Privacy Impact Assessment
for the
Business Development Management Information System
(BDMIS)

Office of Business Development
US Small Business Administration

June 18, 2008

System Owner
Calvin Jenkins, Deputy, GCBD, SBA
202-205-6459
Calvin.Jenkins@sba.gov

System Manager
Joseph Loddo, Director, Office of Business Development, SBA
202-205-5852
Joseph.Loddo@sba.gov

Contact Point
Larry Gottlieb, Project Manager, Office of Business Development, SBA
202-205-6032
Lawrence.Gottlieb@sba.gov

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

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

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

Table of Contents

Abstract

The Office of Business Development (OBD) of the US Small Business Administration (SBA) is upgrading the Business Development Management Information System (BDMIS). This system is used to collect information from US Citizens applying for certification in the 8(a) Business Development Program, or the Small Disadvantaged Business Program. Both programs are designed to provide assistance to socially and economically disadvantaged small business owners in the United States. For a given 8(a) certified firm, an Annual Review is also conducted via the same system for a period of nine years, to ensure that the firm meets the criteria for continued participation in the program. Certification via this system involves the collection of the following personal information from the applicant: Business Owners Name, Birth Date, Address, Tax ID Number, SSN, EIN, Email Address, Primary North American Industry Classification Code (NAIC), Date Firm Established, Type of Business, Three Years Business Income Tax Records, Two Years Personal Business Income Tax Records, Owner Ethnicity, Gender, Duns Number, Business Legal Structure, Articles of Incorporation, Operating Agreement, By-laws, Stockholder and Board Member Meeting Minutes, Partnership Agreement, Articles of Organization, Fictitious Business Name filing, and bank signature cards, Business Ownership Percentage, Personal Net Worth, Personal Assets and Liabilities, Owners Net Compensation, Business Revenues, Business Assets and Liabilities, proof of US Citizenship, personal Resume, including the education, technical training and business and employment experience (employer's name, dates of employment and nature of employment), including the individual's current duties within the applicant firm. Names and addresses of any noteholders (e.g., loans from banks or any other parties) are also required. For the Annual Review, the data collected includes changes to any of the above information, as well as rolling three years revenue data derived from their business attributed to 8(a) and non-8(a) contract sources.

Because the BDMIS collects personally identifiable information (PII) on members of the public, OBD is conducting this Privacy Impact Assessment (PIA) in accordance with the statutory requirements of the E-Government Act of 2002.

Introduction

The 8(a) SDB Certification process and related federal statute(s) were established by Congress to assist American citizens who own small businesses and belong to certain designated groups considered socially and economically disadvantaged. This assistance is intended to help these individuals overcome deeply entrenched social and economic obstacles to their success by providing limited preference in the federal procurement process. The 8(a) SDB Certification process is the vehicle that allows individual small business owners to obtain eligibility for this preference. The eligibility lasts nine years, during which time an Annual Review process is carried out by the SBA to ensure that the applicant meets the statutory and regulatory criteria for continued participation in the program. It involves the same individuals, data and related security issues.

The BDMIS, which automates the 8(a) SDB Certification and 8(a) Annual Review processes, is an initiative undertaken pursuant to the President's Management Agenda for E Government, under the auspices of the Integrated Acquisition Environment (IAE). The BDMIS supports the 8(a) Business Development Program and the Small Disadvantage Business programs. This system automates key business processes that are currently manual and hard-copy based. It provides online form creation and processing, content management, as well as automated alert and email capabilities. Small Business owners benefit from the BDMIS via reduced processing time and faster approval rates. The SBA benefits from labor productivity improvements which allow resources to be redeployed to areas requiring additional attention.

Section 1.0 Information collected and maintained

1.1 What information is to be collected?

For initial certification in the 8(a) or SDB program:
Owners Name, Birth Date, Address, Tax ID Number, SSN, EIN, Email Address, Primary North American Industry Classification Code (NAIC), Date Firm Established, Type of Business, Three Years Business Income Tax Records, Two Years Personal Business Income Tax Records, Owner Ethnicity, Gender, Duns Number, Business Legal Structure, Articles of Incorporation, Operating Agreement, By-laws, Stockholder and Board Member Meeting Minutes, Partnership Agreement, Articles of Organization, Fictitious Business Name filing, and bank signature cards, Business Ownership Percentage, Personal Net Worth, Personal Assets and Liabilities, Owners Net Compensation, Business Revenues, Business Assets and Liabilities and proof of US Citizenship. Personal Resume, including the education, technical training and business and employment experience (employer's name, dates of employment and nature of employment), including the individual's current duties within the applicant firm. Names and addresses of any noteholders (e.g., loans from banks or any other parties) are also required.

For continuing eligibility in the 8(a) program (i.e., the Annual Review): For a period of nine years, any changes to the above data, as well as rolling three years revenue data derived from their business attributed to 8(a) and non-8(a) contract sources.

1.2 From whom is information collected?

This information is collected from US citizens who own small businesses, and wish to obtain certification in the 8(a) Business Development Program or Small Disadvantaged Business Program of the US Small Business Administration. 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.

1.3 Why is the information being collected?

The information is needed to establish proof of eligibility for certification and continued eligibility in the 8(a) and SDB programs. The programs are limited to individuals who

can prove that they are disadvantaged based on economic, social and ethnic criteria set out in the applicable statutes and regulations.

1.4 How is the information collected?

Information is collected in two systems:

The Central Contractor Registry (CCR). This system is managed by GSA and a component of the Integrated Acquisition Environment that is controlled by the U.S. Department of Defense. Central Contractor Registration (CCR) is the primary contractor registrant database for the U.S. Federal Government. CCR collects, validates, stores and disseminates data in support of agency acquisition missions. According to the FAR 4.11, prospective vendors must be registered in CCR prior to the award of a contract; basic agreement, basic ordering agreement, or blanket purchase agreement

The 8(a) SDB Application/Certification System: This system was developed by the SBA Office of Business Development to enable the public to apply for certification to the 8(a) and SDB programs.

Initial information is loaded by the applicant into to the Central Contractor Registry (CCR) and uploaded within 72 hours to the 8a certification system. The applicant is then provided a Transaction Personal Identification Number (TPIN), which enables him/her to enter the 8(a) SDB Application/Certification System via the SBA General Login System (GLS). The latter manages user access to all mainstream SBA applications. All subsequent information required for certification required by the 8a/SDB certification system is provided directly by the applicants with one exception: the applicants are required to sign and submit forms that request copies from the IRS of federal tax returns for the last three years. These copies are forwarded directly from the IRS to the Office of Business Development of the SBA.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

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

1.6 Privacy Impact Analysis

Unauthorized Access to Data

All SBA employees are required to obtain a Public Trust Security Clearance (see OPM Form 85P for details), which includes an exhaustive background check conducted by specialized professionals. Direct access to the system is limited by User ID's and password controls managed via the SBA's General Login System. Access via GLS is provided by the SBA Office of IT security upon receipt of a written request by the user and duly approved by an authorized SBA manager. Further access to data, once the user is admitted to the system, is regulated via access roles and profiles associated with each User ID.

Unauthorized Browsing of data by Authorized Users

Each user is required to have a role in the certification and/or annual review workflow (Roles are defined below in Section 8.1 below), 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.

Downloading Data from System

The system produces an excel extract on demand of any data fields in the system. Access is limited to specific office codes according to role and subject to all the restrictions listed above. After use, any downloaded data is stored on hard-drives in SBA-configured PC's that are password protected, according to SBA standards, and/or in locked file cabinets. Only authorized individuals have keys to these file cabinets. These procedures comply with SOP 90 47, to ensure that data is secured after download.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

The information is used to determine initial eligibility in the 8(a) Business Development Program or Small Disadvantaged Business Program. Eligibility is based on proof that the majority firm owner, usually the applicant, belongs to a predetermined group that historically has suffered certain social and /or economic disadvantages. In addition, the applicant must not possess more than a certain threshold level of income, assets and adjusted net worth. This information is verified by the SBA via access to and review of the personal and business income tax records of the applicant. The firm must be a going concern with potential for success, which can only be verified by analysis of the firm's audited financial statements for a specified number of years. Any business loans to the applicant or the firm in question are also scrutinized. Finally, proof of birth in the US or naturalization is also required to establish US Citizenship of the applicant, as the latter is a requirement for participation in either program.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

The system offers no formal analysis tools to the user. With the proper authority, data fields corresponding to specific date ranges may be downloaded to Excel spreadsheets for further analysis. After use, any downloaded data is stored on hard-drives in SBA-configured PC's that are password protected, according to SBA standards, and/or in locked file

cabinets. Only authorized individuals have keys to these file cabinets. These procedures comply with SOP 90 47, to ensure that data is secured after download.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The data also is reviewed by a trained and qualified SBA/BD Business Opportunity Specialist for completeness and accuracy. A checklist is used to ensure completeness. If there is any omission, a request for the missing information is sent via email or regular mail to the applicant.

Extensive supporting documentation is required from the applicant to substantiate virtually all information collected by the system. Analysts at the SBA use this documentation to verify the data submitted by the applicant via the on-line forms. A subset of the supporting document is shown in Appendix A.

2.4 Privacy Impact Analysis

The controls operate at two levels. First, access to the system is limited by userid and password, which keeps the general public 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 tied to his/her specific userid. 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 three years for existing systems and each instance the system is upgraded or enhancement.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Retention of the information provided is indefinite. Upon completion of the nine-year program term, all data relating to the participant is archived in the system for an indefinite period.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The SBA does not yet have a record retention schedule approved by NARA for records pertaining to this program and must retain these records until such time as a schedule is approved.

3.3 Privacy Impact Analysis

To assist in their decision-making process, the SBA Administrator, Executive Branch and Congress frequently request reports based on historical trend analysis of the characteristics of individuals who participate in the 8(a) and SDB programs. This information is captured by the BDMIS, e.g., gender, ethnic breakdown, disadvantaged status, income, net worth, etc. These needs suggest that such information must be retained since inception of the programs.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

1. Office of the General Counsel (OGC)
2. Office of Hearings and Appeals (OHA)
3. Office of the Inspector General (OIG)

4.2 For each organization, what information is shared and for what purpose?

OGC is required to review automatically any application that is refused certification by the OBD, called a 'decline' in OBD parlance. OGC may uphold or reverse the decision by the OBD. In addition, the applicant in this case may appeal the OBD decision to OHA. OGC represents the SBA in the OHA appeals process. For either purpose, to review the OBD decision, or to represent the SBA in an appeal to OHA, OGC must have access to the full application and supporting documentation. In the case of an appeal, OHA also is given access to the application and supporting documentation. The Office of the Inspector General has general oversight responsibilities for the system, and, as such, requires access to a variety of data on an as-needed basis.

4.3 How is the information transmitted or disclosed?

'Office of General Counsel' is a valid role in the workflow defined in the system, and an attorney from this office is assigned this role. Thus, OGC can review the electronic application in the system, although a file with all the supporting documentation always accompanies the electronic application to the OGC. OHA does not have access to the data electronically, and can only receive information via email or hard-copy.

4.4 Privacy Impact Analysis

Information is shared within SBA among individuals who have a need for the information in the performance of their duties in accordance with the Privacy Act. Privacy protections include strict access controls such as personal security credentials (e.g., Public Trust Clearance or higher), userids and passwords managed via GLS, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors. Access to the hosted certification application (a.k.a.

'Symplicity') is strictly regulated via the General Log-in System of the SBA. Access is not allowed without a userid and password granted by IT Security of the SBA, and only through the GLS log-in front-end.

Section 5.0 External sharing and disclosure

5.1 With which external organizations is the information shared?

The 4506T form is filled out by the applicant and sent to the IRS for processing. This form is a 'Request for Transcript of Tax Return', and includes the following information about the applicant: name, spouse's name, both social security numbers, current address, name, address and telephone number of third party recipient of tax return (e.g., SBA).

5.2 What information is shared and for what purpose?

The form is sent to the IRS to obtain personal tax records for applicants, in order to confirm eligibility for the 8(a) or SDB program.

5.3 How is the information transmitted or disclosed?

The 4506T is sent via mail, by the applicant, to the IRS.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

No MOU exists.

5.5 How is the shared information secured by the recipient?

The IRS maintains among the highest standards of information privacy and security in the US Government, given the sensitivity of the information it collects.

5.6 What type of training is required for users from agencies outside the SBA prior to receiving access to the information?

No training of users outside SBA is required by the Office of Business Development. However, the Office of Business Development requires the information to be handled in accordance with the Privacy Act.

5.7 Privacy Impact Analysis

No privacy risks were identified, as the IRS is deemed to have one of the best protected data privacy and security environments in the US Government.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of

records notice published in the Federal Register Notice. If notice was not provided, why not?

The applicable Privacy Act Systems of Record is referenced on the home page of the system, via the following link:
http://www.sba.gov/aboutsba/sbaprograms/foia/papias/index.html

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Individuals may decline to provide information or withhold their consent for particular uses of the information, but both are conditions for initial acceptance and continuing eligibility in the SBA 8(a) and SDB Business Development Programs. All information is provided on a voluntary basis by the applicants. The information is used solely for the evaluation of the applicant for certification and/or continuing eligibility in the 8(a) or SDB programs, so no consent for any other use is solicited.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No such right is offered to the individual. All uses of the information obtained by the Office of Business Development are consistent with the Privacy Act and the applicable SORN.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, what privacy risks were identified?

None.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

The SBA does not require a special form in order to make a FOIA request. Requests for existing records must be in writing, handwritten or typed, and submitted via mail, fax or electronically. Requests may be sent to SBA program or field offices or to the FOI/PA Office/Requester Service Center, 409 Third St., S.W., Washington, D.C. 20416, or foia@sba.gov (online FOIA Requester Service Center).

7.2 What are the procedures for correcting erroneous information?

An individual may contest information maintained in the system that pertains to them by writing to the Office of Business Development, Assistant Administrator for Certification and Eligibility. The request must describe the nature of the error in the data and include any relevant supporting documentation. Individuals may also request correction of their personal information in this System of Records in accordance with the applicable provisions of the Privacy Act.

7.3 How are individuals notified of the procedures for correcting their information?

The publication of this PIA and of the applicable SORN serves to provide public notice of the collection, use, maintenance, and means of correcting this information.

7.4 If no redress is provided, are alternatives available?

Redress is provided.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided.

Risks to privacy have been minimized 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. Further, individuals may request access to or correction of their personal information pursuant to the procedures outlined in this PIA and in accordance with the Privacy Act.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Access to the system is defined by the role assigned to the individual user by the System Administrator. These roles include:

Access to data is restricted by the role and office code of the user in the system. Valid roles include the following:

- System Administrator (ADM): Full control of the application, for maintenance and security purposes
- Assistant Administrator for Business Development (AA/BD): This user makes the final eligibility determination on 8(a) applicants.
- Assistant Administrator for Certification and Eligibility (AA/CE): This user has 2 roles:
    - Make the final eligibility recommendation on 8(a) applicants.
    - Make the final eligibility determination on SDB applicants. .
- Office of Certification and Eligibility BOS (OCEBOS): This user reviews the 8(a) applicant's information to ensure completeness. If necessary, he procures fingerprint cards for criminal background checks, and other various forms from the applicant, before making an initial recommendation the application's eligibility.
- Business Opportunity Specialist (BOS): This is the SDB version of the OCEBOS role.

- CODS Chief (CC): This role is responsible for assigning new 8(a) applications to the OCEBOS
- Central Office Duty Station (CODS) General User (CG): The general user is responsible for assigning new SDB applications to a BOS.
- Office of the General Counsel (OGC): This user examines the legality of any applications in question, and provides an additional recommendation on whether or not they qualify for certification.
- Office of Hearing and Appeals (OHA): This user reviews applications which receive an initial decline and a decline after reconsideration who request an appeal within the appropriate time frame.
- Field Office (8ASDBFieldOffice): This is a local office user who can see approved 8(a) applications located in their district, but nothing else and they have no workflow role.
- Business Opportunity Assistant: This role allows administrative staff to assist the CODS CG and CC by assigning applications to the BOS or OCEBOS.

8.2 Will contractors to SBA have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes, contractors are involved in the design, development, and maintenance of the system. Contractors are required to pass a rigorous background check and Security Clearance before gaining access to third party personal data (sample contract clause is included below):

SECURITY REGULATIONS

Agency security regulations as well as the Federal Privacy Act of 1974 govern data contained within all SBA computer systems. Contractor personnel assigned to this project will be held accountable for adherence to these regulations.

The work to be performed is unclassified, but may involve data which is restricted under the Privacy and Freedom of Information Acts. However, as a condition for access to government-owned systems and data, contractor personnel must pass background investigations in accordance with OMB Circular A-130, which requires screening of all individuals involved with sensitive applications or data in Federal automated information systems. All SBA automated systems and data are considered sensitive.

The SBA or its designated representative will perform background investigations. Contractor personnel, depending upon the labor category, will be subjected to one of the following background investigations:

National Agency Check and Inquiries (NACI) which consists of:

- *searches of the OPM Security/Suitability Investigations Index (SII)*
- *searches of the Defense Clearance and Investigations Index*
- *searches of the FBI Identification Division, fingerprint charts and FBI records Management Division files and*

- *written inquiries and record searches covering specific areas of a subject's background during the past 5 years.*

Minimum Background Investigation (MBI) which consists of:

- *National Agency Check and Inquiries (above)*
- *Personal Subject Interview and*
- *Credit search*

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, these are defined in Section 8.1 above.

8.4 What procedures are in place to determine which users may access the system and are they documented?

As noted above, the first layer of system security is provided by GLS, which ensures userid and password protected access from the intranet and internet. The second layer of security is provided by the complex role structure, described in Section 8.1 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 and 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 IT system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Employees or contractors are assigned roles for accessing the system based on their function. 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.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

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 three years for existing systems and each instance the system is upgraded or enhancement.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All SBA employees and contractors are required to complete on-line Privacy Training, which includes instructions on handling PII in accordance with the Privacy Act. Compliance with this requirement is audited monthly by the SBA Privacy Officer.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Information in the BDMIS is safeguarded in accordance with the FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. The

Business Development Management Information System (BDMIS) has been certified in accordance with the Small Business Administration's Certification and Accreditation Program. This C&A is provisional, pending migration of the system from a hosted environment to the SBA premises, scheduled to occur in the June-July 2008 timeframe.

8.9 Privacy Impact Analysis

Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled at a high-security facility in Ashburn, VA. This access is regulated by a 24-hour manned security desk at the entrance to verify photo IDs, reinforced doors that respond only to positive identification via magnetic proximity badges, and 24-hour video surveillance of the entire facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The system is a hybrid of COTS and customized program code. The COTS portion is composed of proprietary program development objects called 'Symple Objects'. The owner of these components, Symplicity Corporation, customized them to create the BDMIS system. Other components include the standard programming language PHP, the standard database platform MySQL, and the Linux operating system.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Security and privacy requirements were analyzed based on FIPS-199 methodology. FIPS-199 methodology categorizes a system as High, Medium, or Low, depending on how important the function is to the agency. The result of that analysis was that the system was rated MODERATE for data integrity and confidentiality, and LOW for availability. All security controls are applied in accordance with this rating.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, the Office of Business Development limited its data collection to specific elements necessary to confirm eligibility for participation in the 8(a) and SDB programs. All initial access to the system is managed by the General Login System of the SBA, which meets all applicable statutory and regulatory conventions for data security and privacy. Once admitted to the system, user access is restricted to the information defined by the specific role assigned to the user. All access and transactions in the system are posted to an audit log, and any infractions of information security rules will be addressed appropriately. All SBA and assigned contractor staff receive SBA-mandated privacy training on the use and disclosure of personal data. The procedures and

Privacy Assessment for BDMIS

Responsible Officials - Approval Signature Page

The Following Officials Have Approved This Document

1) System Manager

Sheila D. Thomas (Signature) 6/20/08 (Date)

BOR Name: Joseph Loddo
Title: Director, Office of Business Development, SBA

2) System Owner

_____ (Signature) 6/20/08 (Date)

Name: Calvin Jenkins
Title: Deputy, GCBD, SBA

2) Privacy Official

for _____ (Signature) 6/25/08 (Date)

Name: Christine H. Liu
Title: Chief Information Officer and Chief Privacy Officer, SBA

6/18/08

APPENDIX A : Sample of Supporting Documentation Required for 8(a) or SDB Certification

- Articles of Incorporation filed with the state
- By-laws, including all amendments
- Minutes of all shareholders' meetings for

the past two years,
especially minutes of annual meetings involving
the election Directors

- Minutes of Board of Directors' meeting for the

past two years,
especially minutes of annual meetings involving
the election of Officers

- Stock certificates (front and back)
- The stock register
- Any stock option plans
- Any buy/sell agreements
- Any voting agreements
- A certificate of good standing in the state of

incorporation

- If the firm is not operating in the state of

incorporation,
a certificate to operate as a foreign corporation
(certificate of authority)
and a certificate of good standing in the state
of operation

The following Individual Tax Documents are Required:
Signed copies of personal Federal tax returns for
The two years preceding date of application,
Including all W-2 forms, schedules and attachments. A signed IRS Form 4506T must also be included. If any tax return reflects a Federal Tax liability, the taxpayer must provide SBA with copies of cancelled checks for full payment of the tax liability or a copy of a repayment plan signed by the IRS along with evidence that all payments under the plan are current.

These documents are required from:

- Each individual upon whom disadvantaged eligibility

is based

- Each general partner
- Each management member
- Each officer
- Each director
- Each owner of more than 10 percent of the stock of the applicant concern
- Any spouse of the above, if above is married and

filing separately

The following Business Tax Documents are Required:

- If firm is a Sole Proprietorship, owner must submit

Copies of Schedule C from his/her personal tax returns
For the three years preceding the date of application

- If the applicant is organized as a partnership, corporation

or LLC, it must submit copies of business Federal tax returns
filed for the three years preceding the date of application,
including all schedules and other attachments.

- IRS Form 4506T for the firm and any affiliated firms

Business Financial Statements. The applicant must
submit a copy of the last three fiscal year-end balance
sheets and income statements as well as an interim financial
statement (no older than 90 days prior to the submission of
the application), including a balance sheet and an income
statement with an aging of accounts receivable and accounts
payable. Extraordinary items must be explained.

- A brief narrative describing the history and description of the business.
- ***FORM 1010c: Business Plan***
- A resume for all individuals claiming disadvantaged status, each officer, each director,

each key employee and each owner of more than 10 percent of the stock of the applicant concern.

- Information from the applicant firm's bank or other financial institution to document any available line of credit

or other financing arrangements (long or short term) plus complete copies of any loan agreement(s), including any shareholder,
officer or partner loans and/or inter-company loans.

- Copies of signature cards for all business bank accounts, or a letter from the bank indicating who has signature

authority and how many signatures are required to transact business as well as any limitations placed on the account.

- For construction firms, a statement of the single and aggregate bonding limit from the firm's surety, if applicable.
- Copies of any licenses required to conduct business, including state and local business licenses (as required by law)

and other special licenses, such as Contractor's, CPA, professional engineer, etc.

- Information regarding any affiliates, including all information necessary to determine size, such as tax returns showing

the affiliate's receipts for the past three fiscal years and/or the numbers of employees on the most recent company payroll records.

- Any applicant owned by a trust must submit a copy of the trust agreement. The trust agreement must specify whether or

not the trust is revocable and identify the grantor(s), trustee(s), and current beneficiary(ies).

- If waiving the 2-year rule, copies of contracts or invoices demonstrating performance of work in the industry for which

the applicant seeks 8(a) certification.

- A narrative statement of economic disadvantage from any individual claiming disadvantaged status. The statement

must reflect how their ability to compete in the free enterprise system has been impaired due to discriminatory practices against
them due to their identification as a member of a designated group.

- If the individual is not a member of a group designated by SBA as socially disadvantaged and claims disadvantaged status,

a narrative statement of social disadvantage. The statement must demonstrate social disadvantage by a preponderance of
evidence. .

- If an individual claiming disadvantaged status is a foreign born national, evidence of U.S. citizenship, such as a U.S.

passport or naturalization papers.

- If any sole proprietor, partner, management member, officer, director, or holder of more than a 10 percent ownership interest

in the applicant, or a household member, is an employee of the federal government holding a position of GS-13 or above,
that individual must submit a letter of no objection from his or her employer.

- A Statement of Bonding limit from the firm's surety, if applicable
- A detailed explanation, including supporting documentation, for each "yes" response to questions in Section I
- A detailed explanation, including supporting documentation for each "Yes" response to questions in Section II
- A detailed explanation, including supporting documentation for each "Yes" response to questions in Section III