

Privacy Impact Assessment (PIA)



HUBZone Certification and Tracking System (HCTS)

Government Contracting and Business Development (GCBD)

HUBZone - Historically Under-served Business Zones

Grande H. Lum, Director, HUBZone Program

**U.S. Small Business Administration
409 Third Street, SW
Washington, DC 20416**

A. CONTACT INFORMATION

Guidance: Each listing should include the full name, title, SBA Office and program, SBA phone number and SBA e-mail.

- 1) **Who is the person completing this document?**
Stanley Y. Fujii, Federal Project Manager, GCBD, 202-619-0151,
Stanley.Fujii@sba.gov
- 2) **Who is the system owner?**
Grande Lum, Director, HUBZone Program, (202)205-6487,
Grande.Lum@sba.gov
- 3) **Who is the system manager for this system or application?**
Mariana Pardo, Deputy Director, HUBZone Program, 202-205-2985,
Mariana.Pardo@sba.gov
- 4) **Who is the Chief Information Security Officer who reviewed this document?**
Ja’Nelle DeVore, Chief Information Security Officer (CISO), (202) 205-7103,
Janelle.Devore@sba.gov
- 5) **Who is the Senior Advisor who reviewed this document?**
Ethel Matthews, Senior Privacy Advisor, Office of the Chief Information Officer
(OCIO), (202) 205-7173, Ethel.Matthews@sba.gov
- 6) **Who is the Reviewing Official?**
Paul Christy, Chief Information Officer (CIO), (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.

- a) **Is the information about individual members of the public?**

Yes. The online HCTS is auto-populated by applicant-entered data and from two (2) Federal data collection systems; DOD’s Central Contractor Registration (CCR) and the nested SBA’s Dynamic Small Business Search (DSBS).

The DOD CCR profile is available to the public via the Internet and queries can be run on specific fields. Information (e.g. company officials and financial data) is also applicant-entered into the HCTS.

For senior company officials, this will include business telephone numbers and

business e-mail addresses. The HUBZone-specific data are retained on a secure server that is only available to HUBZone personnel based on assigned security roles and levels of pre-approved access. None of the material collected exclusively by the HUBZone system is ever available to the public for review. We note that the subsystem, HUBZone Procurement Query and Reporting System (HPQRS) exists, however, this system does not contain any information identifiable to an individual that is unique or is not already in existence. That is, the system extracts public information from the FEDBIZOPPS database (notice to the public of what the government is buying) and when a requirement is identified and found suitable for a possible HUBZone set aside, the system allows attachment of HUBZone certified firm profiles already existing in another database, the public database of the Dynamic Small Business Search (DSBS) of the Central Contractor Registration (CCR).

b. Is the information about employees?

Yes, within the scope of that individual's role as an owner and/or Senior Official with the HUBZone applicant concern. Generally, it will include name, e-mail address and ownership interests in other concerns, and whether individual has ever been debarred from Federal contracting.

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

The HCTS system is a multi-level certification system that allows an interested party to apply for HUBZone status online, recertify online once every three years to continue eligibility and participate in randomly generated program examinations (formal SBA audits) that allow the Agency to confirm with documentation a firm's continuing eligibility.

3) Is the system in the development process?

No.

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

There is currently a plan for the modernization of the HCTS system. The current system will be retired and replaced with a completely new system.

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

The HUBZone Program was enacted into law as part of the Small Business Reauthorization Act of 1997 as amended. The program falls under the auspices of the U.S. Small Business Administration.

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

Identified risk - procedures are not in place to manage access controls for personnel who have transferred or terminated employment. This risk has been mitigated by a compensating control to review access requirements and manually remove access to personnel who have transferred or terminated employment

C. SYSTEM DATA

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

As part of the HUBZone certification process, the application form contains data fields requesting identification and e-mails addresses and outside ownership interests of the business owners, and senior company executives. SBA also asks for a point of contacts within the companies who can supply HUBZone application clarifications as needed.

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

The source of information is two-fold. The online HUBZone certification system is designed to 1) extract and 2) auto-populate into the appropriate HUBZone application fields pre-existing data already supplied by the applicant in two other Federal data collection systems, the DOD's Central Contractor Registration (CCR) and the nested SBA's Dynamic Small Business Search (DSBS). Where information is not already available (e.g. other senior company officials and a point of contact who can, as needed, clarify unclear entries in the application), the applicant is requested to insert this material into the data fields.

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?

Individual business owners provide information related to their eligibility for the HUBZone program.

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

As noted, the Department of Defense Central Contractor Registration (CCR) system provides data, although the information is filtered through the SBA's Dynamic Small Business Search (DSBS) and delivered to the HUBZone application as part of an electronic extraction process.

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 applicant will provide documentation supporting affiliation relationships, owners, financial and employment data, as well as legal structure.

3) Accuracy, Timeliness, and Reliability

The HCTS contains a verification process called the Electronic Verification System, in operation since 2002. Following the submission of an online application, the system sends the highest ranking official identified within that applicant concern a separate electronic communication. The highest ranking senior official is asked to verify whether the individual who submitted the online application is authorized to obligate the firm to the program's requirements. That same communication also contains a listing of the consequences facing a senior official who allows misstatements to be made during the HUBZone application process and makes available to the senior official an opportunity to review immediately the entire application submission for accuracy.

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

The applicant completes or updates their DUNS information. The applicant firm then completes their CCR and DSBS updates. The information in DUNS and CCR must match for the application to be able to apply for the HUBZone Program. The HCTS will pull the information from DSBS.

b. How is data checked for completeness?

The HUBZone application contains built-in logic that ensures all required data fields are filled out prior to final submission. In addition, each application is reviewed by a HUBZone analyst to verify that each field been filled out correctly and that any ambiguous entries are resolved either through clarification, withdrawal by the applicant or, in the most extreme cases, the denial of HUBZone status to the applicant concern.

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).

The material extracted from the CCR/DSBS combined database must, by rule, be updated at least once every 12 months and the information inserted into the remaining HUBZone specific fields are reviewed for currency by HUBZone analysts. Certified firms are required by regulation to also recertify their continuing eligibility once every three years.

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

If yes, what is the name of the document?

Yes, data elements are described in detail and documented in the "HUBZone Certification System Data Dictionary."

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

Transmission of the applicants supporting documentation, such as driver's licenses, payroll records and birth certificates are received over unsecure methods. There is currently no mitigation strategy in place to meet this finding but the HZ program is looking at the WOSBPR (Women-Owned Small Business Program Repository) as a means of providing a secure or encrypted method for applicants to upload into a secure environment.

D. DATA ATTRIBUTES

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

The data is relevant and necessary to establish eligibility for HUBZone Certification as stipulated in the Small Business Reauthorization Act of 1997 as amended.

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?

The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

Not applicable.

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.

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

Not applicable.

- 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".**

The security controls to protect the information from unauthorized access or use are pursuant to the A-120 circular and in accordance with SBA's policies and procedures. The HUBZone tracking system is a fully certified and accredited system by the SBA Office of the Chief Information Officer.

- 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.**

We do not retrieve data on an individual for any purpose. The clients fill out the HUBZone application seeking certification. They populate our application with information that indicates whether small business concerns are eligible and qualify for HUBZone certification or not. However, if we collect data for example based on a data collection survey, this information is reported collectively and not individually. The only circumstance where information could be reported using personal identifier information would be in the circumstance of a Freedom of Information Act request. And, in this circumstance the reporting of the information collected would be subject to Freedom of Information Act regulations and exemptions.

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

We do not retrieve data on an individual for any purpose. The clients fill out the HUBZone application seeking certification. They populate our application with information that indicates whether their small business concern is eligible and qualifies for HUBZone certification or not. The only circumstance where information could be reported using personal identifier information would be in the circumstance of a Freedom of Information Act request. And, in this circumstance the reporting of the information collected would be subject to Freedom of information Act regulations and exemptions.

- 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.**

We do not retrieve data on an individual for any purpose. The clients fill out the HUBZone application seeking certification. They populate our application with information that indicates whether they are eligible and qualify for HUBZone certification or not. The only circumstance where information could be reported using personal identifier information would be in the circumstance of a Freedom of Information Act request. And, in this circumstance the reporting of the information collected would be subject to Freedom of Information Act regulations and exemptions. Further, the Freedom of Information Act process would require that if the government was about to release information to another party regarding an individual who applied for HUBZone certification, the government would be required to seek the permission from the party whose information was being released before the Information could be released. Again this process would be restricted to Freedom of information Act rules and regulations.

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

Access to system controlled by user roles.

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 are maintained in all sites?

Not applicable, since the system is resident currently in only one location within SBA headquarters, in the Office of the Chief Information Officer (OCIO).

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

There is no limit on the retention of this electronic data since the current dataset is so small and is not approaching the upper storage limits of the HUBZone servers. In addition, firms are required to recertify their continuing eligibility each year, and each recertification is an extension of the initial application resident within the HUBZone database. The system is designed to accommodate this multi-year continuing eligibility option for several years into the future. Records are retained and archived according to Federal Regulations by the Management Support Specialist.

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?

At the present time, a small amount of data is now in the system that can be maintained within a secure environment. Discussions have been held, however, with SBA'S OCIO archive specialists to anticipate the time when we will have to develop a retention/disposition plan of action.

- 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.**

No, the system does not permit searches using personal identifiers.

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

None.

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

Security controls are in place to prevent unauthorized monitoring as stated in the SOP 90.47.2.

- 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; it is possible that the system is not a Privacy Act system. However, even though information may not fall under the Privacy Act's protection and requirements, 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?**

No.

F. DATA ACCESS

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

Access to the HUBZone Application Tracking System is limited to Federal employees of the HUBZone Program and the contractors hired specifically to review incoming files, and those contractors retained as HUBZone system developers.

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

Levels of authorized access to the secure HUBZone database server are pre-determined through role functions as defined in HUBZone Application Tracking System User's annual.

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

The Deputy Director of the HUBZone Program limits access by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to data and reports that are within the duties and needs of the user.

- 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)**

Agency Security Access Procedures - the Deputy Director of the HUBZone Program limits access by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to data and reports that are within the duties and needs of the user. Education of Agency and contractor staff regarding the Privacy Act rules and prohibitions on the dissemination or use of non-public information is mandatory and ongoing. System audit trails can be used to document suspicious or irregular logons and navigation of the system. Agency network logon procedures mandate a posted Privacy notice be viewed and acknowledged prior to entry.

- 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. Privacy Act contract clauses are inserted in their contract.

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

Not directly, data is pushed through a secure connection to Dynamic Small Business Search (DSBS) .

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

The Director for the HUBZone Program is identified as the security officer.

- 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))?**

No, there are currently no external connections to HCTS.

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

No.

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

N/A

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

Identified Risk - restricting user access. This risk has been mitigated by a compensating control - the Deputy Director of the HUBZone Program limits access by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to data and reports that are within the duties and needs of the user. No information is shared.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) System Owner

 _____ (Signature) 8/5/11 _____ (Date)

Name: Grande H. Lum

Title: Director, HUBZone Program

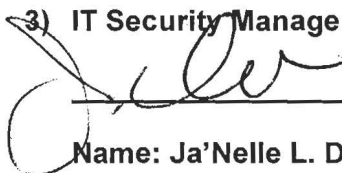
2) Project Manager

 _____ (Signature) 8/5/11 _____ (Date)

Name: Stanley Y. Fujii

Title: Lead Program Analyst, HUBZone Program

3) IT Security Manager

 _____ (Signature) Aug 12, 2011 _____ (Date)

Name: Ja'Nelle L. DeVore

Title: Chief Information Security Officer

4) Chief Privacy Officer

 _____ (Signature) 8-31-11 _____ (Date)

Name: Paul T. Christy

Title: Chief Information Officer\Chief Privacy Officer