Privacy Impact Assessment
Enterprise Local Area Network (ENTLAN)

Cyber and Privacy Policy an Oversight

- Version: 3.0
- Date: October 26, 2010
- Prepared for: USDA DM/WCTS
  John Brown (ISSO)

United States Department
of Agriculture

Privacy Impact Assessment for the

Enterprise Local Area Network (ENTLAN)

October 26, 2010

Contact Point
John Brown
USDA/DM
202-720-8582

Reviewing Official
Michael McGuire, Director of WCTS

United States Department of Agriculture

Abstract

To carry out its wide-ranging responsibilities, the U. S. Department of Agriculture (USDA), and its employees and managers have access to diverse and complex automated information systems, which include system file servers, local and wide area networks running various platforms, and telecommunications systems to include communication equipment. The bureaus and offices within the USDA depend on the confidentiality, integrity, and availability of these systems and their data in order to accomplish day-to-day activities.

Washington Communications and Technology Services Division (WCTS) directs the voice and data network for the Metropolitan Area Network (MAN) and Headquarters (HQ) Local Area Network (ENTLAN), providing telecommunications network and E-mail services to agencies in the Washington, DC Metropolitan area, Fort Collins, Colorado, Kansas City, Missouri, and Elkins, West Virginia. The WCTS provides broadband video services throughout the Washington, D.C. campus, and office automation services and support to the following USDA agencies: Office of the Secretary (OSEC), Office of the Executive Secretariat (OES), Office of the Chief Information Officer (OCIO), National Appeals Division (NAD), Assistant Secretary for Civil Rights (ASCR), Office of Communications (OC) and OC Design.

The Computer Support Branch (CSB) is the division of WCTS that provides LAN support to users in a Microsoft Windows 2003 operating environment. This includes Microsoft Office Automation support, backup/recovery of network data, access support for file/print server resources, filtered Internet access, database support, and web application development and hosting support.

The USDA relies on the Enterprise Local Area Network (ENTLAN) and its information technology systems, to accomplish its mission of providing cost-effective and reliable services to the USDA. In accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, all federal systems have value and require some level of protection. ENTLAN provides authorization, authentication and accountability controls to protect the informational and physical resources of the user community.

A Privacy Impact assessment is being conducted because information in ENTLAN used to authorize and authenticate users may be considered PII.

Overview

The primary purpose of the Enterprise Local Area Network (ENTLAN) is to provide Microsoft infrastructure services to Metropolitan Headquarters Area user community and to provide Microsoft Hosting services to USDA organizational components. These services include Active Directory, DNS, DHCP, and file and print services. ENTLAN is comprised of three Active Directory forest with five domains located in and accessed from the United States Department of Agriculture facilities in Washington, DC, Fort Collins, CO, Elkins, WV, Beltsville, MD (GWCC), and Kansas City, MO. These facilities are government controlled and are not open to the general public. The computer facilities in each location has its own access requirements, but server and communications rooms are separately secured from the rest of the buildings such that only people requiring access in the performance of official duties are authorized unescorted entry. All visitors are required to sign in and are escorted at all times.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

User Name	User ID	Work Address
Agency	Email Address	

1.2 What are the sources of the information in the system?

USDA Departmental Management employees, contractors or business partners submit a new account request form.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is being collected/submitted in order to establish new accounts and to identify an account holder.

1.4 How is the information collected?

The information is collected from the individual via the account request process. The informed consent of the subject individual is required as part of the WCTS New Employee Entry Process.

1.5 How will the information be checked for accuracy?

The government supervisor/sponsor of the employee, contractor or business partner must review the account request form for accuracy. Once the account has been created the employee, contractor or business partner can review their data contained in Active Directory by using the Microsoft Outlook Address book. Information can be updated/corrected by submitting an email request to the DM help Desk. (DM.ServiceDesk@dm.usda.gov)

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

It is required under Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Guidance can be found in Appendix III to OMB Circular No. A-130 and NIST SP 800-30, *Risk Management Guide for Information Technology Systems.*

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The type of data is Name, work email address, work location and work telephone number. The risk to the individual; is very low. This work related information is generally considered not to be PII.

This information is available in the Exchange Global Address List, however, the ability to link this information to other data sources is mitigated by prohibiting access to other data stores by the implemented layers of security to include firewall, intrusion detection system, encryption.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information is used to uniquely identify the individual for authentication, authorization and accountability purposes.

2.2 What types of tools are used to analyze data and what type of data may be produced?

There is no requirement for data analysis. The data can report a list of account holders with their work location, work telephone number and work email address.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

N/A

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Only authorized individuals have access to the system. The information is generally not considered PII. All data is stored in an encrypted database. The work related information is made available to any USDA account holder through the Global Address List.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

All EntLAN system data is retained in accordance with USDA retention requirements. Backups of system data are produced daily, weekly and monthly. Daily (differential) backups are retained onsite for three months before reuse. Weekly and monthly backups are stored off site and rotated back in on after three months. Weekly (full) backups are stored offsite for 2 weeks and monthly backups are stored offsite for 3 years.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

ENTLAN documents are being retained in accordance with DR 3080-001, USDA Records Management Policy, WCTS Document Management Plan and federal regulations established by the National Archives and Records Administration (NARA) and the. The DM CIO has approved the ENTLAN retention periods.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk to the individual is very low. The primary purpose of ENTLAN data is to uniquely identify the account holder. The system does not maintain data is considered PII and there is no perceived risk.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The information is shared throughout USDA by the user of Active Directory and the Global Catalog.

4.2 How is the information transmitted or disclosed?

The information is shared through the Global Address List which uses Kerberos encryption to protect the data in transit.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The risk to the individual is very low. The information that is shared is work related information including work location, work telephone number and work email address. The system does not maintain data is considered PII and there is no perceived risk.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information is not shared outside USDA.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please

describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Information is not shared outside USDA. A SORN is not needed.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is not shared outside USDA.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Information is not shared outside USDA.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Notice is provided during the new account request process. The user must acknowledge the informed consent provisions with a signature during the new account request process.

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

No

The USDA employee, contractor, or stakeholder does not have the opportunity to decline to provide non-PII information. The information requested is required to assign and set up the user account. The user has the right to correct or update information at any time by sending an email request to DM.ServiceDesk@dm.usda.gov.

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

The requirement is for each account to be uniquely tied to an individual, all other may be changed, updated or deleted by sending an email request to DM.ServiceDesk@dm.usda.gov.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The risk to the individual is very low. The user must acknowledge the informed consent provisions with a signature during the new account request process. The information collected is generally considered not to be PII and there is no perceived risk.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

The user may view their information by going into Outlook, select the "Search address book" icon then enter their name with last name first. Once located, the user must double click on his/her directory listing and your detail information will appear.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The user has the right to correct or update information at any time by sending an email request to DM.ServiceDesk@dm.usda.gov. At the present time the user does not have the ability to update/correct their data directly, however, this feature will be available in the future.

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

The user has the right to correct or update information at any time by sending an email request to DM.ServiceDesk@dm.usda.gov.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The user has the right to correct or update information at any time by sending an email request to DM.ServiceDesk@dm.usda.gov.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No additional privacy risks associated with the redress.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

USDA Departmental Management employees and contractors who have a need to access email, office automation and/or online services may be granted access to the system. There are documented procedures to include SAC processing instructions for Individuals, WCTS Access Control Policy and WCTS Account Management Procedures.

8.2 Will Department contractors have access to the system?

Yes, after following the security access control (SAC) procedures which include a background investigation.

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

All USDA users must complete Computer Security Training before they are granted access to the system. Ever time the user logs on to a workstation a splash screen appears that stresses privacy information security. The user must acknowledge this before the user is able to continue. Annual refresher training is provided through AgLearn. There is annual ISA training which includes Privacy. See http://www.hqnet.usda.gov/SystemsSecurityAwarenessFY09.pdf.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes in October 2007. The system is currently under reaccreditation review.

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

None

8.6 <u>Privacy Impact Analysis</u>: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk to the individual is very low. The information collected is generally considered not to be PII and there is no perceived risk.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The is a mandated system by Clinger-Cohen and it is in operational status.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23

"Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

ENTLAN systems do not utilize or interface with third party websites

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

None

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require

either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Does the system use web measurement and customization technology?

N/A – ENTLAN does not use any web measurement and customization technology (i.e., "cookies")

Responsible Officials

Michael McGuire
Departmental Management CIO
United States Department of Agriculture

Approval Signature

Position of Signatory	*Name of Signatory*	*Date Signed*	*Signature*
Approving Authority	Mike McGuire	11/2/2010	
Certifying Authority	Christopher Wood	11/2/2010	Chris Wood
System Owner	Cedric Bragg	11/1/2010	
ISSPM	Carl Holmes	10/29/2010	Carl Holmes
ISSO	John Brown	10/29/2010	John W Brown
Project Manager	Ashwin Karkera	10/29/2010	