Privacy Impact Assessment

Name of System/Application: **Technical ResourceNetwork (Tech-Net)**

Program Office: **Office of Technology**

A. CONTACT INFORMATION

1) Who is the person completing this document?

Lisa Younger
Program Analyst
Office of Technology
(202) 205-6450
lisa.younger@sba.gov

2) Who is the system owner?

Edsel Brown
Associate Administrator Office of Technology
(202)-205-6513
edsel.brown@sba.gov

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

Lisa Younger
Program Analyst
Office of Technology
(202) 205-6450
lisa.younger@sba.gov

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

Ja'Nelle L. DeVore
Chief Information Security Officer
Office of the Chief Information Officer
(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
Office of the Chief Information Officer
(202) 205-7173
ethel.matthews@sba.gov

6) Who is the Reviewing Official?

Paul Christy
Chief Information Officer and Chief Privacy Officer
Office of the Chief Information Officer
(202) 205-6756
Paul.christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

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

The data for Tech-Net includes information about individuals. SBA receives the name of a business official, Principal Investigator, and for Small Business Technology Transfer Awards (STTR), a research institution official. For each of the three categories, SBA asks participating agencies to provide the individuals name, title, phone number, and e-mail address.

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

b. Is the information about employees? Yes

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

SBIR.gov is the primary website for the U.S. Small Business Administration's SBIR and STTR programs. SBIR stands for Small Business Innovation Research and STTR stands for Small Business Technology Transfer Research. The Small Business Innovation Research (SBIR), Small Business Technology Transfer (STTR), and Advanced Technology Program (ATP) are federal grants programs. Rather than loan money to a small business, money is awarded to a small business. The distributing agencies are seeking either the research-benefit results or actual new technologies.

The latest TECH-Net iteration supported award data collection changes. This included the following:

- Limit award data collection and commercialization data either to eXtensible Markup Language (XML) or to web-based screen input.
- Provide additional Phase I and Phase II award tracking functionality.
- Require Phase I award data and commercialization data collection before Phase II award data collection.
- Support Phase II awards going to multiple agencies.
- Restrict which agency has update and viewing rights to commercialization data.
- Maintain audit trails for award data and commercialization data collection

3) Is the system in the development process? Yes

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

The TECH-net technology will not affect existing privacy processes.

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

Public Law 106-554106th Congress "An Act" authorized SBA to develop and Maintain a database of SBIR and STTR awards. This database must be searchable, up-to-date, and available to the public.

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

- Existing privacy issues will not be affected by the SBIR TECH-Net since all data is housed within the system. Access controls are in place for staff that has administrative and supervisory rights to the system.
- This will be a public site and will not hold any individual's records.
- All the sources are coming from 11 government agencies that participated in the SBIR/STTR program. There is no data coming from individuals.
- SBIR TECH-Net maintains basic contact information for individuals associated with small business awardees.
- The TECH-Net database may store a SSN number in certain cases where a small business does not have a EIN/TIN number, and owner of the small business provides there SSN as the identifier. The TECH-Net system does not display the EIN/TIN field in any cases, as a precaution against unauthorized SSN disclosure.

The SBIR TECH-Net system is configured with the security controls consistent with a Moderate FISMA security categorization. This includes building the system consistent with SBA Secure Baseline Configuration Standards, and CIS benchmarks. In instances were data is stored-at-rest (system backups), encryption is used. Within the TECH-Net application, role-based access controls are implemented to ensure least-privilege access rights throughout system.

C. SYSTEM DATA

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

The data in the Tech-Net system contains information about awards made to small businesses through the SBIR and STTR programs. This includes information about individuals who are business contact officials, principal investigators, or research institution officials who are associated with the research effort. The information collected about these individual includes name, title, phone number and, email address. SBA collects from the participating agencies the number of employees of each awardee, if available. The Tech-Net database also stores information about whether business is woman-owned or owned by individuals who are socially and economically disadvantaged. A field in Tech-Net is "EIN/TIN." This information is not available to the public because it could contain SSN information if the award was made to a sole proprietorship and is submitted by participating agencies.

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 Federal agencies that award SBIR and STTR grants or contracts are as follows: USDA, Department of Commerce, Department of Defense, Department of Energy, Department of Education, Department of Health and Human Services, Department of Transportation, Department of Homeland Security, the Environmental Protection Agency, NASA and the National Science Foundation. The agencies collect the data from the awardees and input it into Tech-Net.

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

(See response to 2(a) above)

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

None

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

None

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

The agencies will provide award information. The data that is specific to individuals includes business contact officials, principal investigators, or research institution officials who are associated with the research effort. The information collected about these individuals includes name, title, phone number and, e-mail address. SBA collects from the participating agencies the number of employees of each awardee, if available. The Tech-Net database also stores information about whether business is

woman-owned or owned by individuals who are socially and economically disadvantaged. A field in Tech-Net is "EIN/TIN." This information is not available to the public because it could contain SSN information if the award was made to a sole proprietorship.

3) Accuracy, Timeliness, and Reliability

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

The Federal agencies will verify the data prior to providing it to SBA. Public Laws 106-554 106th Congress "An Act" ,and 107-50 An Act to reauthorize the Small Business Technology Transfer Program require participating agencies to report information about the awards made through the SBIR and STTR programs. Those Public Laws also require SBA to maintain an electronic, searchable, and up-to-date database of all awards made through the two programs.

b. How is data checked for completeness?

Safeguards in the database and code prevent incomplete records from being added. All mandatory fields must be completed before record is accepted.

c. Is the data current?

- The record contains a last modified date
- Congress mandates that the agencies report 6 months after the close of the fiscal year
- SBIR staff will review data periodically
- Data is currently being entered through FY 2009

d. Are the data elements described in detail and documented?

The legislation governing the SBIR program and the STTR program, 106-554 and 107-50, respectively, describe the general requirements for the Tech-Net system. The SBIR and STTR Policy Directives also list what agencies are required to report to SBA

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

As stated in above in question 3(d), our data collection is mandated by legislation and does not allow for decreased changes in scope. Our database System Administrators have database logins and passwords and our Developers are restricted to access in Development only and the Public is restricted to view only.

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.

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

No.

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

N/A.

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

No.

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

N/A

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

N/A

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

N/A

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.

The system is searchable by a number of fields including company name, state, agency, and year of award. It is also possible to search the system by keywords. The keyword search capability allows for searches across all fields including business official, principal investigator, and research institution official. The system is not searchable by EIN/TIN.

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

No reports can be produced on individuals. Businesses profiled on the Tech-Net system contain information such as company name, state, agency, contract/grant award year, socially and economically disadvantaged ownership, woman ownership, etc. The keyword search capability allows for searches across all fields including business official, principal investigator, and research institution official. The default settings result in report out puts that report directly to the screen. Another setting for output is for the system to produce a tab delimited text file.

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.

N/A

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

Users who can access data for the purposes of changing it are limited by their login and associated group rights. The public may also search and view the records contained in the system. The search screens are designed to provide access to parts of the data for this purpose.

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?

One site only

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

Public Laws 106-554 and 107-50 require that SBA maintain a database of all awards made through the SBIR and STTR programs. The first year of awards for the SBIR program was 1983, and the first year of awards for the STTR program was 1994. Therefore, the records in Tech-Net date back to 1983 for SBIR and 1994 for STTR. The records are retained indefinitely to remain responsive to the two pertinent laws.

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 records in Tech-Net will be retained indefinitely in order to be responsive to the legislation governing each program. Tech-Net is designed to be a complete database of awards made through the SBIR and STTR programs.

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

No

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

N/A

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

The users have MySQL accounts. The database administrators can, if necessary, monitor the activity. Also, the web servers log all activity so information about people using the site is also captured. Also, the OCIO Security staff monitors activity across all SBA systems.

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

The Database Activity report captures user name, date and time of activity.

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

The system is protected by both an Intrusion Detection System (Symantec), to detect and protect against network based attacks, and system integrity software (Tripwire). In addition, vulnerability scans are regularly scheduled and analyzed to detect vulnerabilities in both the operating system and network (Nessus) as well as the web application (LANGuard). Anti-virus software is also deployed (Microsoft Forefront).

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

A name or other personal identifier is not used to retrieve information. Certain information may be protected from disclosure under the Freedom of Information Act.

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

N/A

F. DATA ACCESS

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

Users (Small Business), SBIR staff, participating agencies and System Administrators

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

Specific SBA employees with responsibility for Tech-Net and the SBIR and STTR programs can update the system.

Agency representatives are given access rights to update the awards that their agency makes. This process is done by requesting access in Tech-Net. Once the request has been made through the system, an email is sent to the SBA Tech-Net Security Administrator who approves or declines the access request. If the request is from a participating agency, the security administrator will verify that the requester is authorized to update awards on their behalf and access will be approved. If a request for access is made from anyone from other then a SBIR or STTR agency, the request will be declined.

Public can view all non privacy award information resident in Tech-Net.

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

Database System Administrators have database logins and passwords. Developers are restricted to access in Development Only. Public is restricted to view capability only. Agencies are restricted to their own portfolio. Office of Technology staff can view and update all records. Access to this part of the system requires a user name and password.

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)

Users who can access data for the purposes of changing it are limited by their login and associated group rights**.** The search screens are designed to provide access to parts of the data.

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?**

No

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

No

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

Office of Technology

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))?**

Agencies will have access to their own portfolio and can only view the awards made by another agency. The public may also search and view the records contained in the system.

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

The shared data is only available for viewing.

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

Users who can access data for the purposes of changing it are limited by their login and associated group rights**.** The search screens are designed to provide access to parts of the data.

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

The information in the Tech-Net database is for public use as mandated by Public Law 106-554 and requires no memorandum of understanding between participating agencies.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) **System Owner**

Edsel M Brown Jr. **(Signature)** 7/15/11 **(Date)**

Name: Edsel Brown

Title: Assistant Administrator Office of Technology

2) **Project Manager**

Lisa Younger **(Signature)** 7/15/11 **(Date)**

Name: Lisa Younger

Title: Program Analyst

3) **IT Security Manager**

J. DeVore **(Signature)** 7-25-11 **(Date)**

Name: Ja'Nelle L. DeVore

Title: Chief Information Security Officer

4) **Chief Privacy Officer**

(Signature) 8-1-11 **(Date)**

Name: Paul T. Christy

Title: Chief Information Officer