

SMALL BUSINESS ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

Name of Project: Automated Labor and Employee Relations Tracking System
(ALERTS)

Program Office: Office of Human Capital Management (OHCM)

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Kelly M. Robinson
Senior Policy Analysis
Office of Human Capital Management
HR Policy
202-205-7418
Kelly.Robinson@sba.gov

2) Who is the System Owner?

Napoleon Avery
Chief Human Capital Officer
Office of Human Capital Management
202-205-6784
Napoleon.Avery@sba.gov

3) Who is the System Manager for this system or application?

Stevie Gray
Labor and Employee Relations Branch Chief
Personnel Services Division
202-205-6119
Stevie.Gray@sba.gov

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

Dave McCauley
Chief Information Security Officer
Office of the Chief Information Officer
202-205-7103
David.McCauley@sba.gov

5) Who is the Bureau/Office Privacy Act Officer who reviewed this document?

Ethel Matthews
Senior Advisor to the Chief Privacy Officer
Office of the Chief Information Officer
(202) 205-7173
Ethel.Matthews@sba.gov

Who is the Reviewing Official? (According to OMB, this is the agency CIO or other agency head designee who is other than the official procuring the system or the official who conducts the PIA).

Christine Liu
Chief Information Officer/Chief Privacy Officer
Office of the Chief Information Officer
(202) 205-6708
Christine.Liu@sba.gov

B. PIA PROCESS APPLICATION/GENERAL INFORMATION

1) Does this system contain any information about individuals?

a. Is this information identifiable to the individual?

Yes

b. Is the information about individual members of the public?'

No

c. Is the information about employees?

Yes

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

The system is used to track labor and employee relation actions to include adverse actions, exceptions to arbitration awards, unfair labor practices, grievances and negotiability appeals. It will also serve as the repository of bargaining history for negotiations between management and the union.

3) What: legal authority authorizes the purchase or development of this PIA Process?

Privacy Act of 1974, 5 USC 552a and related statutes (Electronic Communications Privacy Act of 1986; Computer Matching and Privacy Protection Act of 1988)

Paperwork Reduction Act of 1995; 44 USC 3501.

Government Paperwork Elimination Act of 1998.

Federal Records Act of 1950 and National Archives and Records Administration (NARA) implementing regulating at 36 CFR 1220 and 41 CSR 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 management (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 Title 13 of the Code of Federal Regulations (13 CFR), Part 123.

C. DATA IN THE PROCESS:

1) Generally describe the type of information to be used in the system and what categories of individuals are covered in the System?

Confidential information on employees related to employee and labor relations cases may include personal information such as names, addresses and emergency contact/representative name and telephone number, personnel data and employment history including field duty locations, results of background investigation, suitability status, performance appraisals, retirement estimates, retirement applications. This data may be collected via employment application, acceptance and entrance on duty forms.

The system does not require PII (i.e. SSNs, DoB), but there may be documents that are uploaded in a case to include the Standard Form 52/50 Request for or Personnel Action, OPM retirement applications (SF-2801 or SF-3107), which may have PII.

All SBA employees, agency-wide are covered in the system.

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, source then what other source**

Information is collected from several sources: employees, unions, employee representatives, results of investigations, National Finance Center (NFC) personnel and payroll system, employment applications, electronically from the FBI for fingerprint checks.

- b. What Federal agencies are providing data for use in the process?**

The Federal agencies that may provide data which would be used in this process may include FBI for employee fingerprint checks and background investigations, OIG, NFC, EEO, and OPM.

- c. What State and local agencies are providing data for use in the process?**

All state employment agencies, unemployment offices and court systems..

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

Information could be collected from private physicians, EAP counselors, employee representatives (attorneys, unions).

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

The employees provide their Social Security Number, home address, contact information (home phone, emergency contacts), prior employment records.

3) Accuracy, Timeliness, and Reliability

- a. How will data collected from sources other than SBA records be verified for accuracy?**

Data from federal agency records is identified by name, address, and/or SSN and is subject to Privacy Act regulation and documented practices for accuracy. Data from commercial entities is subject to regulation and identified by name, address and SSN. All information must be verified by the employee.

b. How will data be checked for completeness?

Applicant data is compared and reconciled with any third party data received. Agency business rules and system edits require critical information be complete before processing. Discrepancies are discussed with applicants.

c. Is the Data Current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (i.e., data models)

Yes. Data collected directly from applicants is updated as provided.

d. Are the data elements described in detail and documented? If Yes, What is the name of the document?

The Micropact IT Configuration and IT Contingency Plan identifies the names of the data elements for the system.

D. ATTRIBUTES OF THE DATA

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

Yes. The information is based on specific need to maintain adverse actions and appeals and labor relations third party proceedings which have timeframes that are prescribed by statute, government-wide regulations and agency policy and regulations.

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

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

N/A

3) Can the system make determinations about employees/public that would not be possible without the new data?

N/A

4) How will the new data be verified for relevance and accuracy?

N/A

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

The ALERTS consolidates data previously housed in multiple legacy systems (i.e., NFC Personnel and Payroll System). Information from the legacy system and other sources previously identified are uploaded into the system and is controlled based on the type/category of information provided. All data is resident on one system, with User ID, passwords and role responsibility based access controls. Prior to accessing the system, all users must acknowledge and accept warning banners which denotes the user's understanding of the rules and regulations based on the policies displayed with the warning banner.

6) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access through the process? Explain.

No processes are being consolidated.

7) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data is accessed by authorized users with sufficient privileges. The data may be retrieved by employee's name, case manager's name, or automated system tracking case number.

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

Reports can be produced on individual's records for the purpose of workload management, third party proceedings (arbitration and court hearings, etc) and inquiries which comply with Federal Service Labor Management Relations Statute (FSLMRS), and Privacy Act requirements. Access is restricted to the Office of Human Capital Management OHCM officials with the "need to know" and to other inquiries where the specific data complies with FSLMRS, Privacy Act and other government-wide guidelines.

Reports generated may be used for the daily operation of the OHCM offices and other human capital management purposes. These reports are restricted to specific office management and individuals involved with insuring accuracy of the data.

- 9) **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 or authorized uses), and how individuals can grant consent.)**

The collected employee data which is stored electronically is the same mandatory data required to determine and maintain conditions of employment. considerations. Where specific data elements on the employment application and hiring paperwork are identified to not be required or are listed only 'if applicable,' the individual has the option to not provide any information.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

- 1) **If the information in the process is operated in more than one site, how will consistent use of the 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. Consistent use will be maintained by internal standard operating procedures.

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

Data retention standards are consistent with OPMs Guide to Personnel Recordkeeping, Guide to Processing Personnel Actions, and other government-wide regulations. Refer to SBA SORN 23.

- 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?**

Electronic records and backups are retained for prescribed period of time and are the disposition of the data must comply with OPM Guide to Recordkeeping and other government-wide regulations.

Distributed reports and other data extracts will be sanitized of any PII or sensitive data. Refer to SORN 23.

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

Future enhancements may utilize technologies not previously employed. However, no current use of technology can be characterized as such to date.

- 5) **How does the use of this technology affect public/employee privacy?**
N/A
- 6) **Will this system in the processes provided have the capability to identify, locate, and monitor individuals? If yes, explain**
No
- 7) **What kinds of information are collected as a function of the monitoring of individuals?**
None
- 8) **What controls will be used to prevent unauthorized monitoring?**
N/A
- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name**
Small Business Administration Privacy Act System of Records SBA 23
- 10) **If the system is being modified, will the Privacy Act Systems of records notice require amendment or revision? Explain.**
No revision is necessary. While the system is new, the types of data collected and the handling of privacy data remain the same.

F. ACCESS TO DATA:

- 1) **Who will have access to the data in the System?** (e.g., system users, contractors, managers, system administrators, developers, tribes, other)
Access is limited to Agency OHCM officials acting in their official capacity, with a need to know, and certified contractors under confidentiality agreements while actually engaged in system development, modification or maintenance. This may include users, managers, or system administrators.
- 2) **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 User IDs, password controls, and the assignment of a role responsibility profile to all User IDs. Each Responsibility 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. The system owner makes the final determination of what user will have which privileges.

- 3) **Will users have access to all data on the system or will the users' access be restricted? Explain.**

Users have access only to screens, reports and data corresponding to the assigned system Responsibility the user holds. Managers have control over assigned responsibilities, through authorized system administrators.

- 4) **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 User IDs, password controls, and the assignment of a role responsibility profile to all User IDs, effectively limiting browsing. Education of Agency and contractor staff regarding the Privacy Act rules and prohibitions on the dissemination or use of non-public information is mandatory and ongoing. System audit trails will be used to document suspicious or irregular log-ins and navigation of the system. Agency network log-on procedures mandate a posted Privacy notice be viewed and acknowledged prior to entry. SBA Privacy Act System of Records SBA 23 defines routine uses of this information and serves as a control by defining acceptable uses. Limiting access to sensitive information to only those with a need-to-know remains the best and primary control.

- 5) **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, contractors are involved in the design, development, and maintenance of the system. Yes, each contractor employee involved with the system has/ is required to complete a SBA 1228, Computer Access-Clearance Security Form certifying they understand and agree to protect Privacy Act and other sensitive data in accordance with the Privacy Act or 1974, and SBA regulations..

- 6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No, to date, there is no other data system interfaces.

- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

N/A

8) Will other agencies share data or have access to the data in this system?

No other system has access to the data in the system. Data is periodically shared with other Federal and State agencies follow the proper procedures to redact PII information, if required. All information requests are cleared through the appropriate Agency Offices.

9) How will the data be used by the other agency?

MSPB, FLRA and district and federal courts may use the data to implement statutory requirements and legal proceedings.

10) Who is responsible for assuring proper use of the data?

The system owner will determine the appropriate users and the accessed based on established roles and responsibilities.

G. PRIVACY IMPACT ANALYSIS

1) Discuss what privacy risks were identified and how they were mitigated for types of information collected.

Because ALERTS is primarily a management tool, and access to the information contained in the system is restricted, most of the risks identified involved the technological aspects of the design, development and maintenance of the system. Deliberate thought was given to the type of data collected during the requirements generation process. All users must acknowledge and accept the prescribed warning regarding misuse of the information contained in this system.

2) Describe any types of controls that may be in place to ensure that information is used as intent.

Before gaining access to the ALERTS, all users accept a "Rules of Behavior" contained in the security warning banner which states, in part, that they are prohibited from accessing or attempting to access systems or information for which they are not authorized. The form stipulates that users may not read, store or transfer information for which they are not authorized, and that disciplinary action may result from any unauthorized use of SBA systems and computer resources for non-work-related activities. In accepting this agreement, users state that they have read and understand their responsibilities and will comply with the form's rules.

User access is based on need-to-know and the duties and responsibilities of the position the employees are assuming. Therefore, staff only can access PII that they definitely need in the performance of their work. Inappropriate use of data may result in disciplinary action up to and including removal from Federal Service.

3) Discuss what privacy risks were identified and how they were mitigated for information shared internal and external?

Laws, rules and government-wide regulations are established which dictate the use of the system data.

Electronic data can be accessed and retrieved via secure interfaces, including VPN and secure leased lines.

Recipients of PII are informed of their responsibilities for protecting the data and for deleting it after a defined period.

4) What privacy risks were identified and describe how they were mitigated for security and access controls?)

To ensure data extracts containing PII are not exposed for any longer a period than necessary, they are identified, tracked, and overwritten 3 times once their expiration dates are reached.

To ensure employees do not view PII data not required in the performance of their jobs, ALERTS user accounts are assigned specific roles and responsibilities. Users are limited in their access to areas of the system appropriate for those responsibilities. Passwords are changed every 90 days to ensure access to appropriate users.

**APPENDIX A
DECLARATION OF PRIVACY PRINCIPLES**

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the Small Business Administration to the public and are the responsibility of all SBA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the SBA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of SBA data systems, processes and facilities.

All SBA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the SBA, the SBA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.
Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.
Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the SBA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any SBA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.

Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.
---------------	---

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the SBA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

APPENDIX B
POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The SBA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the SBA recognizes that compliance with legal requirements alone is not enough. The SBA also recognizes its social responsibility which is implicit in the ethical relationship between the SBA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the SBA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the SBA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The SBA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. SBA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the SBA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

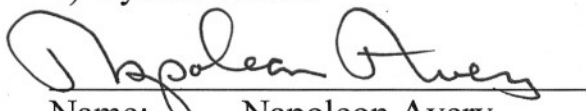
As an advocate for privacy rights, the SBA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the SBA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.

Privacy Assessment for ALERTS


Responsible Officials - Approval Signature Page

The Following Officials Have Approved This Document

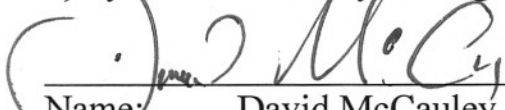
1) System Owner

 (Signature) 9-12-08 (Date)
Name: Napoleon Avery
Title: Chief Human Capital Officer

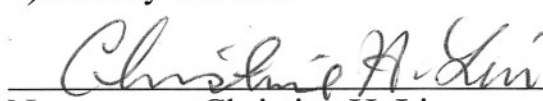
2) System Program/Project Manager

 (Signature) 9/12/08 (Date)
Name: Stevie Gray
Title: Branch Chief

3) System IT Security Manager

 (Signature) 9/26/08 (Date)
Name: David McCauley
Title: Chief Information Security Officer

4) Privacy Official

 (Signature) 9/26/08 (Date)
Name: Christine H. Liu
Title: Chief Information Officer and Chief Privacy Officer