall at ServerVault allows traffic only from SBA IP address range.

D. DATA ATTRIBUTES

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes, the information is necessary and based on the specific need to evaluate employee performance as required by 5 CFR, Part 430.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No

3) Will the new data be placed in the individual's record?

No

4) Can the system make determinations about employees or members of the public that would not be possible without the new data?

No

5) How is the new data verified for relevance, timeliness and accuracy?

N/A

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

No data is being consolidated in this system.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If process is not consolidated please state, "N/A".

N/A

8) How will the data be retrieved? Does a personal identifier retrieve the data?

Data is accessed by authorized users with sufficient privileges by name and employee email address.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The performance plan report (Personal Business Commitment Plan) can be run by the employee and their supervisor. HR System Administrators will be able to generate the reports on outstanding performance related documents such as progress reviews that have not been completed; employees who are overdue for a performance rating; organizational performance reports, ratings distribution reports, and performance cycle status reports. These reports will be used by HR Specialist to monitor the performance appraisal program and to insure that SBA is in compliance with federal regulations that govern performance management.

Organizational performance reports are generated for individual offices. These reports will be used for the daily operation of the offices and other staff management purposes. These reports are restricted to specific office management and individuals involved with insuring accuracy of the data.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required authorized uses), and how individuals can grant consent.

The collected employee data is the same mandatory data required for employment consideration. The performance data and individual performance feedback data that is entered by the supervisor is required for conducting annual performance appraisals. The employee may (not required) enter their own performance progress information into the system. All performance data (whether provided by the employee or documented by the supervisor) will be maintained in accordance with the Privacy Act and will not be used for any other purpose that for which it was collected.

11) Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used as intended.

Goalowner Solution provides three types of roles at each of the Server Layer to enforce Access Levels; Application Role at the Presentation Server, Business Role at the Business Object Server and Action Roles at the Database Server. Goalowner Solution also, utilizes Microsoft Windows 2003 Server Active Directory. Active Directory provides protected storage of user account and group information by using access control on objects and user credentials. Because Active Directory stores not only user credentials but also access control information, users who log on to the network obtain both authentication and authorization to access system resources.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system operates from a single site with a separate site as a backup. Data is replicated to the backup site for disaster recovery purposes.

2) What are the retention periods of data in this system?

Data retention standards are consistent with SOP 34 30, which requires performance data to be maintained on employees for a period of three years.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Data retention and reports retention standards are recorded in the System Security Plan. Performance appraisal records older than 3 years will be expunged from the system.

4) Is the system using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No

5) How does the use of this technology affect public/employee privacy?

N/A

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The system will contain general employee information such as name, email, grade, series, step, organizational unit. It will maintain and track this information throughout the employment tenure of each employee. If the employee changes grade, series, organizational component, etc. this information will be updated in the system. This will allow rating officials and HR Administrators to track employee general information and performance data. This information is also tracked through our payroll system which is the source from which the information in Goalowner will be updated.

7) What kinds of information are collected as a function of the monitoring of individuals?

The system will contain the general employment information mentioned in E6 as well as specific information on employee performance, organizational performance, performance awards data, and competency development, work accomplishments, etc.

8) What controls will be used to prevent unauthorized monitoring?

Access is limited by control of Users ID's, password controls, and the assignment of a User Role profile to all User ID's. Each user role comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user. A Goalowner user manual details the various roles within the system and explains the access associated with each User Role profile. HR Systems Administrators have control over assigned user roles and will have access to audit logs that record the activities that occur within the system. Agency network log-on procedures mandate a posted Privacy notice be viewed and acknowledged prior to entry. Additionally, all system users will be

trained prior to initial system deployment and refresher training will occur every two years. This training will include Privacy Act rules and prohibitions on the dissemination or use of non-public information.

9) Under which Privacy Act systems of records notice (SORN) does the system operate? Provide number and name.

SBA Privacy Act System of Records

Employee Information Files- SBA 9 & SBA 23

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?

No revision is necessary.

F. DATA ACCESS

a. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, tribes, other)

Access is open to all SBA employees; SBA supervisors/rating officials acting in their official capacity, with access to information on their direct reports only; and certified contractors under confidentiality agreements while actually engaged in system development, modifications or maintenance.

b. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access is limited by control of Users ID's, password controls, and the assignment of a User Role profile to all User ID's. Each user role comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user. Goalowner users manual details the various roles within the system and explains the access associated with each User Role profile.

c. Will users have access to all data on the system or will the user's access be restricted? Explain.

Users have access only to screen, reports and data corresponding to their assigned system user roles. HR System Administrators have control over assigned user roles and will have access to audit logs that record the activities that occur within the system.

d. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

Access is limited by control of Users ID's, password controls, and the assignment of a User Role profile to all User ID's. Each user role comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user. Audit logs record every user who access the system to include date, time, what was accessed and any action (add, delete modify).

e. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes

f. Do other systems share data or have access to the data in the system? If yes, explain.

No

g. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The System owner and the System manager are jointly responsible for protecting the privacy rights of the public and employees.

h. How will the shared data be used by the other agency?

N/A

i. What procedures are in place for assuring proper use of the shared data?

N/A

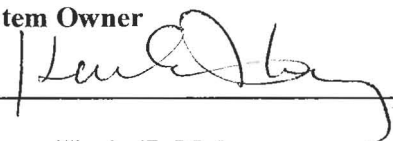
j. Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for information shared internal and external.

Goalowner does not provide access to external organizations for information sharing nor is it integrated with other systems.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

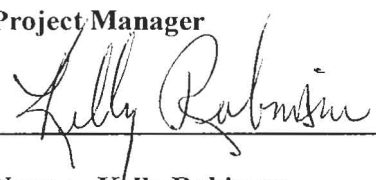
1) System Owner

 (Signature) 4/8/11 (Date)

Name: Kevin E. Mahoney

Title: Chief Human Capital Officer


2) Project Manager

 (Signature) June 8/2011 (Date)

Name: Kelly Robinson

Title: Chief Workforce Relations

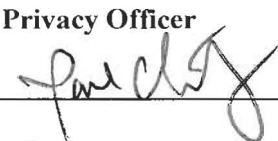
3) IT Security Manager

 (Signature) 6/10/11 (Date)

Name: Ja'Nelle L. DeVore

Title: Chief Information Security Officer

4) Chief Privacy Officer

 (Signature) 7/15/11 (Date)

Name: Paul Christy

Title: Chief Information Officer