PRIVACY IMPACT ASSESSMENT

U. S. Small Business Administration – LAN/WAN

FY 2011

Name of System/Application: LAN/WAN

Program Office: Office of the Chief Information Officer

A. CONTACT INFORMATION

1) Who is the person completing this document?

Sherry C. Hill
Director, Office of Communications Technology Services
(202) 205-6257,
Sherry.Hill@sba.gov

2) Who is the system owner?

Sherry C. Hill
Director, Office of Communications Technology Services
(202) 205-6257,
Sherry.Hill@sba.gov

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

a) Linda Terrell
Chief, Network Integration Branch
(202) 205-6247
Linda.Terrell@sba.gov

b) James Montrose
Information Technology Specialist, SBA Office of the CIO
(202) 205-6926
James.Montrose@sba.gov

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

Ja'Nelle DeVore
Chief Information Security Officer, SBA Office of the CIO
(202) 205-7103
Janelle.Devore@sba.gov

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

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

6) Who is the Reviewing Official?

Paul T. Christy
Chief Information Officer, SBA Office of the CIO
(202) 205-6708
Paul.Christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

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

There is the potential for Personally Identifiable Information (PII) to reside within the LAN/WAN, either as the result of being typed into the text of an e-mail message or attached to an e-mail message sent or received by an SBA employee or contractor, or by being downloaded from another system and saved by that system's user to his or her SBA-issued personal computer. Examples of records containing PII that could be stored or transmitted using the LAN/WAN include travel, payroll, time and attendance, and other agency personnel records containing PII pertaining to employees and contractors; agency program records containing PII pertaining to members of the public, and employees' and contractors' personal records (non-agency records).

Data Element	Collected or not Collected (Yes/No)
Name	**Yes** – collected by Active Directory
Social Security Account Number	**Yes –** Employees and contractors using the LAN/WAN potentially may use the e-mail system to transmit this information. However, all users are cautioned that transmission of a complete SSA Number is to be kept to the absolute minimum consistent with mission requirements and applicable policies.
SBA Telephone Number	**Yes** – collected by Active Directory
SBA E-mail address	**Yes** – collected by Active Directory
SBA Office Street address	**Yes** – collected by Active Directory
Financial data (i.e.: account numbers, tax ids, etc.)	**Yes –** Employees and contractors using the LAN/WAN might use the e-mail or other systems to transmit this information. Users are restricted by domain asset (servers, folders, etc) security rights and restrictions to this type of data. Users are cautioned that transmission of this type of information is to be kept to the absolute minimum consistent with mission requirements and applicable policies.
Health data (e.g.: Health Insurance Portability and Accountability Act – HIPAA)	**Yes –** Employees and contractors using the LAN/WAN potentially may use the e-mail system to transmit this information. However, all users are cautioned that transmission of this type of information is to be kept to the absolute minimum consistent with mission requirements and applicable policies.
Biometric data	**No –** This type of data is very unlikely to be transmitted

TABLE 1 – DATA ELEMENTS AND COLLECTION PARAMETERS

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

The potential for information about individual members of the public to be stored on the LAN/WAN exists. This information would be found in file captures and databases and possibly on desktop computers and servers.

b) Is the information about employees?

Yes. Active Directory stores information about employees – full name, SBA office telephone number, SBA e-mail address and SBA office address. This type of information is releasable to the public.

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

The SBA LAN/WAN provides office automation capabilities for approximately 4,500 government and contractor personnel. The SBA LAN/WAN is comprised of approximately 140 Windows servers located in SBA offices throughout the United States.

The SBA LAN/WAN provides the networking and telecommunication infrastructure to support interconnection and information sharing among applications, organizations, and individuals. The SBA WAN uses frame relay technology to interconnect LAN segments at SBA offices nationwide using AT&T Network and managed services.

The LAN/WAN is the platform that provides the transport medium for:

a) Inter-office/inter-agency/inter-governmental and external communications
b) Electronic messaging (email and PDA communications)
c) Telecommunications
d) Remote access (VPN)
e) Desktop faxing
f) Agency applications (client/server, web-based)
g) Mainframe access
h) High speed data backup
i) Internet access

3) Is the system in the development process?

No.

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

Not applicable.

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

a) The American Recovery and Reinvestment Act of 2009 (PL 111-5).

b) 15 U.S.C. § 634(b) (6), 44 U.S.C. § 3101.

c) Privacy Act of 1974, 5 U.S.C. 552a and related statutes (Electronic Communications Privacy Act of 1986; Computer Matching and Privacy Protection Act of 1988).

d) Paperwork Reduction Act of 1995; 44 U.S.C. 3501.

e) Government Paperwork Elimination Act of 1998.

f) Federal Records Act of 1950 and National Archives and Records Administration (NARA) implementing regulating at 36 C.F.R. 1220 and 41 C.S.R. 201-22.

g) The Office of Management and Budget (OMB) Circular A-l30, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems." OMB Circular A-130 implements a number of Federal laws relating to information resources ID (for example, the Paperwork Reduction Act, the Clinger-Cohen Act; and the Government Performance and Results Act).

h) The Federal Information Security Management Act of 2002 (FISMA).

i) Additional program definition is detailed in 13 C.F.R., Part 123.

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

There is potential for personally identifiable information, such as social security numbers, to be transmitted across and outside the LAN/WAN using e-mail, desktop faxing or other media. SBA has policies and procedures in place to mitigate the risks (e.g., SOP 90-47.2; SOP 90-49.1) and the agency adheres to NIST 800-53 rev. 3 controls. Electronic tools are used to monitor the network (such as Fidelis), and security software is in place and operational that has the ability to identify and quarantine PII that may be e-mailed outside the network. Layered security, perimeter security and vulnerability scanning are in place and operational. Users must log on using two-factor authentication (PIV card and PIN or User ID and password for access). A virtual private network provided by AT&T allows remote access to the LAN/WAN, and perimeter security applies to this as well as the use of RSA tokens. To access the SBA LAN/WAN from outside the network perimeter, users must be issued and utilize a valid RSA SecurID token.

C. SYSTEM DATA

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

Internal users, system operators, administrators, IT management (employees and contractors).

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

Microsoft Active Directory is one source of personal information – users provide personal information when applying for SBA accounts and an e-mail address is created for them.

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 information is initially taken from an individual. A new employee or contractor submits PII to the SBA Inspector General, who performs a background investigation and issues a clearance for access to the system. Form 1228, with the individual's PII and new SBA contact information, is then provided to the SBA OCIO IT Security team, who opens a ticket through a HelpDesk software system to create an Active Directory account. The individual's SBA e-mail address is generated by the administrator when the Active Directory account is created.

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

Not Applicable. All data within the system is generated internally by SBA.

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?

Employee information will be collected by Active Directory – name, office, address, e-mail address, telephone number, agency role. Information pertaining to public entities is not actively collected.

3) Accuracy, Timeliness, and Reliability

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

Because the LAN/WAN is not a system of records (and therefore not a source system), the LAN/WAN cannot and does not ensure data accuracy. Active Directory records are checked for accuracy by the administrator entering the information.

b. How is data checked for completeness?

Active Directory records are checked for completeness by the administrator entering the information.

c. Is the data current?

Data will be kept current by the system administrators; administrators will be notified by a HelpDesk ticket created by OCIO management when a change is made to an individual's information.

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

Data elements are described clearly and documented within Active Directory.

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

Active Directory data is available to everyone using the SBA LAN/WAN. While unlikely, this data has the potential to be released to the public. SBA Standard Operating Procedures 90-47.2 and 90-49.1 outline appropriate use of automated information systems. NIST 800-53 rev. 3 controls are in place, and all employees must undergo a 'Public Trust' background investigation and must sign a Rules of Behavior agreement prior to their first access of the LAN/WAN.

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 system is a data transport system. The specificity of the data is dependent on what an individual may choose to transmit. Active Directory contains a minimal amount of personal information.

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. The system does not derive new data or create previously unavailable data.

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?

No – the LAN/WAN itself will not make any determinations; it only transports data.

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?

The LAN/WAN itself will not consolidate any data – it only passes data. Refer to Section B, Question 6 in regards to controls in place to prevent unauthorized access or use.

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

N/A

8) How will the data be retrieved? Does a personal identifier retrieve the data?

Not Applicable.

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

Active Directory audit reports contain information regarding an individual's user ID and computer name (and other information related to a security event, but not the individual). The reports are used for reviewing security incidents and will be accessible by system administrators and SBA senior management, if requested.

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 authorized uses), and how individuals can grant consent.

Individuals must provide their name and office telephone number for Active Directory; an e-mail address is created based on the individual's name. An individual requesting an Active Directory account with SBA must provide this information, otherwise an account will not be created and they will not have access to the LAN/WAN. Information provided by the individual is only used as required and authorized.

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

SBA has policies and procedures in place to mitigate the risks (e.g., SOP 90-47.2; SOP 90-49.1) and the agency adheres to NIST 800-53 rev. 3 controls. To ensure only authorized users have access to the LAN/WAN, layered security, perimeter security and vulnerability scanning are in place and users must log on using two-factor authentication (PIV card and PIN or userID and password for access). A virtual private network provided by AT&T allows remote access to the LAN/WAN, and perimeter security applies to this as well requiring two-factor authentication (RSA token and PIN). In addition, beyond standard accesses that have been established as a minimum for users of the LAN/WAN, supervisors must approve additional security accesses prior to the user being granted access to that resource.

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?

The system has operations centers in Washington, D.C. and Denver, CO. Because the LAN/WAN is not a system of records (and therefore not a source system), the LAN/WAN does not ensure data accuracy.

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

Each Active Directory account holder (i.e. employee or contractor) controls the retention and deletion of information in his or her account while the account is active. All LAN/WAN accessibility accounts on the LAN/WAN are disabled immediately after the employee or contractor leaves the SBA. If possible, files and e-mails that fall under NARA record retention guidelines are forwarded by the user to their supervisor or other designated employee/contractor. If this is not possible (e.g.: adverse termination or death of the employee), the supervisor will request approved access to that user's e-mail and file folders to ensure continuity of mission requirements and that record retention policies are adhered to.

All employees and managers are briefed on the required records retention policies on an annual basis.

For Active Directory security events, certain audit records are kept for a minimum of seven years.

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?

SBA policy (SOP 90-47.2) states that all records are retained, archived and disposed in accordance with Federal regulations. Refer to General Records Schedule 20 of the National Archives and Records Administration for procedures.

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

In August 2010, SBA deployed Smart Card capability enterprise wide for the purpose of logical access. Each SBA employee and contractor, upon reporting for work, is issued a Personal Identification Verification (PIV) card. This PIV card, in conjunction with a SmartCard reader on the user's system and their Personal Identification Number (PIN), permits the user access to the LAN/WAN.

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

The above PIV card system provides enhanced security as the card itself and a properly entered PIN is required to access the LAN/WAN (two-factor authentication). This is an enhancement and improvement over the standard UserID/password entry system previously in place.

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

The LAN/WAN will be able to identify those using the network and locate them by IP address. It will provide system administrators the capability to monitor connections while logged on through DNS, networking monitoring, event viewer and terminal server management.

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

Active Directory has the capacity and capability to monitor:

a) User management activities
b) Last logon to workstations
c) Security and distribution groups
d) Membership changes
e) User logon activities
f) Logon failures
g) Domain controller, member server or workstation logon activities
h) Passwords changed / set
i) Enabled / disabled users
j) Account lockouts
k) Creation, modification or deletion of AD accounts
l) Domain policy changes

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

All activity on the LAN/WAN is subject to monitoring as it is a government computer system. Only system administrators have the ability to monitor activity on the LAN/WAN, and the following access control policies are in place. SBA has policies and procedures in place to mitigate the risks (e.g., SOP 90-47.2; SOP 90-49.1) and the agency adheres to NIST 800-53 rev. 3 controls. Electronic tools are used to monitor the network (such as Fidelis), and security software is in place and operational that has the ability to identify and quarantine PII that may be e-mailed outside the network. Layered security, perimeter security and vulnerability scanning are in place and operational. Users must log on using two-factor authentication (PIV card and PIN or User ID and password for access). A virtual private network provided by AT&T allows remote access to the LAN/WAN, and perimeter security applies to this as well as the use of RSA tokens. To access the SBA LAN/WAN from outside the network perimeter, users must be issued and utilize a valid RSA SecurID token.

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

Because the LAN/WAN is not a system of records for purposes of the Privacy Act, a SORN is not required to be published.

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)

All users of the system (contractors, users, managers, etc.) will be able to transmit data across the system and will have access to personal information stored within Active Directory. PII transmitted across the system (e.g., via e-mail) will be accessible only by the intended recipient and administrators, if authorized.

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

Access to data by a user is determined by Active Directory access controls via approval of SBA Form 1228. E-mail messages are directed only to the intended recipients.

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

Administrators will have access to all data being transmitted across the system. User's access will be restricted to personal information stored within Active Directory and to e-mail communications that are sent between individuals, meant for the recipients.

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

Active Directory data is available to everyone using the SBA LAN/WAN. All information stored on LAN/WAN pertaining to users and sent by users is accessible to system administrators. All employees must undergo a "Public Trust" background investigation and sign a Rules of Behavior agreement prior to first access of the system. SBA has policies and procedures in place to mitigate the risks (e.g., SOP 90-47.2; SOP 90-49.1) and the agency adheres to NIST 800-53 rev. 3 controls. Electronic tools are used to monitor the network (such as Fidelis), and security software is in place and operational that has the ability to identify and quarantine PII that may be e-mailed outside the network. Layered security, perimeter security and vulnerability scanning are in place and operational. Users must log on using two-factor authentication (PIV card and PIN or User ID and password for access). A virtual private network provided by AT&T allows remote access to the LAN/WAN, and perimeter security applies to this as well as the use of RSA tokens. To access the SBA LAN/WAN from outside the network perimeter, users must be issued and utilize a valid RSA SecurID token.

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?

Contractors are involved in the design, development and maintenance of the system. Privacy Act contract clauses are inserted into their contracts and SBA SOP 90-49 addresses other regulatory measures.

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?

N/A

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

N/A

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

N/A

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

Active Directory data is available to everyone using the SBA LAN/WAN. All information stored on LAN/WAN pertaining to users and sent by users is accessible to system administrators. Administrators must go through a rigorous investigative process and sign a Rules of Behavior agreement prior to first access of the system. Applicable NIST 800-53 rev. 3 access controls are in place. Information is not shared externally except by user e-mail transmission, and controls to regulate this are addressed at Section B, Question 6.

LAN/WAN PRIVACY IMPACT ASSESSMENT APPROVAL PAGE

The Following Officials Have Approved this Document:

System Owner

Signature **Date**

Sherry C. Hill
Director, Office of Communications Technology Services

Project Manager

Signature **Date**

Linda Terrell
Chief, Hetwork Integration Branch

IT Security Manager

Signature **Date**

Ja'Nelle L. DeVore
Chief Information Security Officer

Chief Privacy Officer

Signature **Date**

Paul T. Christy
Chief Information Officer/Chief Privacy Officer

LAN/WAN PRIVACY IMPACT ASSESSMENT APPROVAL PAGE

The Following Officials Have Approved this Document:

System Owner

Sherry C Hill — 5/31/11

Signature **Date**

Sherry C. Hill
Director, Office of Communications Technology Services

Project Manager

Linda Terrell — 6-1-11

Signature **Date**

Linda Terrell
Chief, Hetwork Integration Branch

IT Security Manager

for CISO — 6/2/11

Signature **Date**

Ja'Nelle L. DeVore
Chief Information Security Officer

Chief Privacy Officer

— 7/21/11

Signature **Date**

Paul T. Christy
Chief Information Officer/Chief Privacy Officer