

PRIVACY IMPACT ASSESSMENT

Name of System/Application: Business Development Management Information System
(BDMIS)

Program Office: Government Contracting & Business Development

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

A. CONTACT INFORMATION

1) Who is the person completing this document?

CaSandra L. Smith, Program Analyst/Acting Project Manager
Office of Business Development
6302 Fairview Road, Suite 300
Charlotte, NC 28210
(704) 910-7250
Cassandra.smith@sba.gov

2) Who is the system owner?

Darryl K. Hairston, Associate Administrator, Business Development
Office of Government Contracting and Business Development
409 3rd Street, SW, 8th Floor
Washington, DC 20416
(202) 205-5852
Darryl.hairston@sba.gov

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

Sheila D. Thomas, Director
Office of Program Review
409 3rd Street, SW, 8th Floor
Washington, DC 20416
(202) 205-5852
Sheila.thomas@sba.gov

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

Ja'Nelle Devore, Chief Information Security Officer (CISO)
Chief Information Security Officer
409 3rd Street, SW., 4th Floor
Washington, DC 20416
(202) 205-7103
Janelle.devore@sba.gov

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

Ethel Matthews, Senior Advisor to the Chief Privacy Officer
409 3rd Street, SW, 4th Floor
Washington, DC 20416
Ethel: (202) 204-7173, Ethel.matthews@sba.gov

6) Who is the Reviewing Official?

Paul Christy, Chief Privacy Officer
Office of the Chief Information Officer
409 3rd Street, SW., 4th Floor
Washington, DC 20416
(202) 205-6756
Paul.christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

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

Yes, the system contains information about individuals. A profile is put together in the Central Contractor Registration (CCR) by the individual, who creates his/her User ID and password. This system is managed by General Services Administration (GSA) and a component of the Integrated Acquisition Environment (IAE) controlled by the U.S. Department of Defense (DOD). The Internal Revenue Services (IRS) provides the applicant's/company's tax return information. The applicant's information in the CCR is uploaded, via automation, within 72 hours to the SBA's 8(a) certification system/BDMIS. A profile is then put together in the SBA's General Login System (GLS) by the individual, who creates his/her User ID and is issued a temporary password. Subsequent information required for certification in the 8(a) Business Development Program is electronically submitted by the applicant once he/she accesses the GLS and changes the temporary password to a new one that only he/she has privy of. Upon completion of all required electronic forms, the applicant is prompted to print, sign and date these standard forms and mail them to the appropriate SBA Processing Center, along with their supporting documentation. Applicants and 8(a) firms are not mandated to submit an electronic application or annual update. "Hard-copy" applications/annual updates are input into the system by SBA personnel. SBA personnel will review this information and reflect notes/recommendation in the system. Firms certified into the 8(a) Program use this system to complete standard forms, including Annual Update (Form 1450) in order to be considered for continued participation in the Program. Upon completion of all required electronic forms the 8(a) firm is prompted to print, sign and dated the standard forms and mail them to the SBA District Office that services that firm. SBA personnel will review this information and reflect notes/recommendation in the system. The following information is collected from the public: Name, Date of Birth, Address, Tax ID Number, Social Security Number, Employee Identification Number, Email Address, Primary North American Industry Classification System Code (NAIC) Code, Date firm was established, Type of Business, 2 years Tax Information (Business & Personal), Ethnicity, Gender, DUNS, Business Legal Structure, Articles of Incorporation, Operating

Agreements, By-laws, Stockholder and Board Member Meeting Minutes, Partnership Agreements, Articles of Organization, Fictitious Business Name filing, bank signature cards/letters, Ownership Percentage, Net Worth, Owners Net Compensation, Business Revenues, Business Liabilities, and Business Assets, 8(a) and non-8(a) revenue, resumes, and information on noteholders. Proof of United States Citizenship is also required from applicants. This nightly feed of data is transmitted from BDMIS to the E 8(a) System at the SBA.

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

Yes. This information is collected from United States citizens who own small businesses and wish to obtain certification in the 8(a) Business Development Program of the U.S. Small Business Administration (SBA). For continued eligibility in the 8(a) Program, the information is obtained from individuals already certified in the program and reviewed annually by the SBA.

b. Is the information about employees?

No information from SBA employees is collected by BDMIS.

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

The 8(a) Business Development Program was established by Congress to assist small businesses that are unconditionally owned and controlled by one or more socially and economically disadvantaged individuals, who are of good character, citizens of the United States, and which demonstrates the potential for success. Individual(s) that claim disadvantaged status and firms used for participation can only participate one time, once approved into the program. Participation in this program lasts no longer than nine (9) years. The Business Development Management Information System (BDMIS) is a vehicle that allows these individuals to apply for certification in the 8(a) Business Development Program. Upon certification into the 8(a) Program, BDMIS is used by these individuals to submit Annual Updates to the SBA for review of continued eligibility and participation in the program. (See 13 CFR 124.1). As of October 3, 2008, firms wishing to certify as a Small Disadvantaged Business (SDB) can do so on a "self-certification" basis; which means they no longer need to submit an application to the Small Business Administration (SBA) for approval. As long as requirements for the SDB program are met, they may claim their business as such. Firms that are certified in the 8(a) Program are automatically deemed as Small Disadvantaged Businesses (SDB).

This electronic system is an initiative undertaken pursuant to the President's Management Agenda for E-Government, under the auspices of the Integrated Acquisition Environment (IAE). BDMIS supports the 8(a) Business Development Program, replacing systems with the Contractor Tracking System and consolidated their functionalities on a single platform. It automates key business processes that were previously manually-based. The system provides online form creation/processing, content management, as well as automated alert and email capabilities. Both small business owners and SBA personnel benefit due to the reduced submission and processing time.

3) Is the system in the development process?

No. This is in the operations and maintenance phase of the system development life cycle.

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

This technology investment (new or updated) will not affect existing privacy processes. The precursor system to BDMIS was built on the same technology platform, so privacy processes have not changed. SBA maintains and operates internal security controls and authentication. These security controls ensure that data is fully secured against unauthorized access and prevent the loss of confidentiality and integrity, as well as unauthorized modification or destruction of data. SBA also maintains internal management controls through periodic auditing from the Office of the Inspector General (OIG) and the Office of Program Review. Certification and Accreditation of the system is provided by the Chief of Information Office and includes a System Security Plan, Risk Assessment, and Security Test & Evaluation every three years for existing systems, or sooner if there is a major system change and the system is upgraded/enhanced as needed. Each 8(a) firm is assigned an SBA case number as an internal identifier. SBA employees are given access and roles such as “Business Opportunity Specialist,” “Assistant District Director,” “District Director,” “Associate Administrator for Certification & Eligibility,” etc. Data can also be retrieved by DUNS, Business name, EIN, Case Number, etc. The information is processed in a single hosted site, not on the premises of the SBA but rather at the contractor. Retention of the information provided is indefinite. Upon completion of the nine-year program participation term, all data relating to the participant is archived in BDMIS for an indefinite period. All information in BDMIS can be retrieved by the Developer upon request. No data is deleted therefore, there is no “retention” period.

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

§ 7(j), 8(a) and 8(d) of the Small Business Act of 1953 (Public Law 85536) as amended and as recorded in 13 CFR 124.

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

Access Controls

The controls operate at two levels. First, access to the system is limited by User ID and password, which keeps the general public from entering unauthorized areas in the system. Second, an individual with authority to access the system has his/her access limited to the roles defined in a profile tied to his/her specific User ID. Training on Privacy Act rules and prohibitions on the dissemination or use of nonpublic information is mandatory and ongoing for SBA staff and contractors. Agency network logon procedures mandate viewing and acknowledgement of a posted Privacy notice prior to entry. SBA Privacy Act System of Records defines routine uses of this information and serves as a control by defining acceptable uses.

SBA maintains Internal Management Controls through periodic auditing from the office of the Inspector General and the office of Program Review. Certification and Accreditation of the system is provided by the Chief Information Office and includes a System Security Plan, Risk Assessment, and Security Test & Evaluation every 3 years for existing systems, or sooner if there is a major system change and each instance the system is upgraded or enhanced.

Unauthorized Browsing of data by Authorized Users

Each user is required to have a role in the certification and/or annual review workflow, as well as an individual system profile. Access to data, screens functions and reports is a function of the user's role in the workflow and his/her individual profile. In addition, with the exception of executive level roles (such as System Administrator, Associate Administrator for Business Development, Assistant Administrator for Certification and Eligibility and the Business Opportunity Assistant), access to information for a given role is limited to a specific Office Code.

C. SYSTEM DATA

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

This information is collected from United States citizens, tribal entities, Alaska National Corporations, Native Hawaiian Organizations and Community Development Corporations who own small businesses and wish to obtain certification in the 8(a) Business Development Program of the SBA. For continued eligibility in the 8(a) Program, the information is obtained from individuals already certified in the program and reviewed annually by the SBA.

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?

The source is taken from United States citizens, tribal entities, Alaska National Corporations, Native Hawaiian Organizations and Community Development Corporations. The Central Contractor Registration (CCR) which allows them to create a User ID and Password. The applicant's information in the CCR is uploaded within 72 hours to the SBA's 8(a) certification system/BDMIS. Subsequent information required for certification in the 8(a) Business Development Program is electronically submitted by the applicant. There is no other source used for collecting information other than from individuals.

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

The initial data loaded by the applicant is to the Central Contractor Registration (CCR). This system is managed by General Services Administration (GSA) and a component of the Integrated Acquisition Environment (IAE) controlled by the U.S. Department of Defense (DOD). The Internal Revenue Services (IRS) provides the applicant's/company's tax return information.

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

None. All data is provided by private individuals and/or non-public sector entities.

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

Data is collected from the Central Contractor Registration (CCR). This system is managed by General Services Administration (GSA) and a component of the Integrated Acquisition Environment (IAE) controlled by the U.S. Department of Defense (DOD). The applicant's information in the CCR is uploaded, via automation, within 72 hours to the SBA's 8(a) certification system/BDMIS.

What information will be collected from the employee and the public?

Name, Date of Birth, Address, Tax ID Number, Social Security Number, Employee Identification Number, Email Address, Primary North American Industry Classification System Code (NAIC) Code, Date firm was established, Type of Business, 2 years Tax Information (Business & Personal), Ethnicity, Gender, DUNS, Business Legal Structure, Articles of Incorporation, Operating Agreements, By-laws, Stockholder and Board Member Meeting Minutes, Partnership Agreements, Articles of Organization, Fictitious Business Name filing, bank signature cards/letters, Ownership Percentage, Net Worth, Owners Net Compensation, Business Revenues, Business Liabilities, and Business Assets, 8(a) and non-8(a) revenue, resumes, and information on noteholders. Proof of United States Citizenship is also required from applicants.

3) Accuracy, Timeliness, and Reliability

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

Data received from the Central Contractor Registration (CCR) is subject to internal logic edits and error checks. Firms provide their Tax Identification Numbers (TIN) because agencies are required to have and include them on vouchers submitted for payment [31 U.S.C.7701(c)] and 31 U.S.C. 3325(d)]. The integrity of the data is pertinent therefore the Internal Revenue Service (IRS) is responsible for validating the TIN and Taxpayer Names. This is done prior to the firm having a valid profile in the CCR and prior to applying into the 8(a) Business Development Program. A February 2004 Government Accountability Office (GAO) report recommended that the Department of Defense and IRS consider a TIN matching program to ensure valid TINs in the CCR to aid in accurate information reporting, payment certification, and federal tax collection with respect to vendors. The SBA may also use the IRS's Form 4506-T to verify/compare financial reporting documents submitted by the firm. The electronic system/BDMIS requires applicants to sign and notarize the Authorization Form regarding data accuracy and submit with the application. 8(a) certified firms are required to sign/date form with the Annual Update. These individuals are subject to penalties under law if the information proves fraudulent.

b. How is data checked for completeness?

The data entry fields in BDMIS correspond to the actual fields in the required OMB-approved forms for applying for certification in the 8(a) Program. The data uploaded

from CCR contains logical edits and error checks that ensure completeness of data. The SBA system also contains logical edits and error checks that prevent incomplete submission of data in the application or annual review processes. The data is normally reviewed by multi-tiered SBA personnel (i.e., Specialist, Supervisor, District Director/Manager, Office of General Counsel).

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 (e.g., data models).

Accuracy and timelines of personal data is optimized by allowing applicants to correct the personal information they provide in the system until completion of the initial application for certification. They also have multiple opportunities to update and correct personal information later in the program, when entering data in the system for the Annual Review, which occurs on an annual basis for a period of 9 years. The individual may also request access to correct their information pursuant to the procedures outlined in the Privacy Act of 1974.

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

Data elements are described in detail and documented in the “8aSDB MIS Data Dictionary/BDMIS.”

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

The system poses minimal threat to public/employee privacy via the use of a secure web site and the authentication controls. The system uses the internet to capture information on companies/individuals. All authorized-related system interaction is protected by using secure encrypted communication (SSLv3 with 128-bit encryption) to ensure that system passwords cannot be detected by network intruders. SSL is the industry standard for secure network communications.

You may read more about our privacy and security activity by going to:
<http://www.sba.gov/privacysecurity/index.html>

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 8(a) Program Participation is based on eligibility and is included in the Small Business Act (Public Law 85536). Information submitted by applicants and 8(a) certified firms are required in order for the SBA to determine the applicant’s eligibility and approval and the 8(a) firm’s continued eligibility in the 8(a) Business Development Program.

2) Will the system derive new data or create previously unavailable data

The system does not derive new data or create previously unavailable data about an individual through aggregation from the information collected. All data fields are subject to query. With proper authority, data fields corresponding to specific data ranges may be downloaded to Excel spreadsheets for further analysis. A nightly feed of data is transmitted from BDMIS to the E 8(a) System at the SBA.

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

Not Applicable. As stated above, the system does not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

Not applicable.

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

Not applicable. No data is formally derived or aggregated.

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

Not applicable. No data is formally derived or aggregated.

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

Not applicable. No data is formally derived or aggregated.

8) 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.

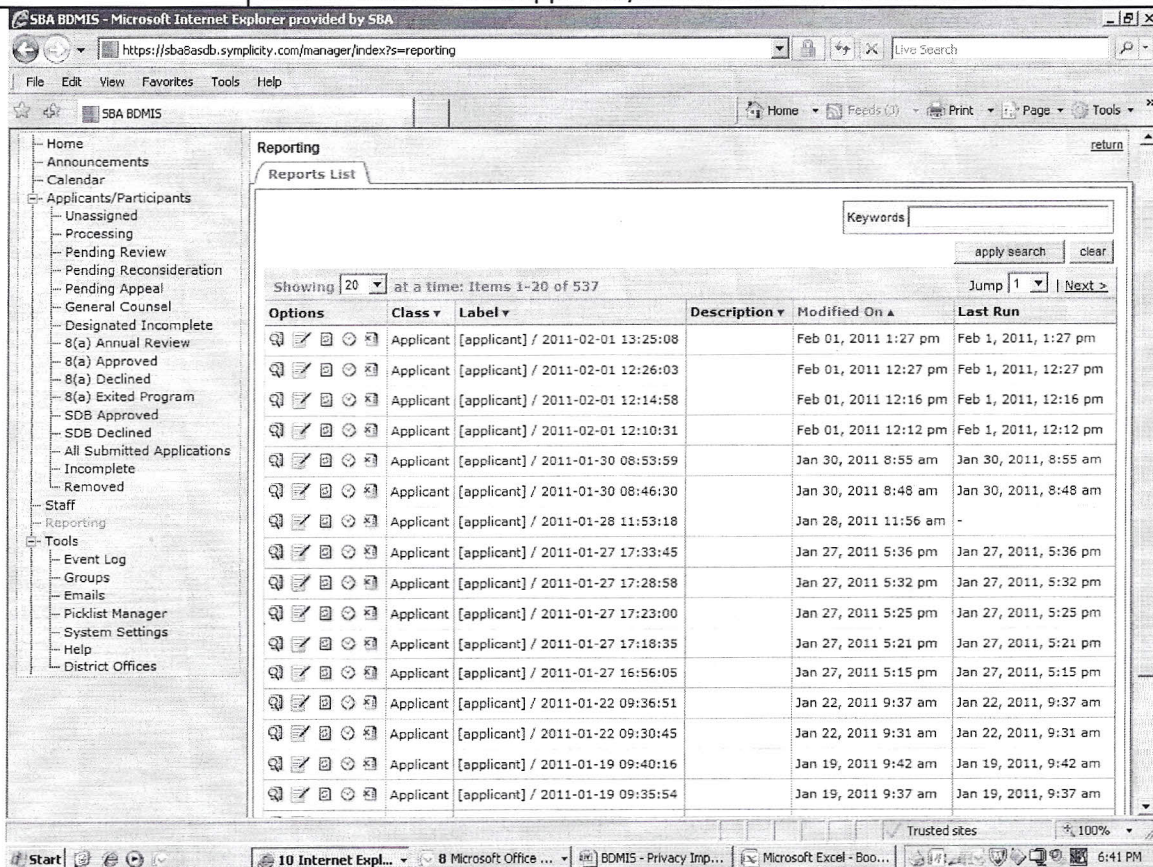
Not applicable. No data is formally derived or aggregated.

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

Reporting is ad hoc. There are no pre-defined or 'canned' reports. With full authority, any data element can be queried over any range and added to a report. Access to data for reporting purposes is restricted according to the role granted to the user (please see below). Also, below shows a list of the ad hoc reports created and stored in BDMIS.

ROLE	FUNCTION
System Administrator	Has full control of the application, for maintenance & security purposes
Assistant Administrator for BD	Makes the final determination on 8(a) applications
Assistant Administrator for CE	Makes final recommendation on 8(a) applications
CODS Chief	Supervisor of Central Office Duty Station/Processing Center

OCEBOS	Office of Certification & Eligibility Business Opportunity Specialist/Processing Center
CODS	General User responsible for assigning new applications to a BOS
OGC	Office of General Counsel/Examines & adds comments on legality of applications in question
OHA	Office of Hearing & Appeals/Reviews declined applications that requested an appeal
Field Office (8AFieldOffice)	Can view companies approved in the 8(a) Program
BDS	Business Development Specialist who performs an Annual Review on an 8(a) firm
ADD	Assistant District Director who approves/declines the recommendation of the BDS
DD	District Director who approves/declines the recommendation of the ADD



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

Individuals may decline to provide information or consent for particular uses of the information however, both are conditions for initial acceptance and/or continued eligibility in the SBA 8(a) Business Development Program. All information is provided on a voluntary basis by individuals. The information is not used for any other purpose than to evaluate the applicant for eligibility and 8(a) firm for continued participation, therefore, no consent for any other use is solicited.

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

§ 7(j), 8(a) and 8(d) of the Small Business Act of 1953 (Public Law 85536) as amended and as recorded in 13 CFR 124 identifies the regulatory requirements and govern the use of this information.

The system is in compliance with NIST 800-53A. The first layer of system security is provided by the General Login System (GLS), which ensures User ID and password protected access from the intranet and internet. The second layer of security is provided by complex roles described in Section 9 above. These procedures are documented in system documentation available on demand. In addition, all SBA employees and assigned contractor staff receive SBA-mandatory privacy training on the use and disclosure of personal data. They also receive appropriate security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on SBA security policies and procedures.

All government contractor personnel are vetted and approved access to the data center where the system is housed, issued picture badges, and given specific access to areas necessary to perform their job function. A Rules of Behavior document provides an overall guidance of how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees are required to read and sign a copy of the Rules of Behavior prior to getting access to any information technology (IT) system.

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?

Information is processed in a single-hosted site, hosted by the contractor and on the contractor's server.

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

Retention of the information provided is indefinite. Upon completion of the nine (9) year participation of the 8(a) Business Development Program term, all data relating to the participant is archived in the system for an indefinite period.

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?

The procedures for disposition of the data at the end of the retention period are outlined in Chapter 5 of SBA SOP 00 41 02, "Records Management Program," at this link:

<http://www.sba.gov/sops/0041/sop0041.pdf>

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

No. The system does not use technologies in ways that the SBA has not previously used. We are using the same methods.

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

This system poses minimal threat to public/employee privacy via the use of a secure web site and the authentication controls previously described.

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

Yes. As data is collected, and updated over a period of several years, for the purpose of original certification, and annual reviews. Each application/profile in the system is tracked via an "Action History" audit log that records all procedural actions that affect a particular firm's application/annual update forms.

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

BDMIS records all actions in the system, along with a User ID of the individual and the time/date of the action. Invalid login attempts are recorded and stored in the GLS security front-end, which is maintained by the SBA. Authentication and identification upon login are also controlled and tracked via the GLS security front-end.

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

Employees or contractors as assigned roles for accessing the system based on their function. Controls include a secure User ID and password specifically tied to the individual's personal information. In addition, SBA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. All personnel are trained on information security when they join the organization and periodically thereafter. The Information Systems Security Officer ensures compliance with policy and manages the activation or deactivation of accounts and privileges as required or when expired.

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

The BD Management Information System operates under Privacy Act 30 for the Servicing and Contracting System/Minority Enterprise Development Central Repository.

http://www.sba.gov/idc/groups/public/documents/sba_program_office/foia_sys_of_rec.pdf

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

No.

F. DATA ACCESS

1) Who will have access to the data in the system?

Contractors, Users, Managers, System Administrators, Developers, etc. have access to the data in the system. Users include the following: SBA Officials, the Office of Government Contractor and Business Development responsible for reviewing and approving/declining applications for participation in the SBA 8(a) Business Development Program, SBA Processing Centers (Division of Program & Eligibility) and other SBA HQ and SBA Field personnel.

The following are valid roles:

<u>ROLE</u>	<u>FUNCTION</u>
System Administrator	Has full control of the application, for maintenance & security purposes
Assistant Administrator for BD	Makes the final determination on 8(a) applications
Assistant Administrator for CE	Makes final recommendation on 8(a) applications
CODS Chief	Supervisor of Central Office Duty Station/Processing Center
OCEBOS	Office of Certification & Eligibility Business Opportunity Specialist/Processing Center
CODS	General User responsible for assigning new applications to a BOS
OGC	Office of General Counsel/Examines & adds comments on legality of applications in question
OHA	Office of Hearing & Appeals/Reviews declined applications that requested an appeal
Field Office (8AFieldOffice)	Can view companies approved in the 8(a) Program
BDS	Business Development Specialist who performs an Annual Review on an 8(a) firm
ADD	Assistant District Director who approves/declines the recommendation of the BDS
DD	District Director who approves/declines the recommendation of the ADD
Public	Applicants for the 8(a) Program
Public	Firms certified in the 8(a) Program
Contractors	Developers/Data Base Manager/Project Manager

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

Access is limited by the User's ID and Password controls. The system has predetermined access and roles/responsibilities for each User. Access is granted to screens, functions and reports based on the individual's role and responsibility in the processing and approval workflow. Access is provided by the SBA Office of IT Security upon receipt of documented authorization and approval of the individual's manager with specified authorization approval levels. Access is regulated via the General Log-in System (GLS). Access to data is restricted by the role and office code of the User in the system. Only System Administrators are authorized to assign and change roles.

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

Access is limited by the User's ID and Password controls. The system has predetermined access and roles/responsibilities for each User. Access is granted to screens, functions and reports based on the individual's role and responsibility in the processing and approval workflow. Access is provided by the SBA Office of IT Security upon receipt of documented authorization and approval of the individual's manager with specified authorization approval levels. Access is regulated via the General Log-in System (GLS). Access to data is restricted by the role and office code of the User in the system. Only System Administrators are authorized to assign and change roles.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

The controls operate at two levels. First, access to the system is limited by the User ID and password; which keeps the mass of unauthorized individuals from entering the system. Second, an individual with authority to access the system has his/her access limited to the Roles defined in a profile "married" to his/her specific User ID. Training on Privacy Act rules and prohibitions on the dissemination or use of nonpublic information is mandatory and ongoing for SBA personnel and contractors. Agency network logon procedures mandate viewing and acknowledgement of a posted Privacy notice prior to entry. SBA Privacy Act System of Records defines routine use(s) of this information and serves as a control by defining acceptable uses.

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, clauses are inserted into the contracts that protect privacy and other sensitive data.

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

A nightly feed of data is transmitted from BDMIS to the E 8(a) System at the SBA. The data feeds certain fields in the latter system, which serves as a repository of data about firm in the Annual Review process.

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

The SBA's System Administrator and Systems Manager are responsible for protecting the privacy rights of the public and employees affected by this interface.

8) Will other agencies share data or have access to the data in this system via transferred or transmitted (Federal, State, and Local, Other (e.g., Tribal))?

The Form 4506-T, Request for Transcript of Tax Return, is completed by the applicant/8(a) firm and may be sent by the SBA to the Internal Revenue Service (IRS) to request information about the applicant/8(a) firm/individual.

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

Please see response above (#8). The data in the form is used by the IRS to provide a transcript of the applicant's/8(a) firm's Federal tax return to the SBA.

10) What procedures are in place for assuring proper use of the shared data?

The electronic 4506-T form and the data it contains is maintained in BDMIS for an indefinite period of time, and is secured by the processes and procedures for data security outlined in this document and the current approved System Security Plan for BDMIS, on file with the Office of Chief Information Officer (OCIO). Paper copies of the 4506-T for the firms in the 8(a) Program are maintained in secured and locked premises at the various SBA District Offices across the United States. The IRS maintains among the highest standards of information privacy and security in the United States Government, given the sensitivity of the data it collects.

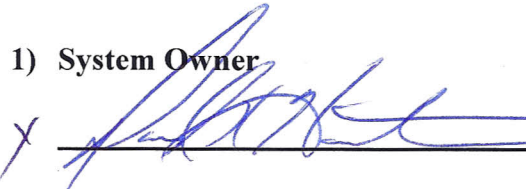
11) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for information shared internal and external.

The Form 4506-T requires the individual to reflect personal data on the forms (i.e., social security number, address, telephone number, etc.). The form is not downloaded/updated into BDMIS; however, paper copies of the 4506-T for the firms in the 8(a) Program are maintained in secured and locked premises at the various SBA District Offices across the United States. The IRS maintains among the highest standards of information privacy and security in the United States Government, given the sensitivity of the data it collects. Only authorized personnel with the SBA and the IRS have access to the individual's/firm's information on this form.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) System Owner

X  (Signature) 3/7/11 (Date)

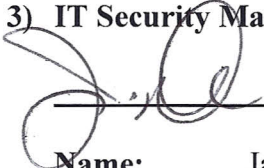
Name: Darryl K. Hairston
Title: Associate Administrator
Office of Business Development

2) Project Manager

 (Signature) 3-7-11 (Date)

Name: CaSandra L. Smith
Title: Program Analyst/Acting Project Manager
Office of Business Development

3) IT Security Manager

 (Signature) 3-8-11 (Date)

Name: Ja'Nelle Devore
Title: Chief Information Security Officer
Office of Chief Information Security Officer

4) Chief Privacy Officer

 (Signature) 3-9-11 (Date)

Name: Paul Christy
Title: Chief Privacy Officer
Office of the Chief Information Officer