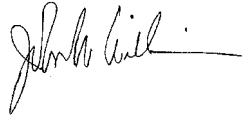


For: All FSA Employees (Federal and Non-Federal) and Contractors

**Interim Encryption Solution Approved for the Protection of
Sensitive (Privacy Act Protected) Data**

Approved by: Deputy Administrator, Management



1 Encrypting Sensitive Data

A Background

Notice IRM-371 provided FSA policy on the management of sensitive (Privacy Act protected) data to help safeguard the information. All FSA employees, contract employees, and partners who handle Privacy Act protected data in the performance of their duties must comply with this and all other applicable Federal, USDA, FSA, and OCIO ITS requirements. Notice IRM-371, subparagraph 2 D identified restrictions on the transmission of Privacy Act protected data and provided contact information for obtaining technical information on how Privacy Act protected data should be protected through encryption during transfer or transmission.

In response to OMB Memorandum 06-16, a memorandum from the USDA, Chief Information Officer (CIO), dated July 13, 2006, (Exhibit 1) provides additional technical information and describes interim steps that USDA Agencies may take to protect Privacy Act protected and other sensitive data on Government systems. The memorandum suggests using existing software in the standard computer configurations already in-place in the USDA to encrypt Privacy Act protected and other sensitive data.

WinZip is currently available to all FSA employees (Federal and non-Federal) and contractors with a Government-furnished computer. WinZip supports the Advanced Encryption Standard (AES), 256-bit encryption that is approved for use by the Government by the National Institute of Standards and Technology in Federal Information Processing Standards Publication 197. Accordingly, as an interim solution, WinZip AES encryption with 256-bit keys is approved for the protection of FSA Privacy Act protected and other sensitive data on Government systems, until additional USDA-wide solutions can be developed and deployed.

B Purpose

This notice provides instructions for using WinZip with 256-bit AES encryption to protect Privacy Act protected and other sensitive data on FSA systems.

Disposal Date	Distribution
October 1, 2007	All FSA Employees and Contractors; State Offices relay to County Offices

Notice IRM-372

1 Encrypting Sensitive Data (Continued)

C Authorities

The sources of authority are:

- The Privacy Act of 1974, as amended (Pub. L. 93-579, 5 U.S.C. 552a)
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, dated June 23, 2006
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, dated May 22, 2006
- OMB Circular A-130, Management of Federal Information Resources
- Memorandum for all USDA Agency CIO's and Agency ISSPM's from the CIO about "Interim Steps for Office of Management and Budget 06-16," dated July 13, 2006 (Exhibit 1)
- Memorandum for all USDA employees and contractors from the CIO about "Protecting and Safeguarding Privacy Act Protected Information," dated July 18, 2006
- Memorandum for all USDA employees and contractors from the CIO about "Protecting and Safeguarding Privacy Act Protected Information," dated June 16, 2006
- USDA Cyber Security Manual Series 3500 and associated Cyber Security guidance
- Notice IRM-371
- Notice IRM-364
- 6-IRM
- especially the following:
 - USDA Departmental Manual (DM) 3505-000, USDA Computer Incident Response Procedures Manual (March 20, 2006)
 - DM 3530-005, Encryption Security Standards (February 17, 2005)
 - DM 3550-002, Sensitive But Unclassified (SBU) Information (February 17, 2005)
 - USDA Administrative Bulletin Departmental Regulation (DR) 3602-001, OCIO-ITS Security Policy Manual

Notice IRM-372

1 Encrypting Sensitive Data (Continued)

D Instructions For Using WinZip AES, 256-bit Encryption

Instructions for using WinZip are provided in Exhibit 2.


E Points of Contact for Additional Information

Questions about using WinZip encryption features should be directed to user's local help desk. Notice IRM-364 contains information on how to contact user's local help desk personnel.

For policy related questions about the need for protection of Privacy Act protected data, contact the ITSD Information Security Office help desk, by:

- e-mail to security@kcc.usda.gov
- telephone at 816-926-6537.

Memorandum About "Interim Steps for Office of Management and Budget 06-16"

RECEIVED FAX	JUL 10 2006 6:50PM	FOIA CASE NO.	OFFICE OF MANAGEMENT AND BUDGET
Jul 18 06 03:40p	Cyber Security	202 205-3755	p. 3
			
JUL 13 2006			
United States Department of Agriculture Office of the Chief Information Officer 1400 Independence Avenue SW Washington, DC 20250	TO: Agency Chief Information Officers Agency Information System Security Program Managers		
	FROM: Lynn Allen <i>[Signature]</i> Associate Chief Information Officer Cyber Security		
	SUBJECT: Interim Steps for Office of Management and Budget (OMB) Memorandum 06-16		
<p>On June 23, 2006, OMB issued guidance that requires federal agencies to take four specific actions to protect Privacy Act and other sensitive data on agency systems within 45 days. OCIO established a working group, chaired by my Operations group, to address the first two requirements: (1) encryption of portable devices and (2) use of two-factor authentication. The working group will identify processes, evaluate products, and establish a timeline to implement the OMB mandate successfully Department-wide.</p> <p>In the interim, individual agencies can take several actions, which have little to no cost associated with them, to protect our sensitive information. While these actions are not long-term solutions, they are 'first steps' in protecting your data. Agencies are encouraged to implement those that you feel work best in your environment.</p>			
<p>1. <u>Encrypt all data on mobile devices/computers</u></p> <ul style="list-style-type: none"> • Inform users what data is considered sensitive within your agency and remind them of their responsibilities for protecting such data. • Use the Encrypted File System (EFS) available in current versions of Microsoft Windows • Use the built-in encryption function in Microsoft Excel or Word, or use inexpensive encryption software in compression software (i.e., WinZip) or similar programs. • Replace existing USB 'thumb' drives with ones that are accompanied by strong encryption software. • When obtaining data extracts from databases, do not include Privacy Act protected or other sensitive data unless absolutely necessary. • Ensure that contracts explicitly require that contractors are responsible for controlling and protecting Privacy Act and other sensitive data in their possession, and that they destroy such data when the contract has ended. 			
AN EQUAL OPPORTUNITY EMPLOYER			

Memorandum About "Interim Steps for Office of Management and Budget 06-16" (Continued)

Received Fax : JUL 18 2006 2:05PM FAX SERIAL : U.S. DEPARTMENT OF AND INSURETY
Jul 18 06 03:40p Cyber Security 202 205-3755 P. 4

2. Remote Access with two-factor authentication

- Do not allow traffic from remote access software through your firewall. Instead, require telework employees and contractors to enter the network through a Virtual Private Network (VPN), before launching remote access software.
- Limit remote access through VPN by specific Internet Protocol (IP), or hardware (MAC) address rather than allowing anyone to make such a connection.
- Remind employees to use strong passwords, and enforce the use of such strong passwords within the operating system when possible. Strong passwords are at least eight characters long and include a combination of upper and lower-case letters, numbers, and special characters.
- Ensure that default software passwords are changed to strong passwords as defined above.
- Rename the Administrator account in Windows and ensure that Guest accounts are disabled.

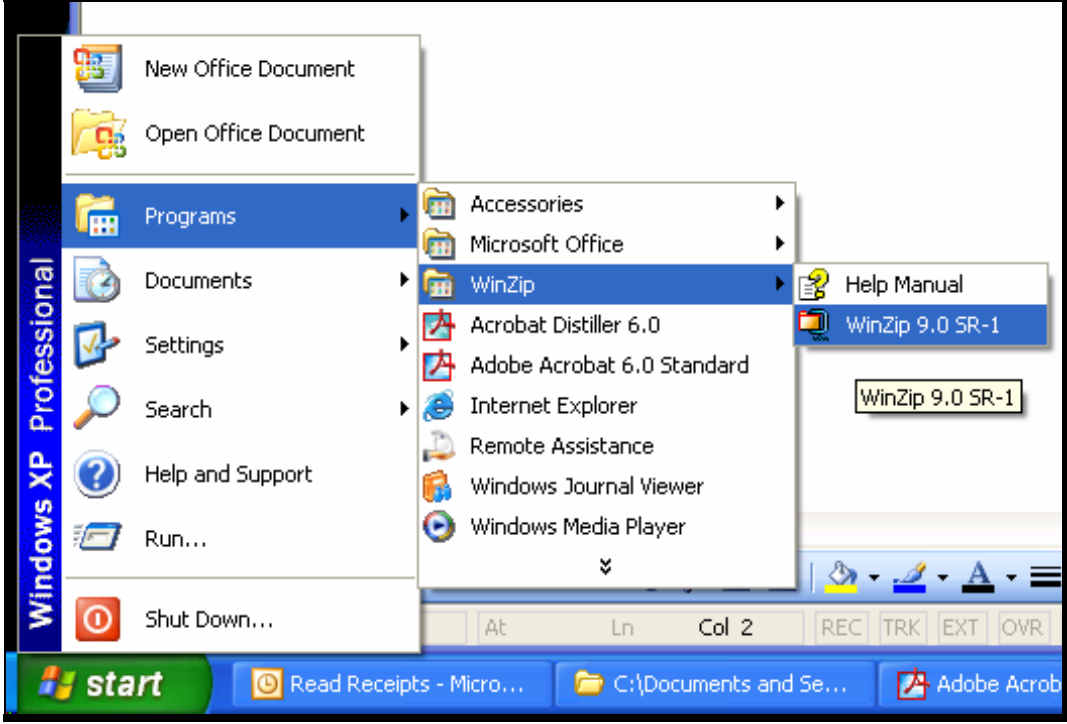
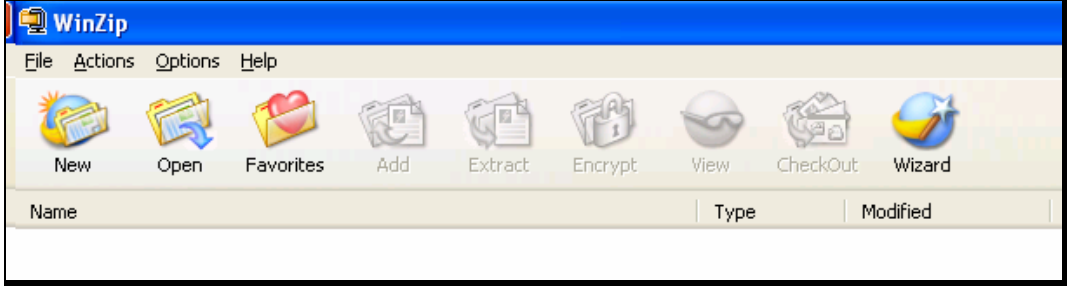
The third and fourth actions outlined in the OMB memorandum are security practices that should already be in place. Please review your policies and processes to ensure that controls have been established and are operating effectively for these two items.

The full text of OMB's memorandum can be found on OMB's website www.whitehouse.gov/omb. If you have any questions, please contact Steven Bryce Eckland, Computer Security Operations Division, at 816-926-7330.

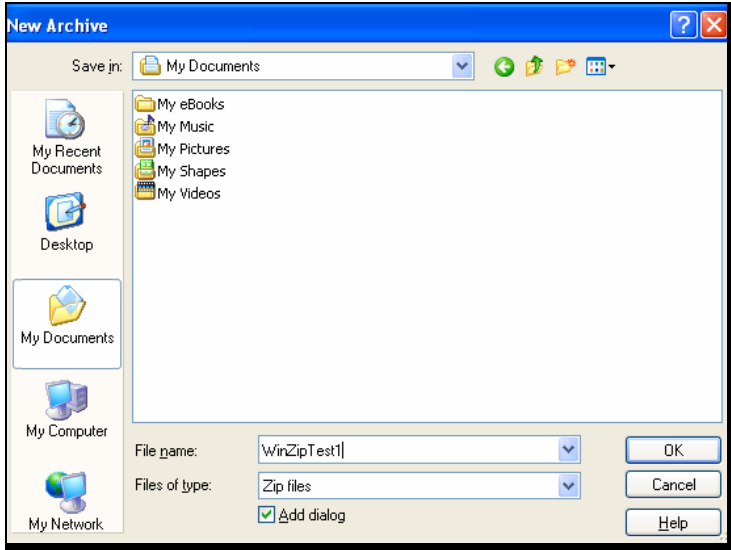
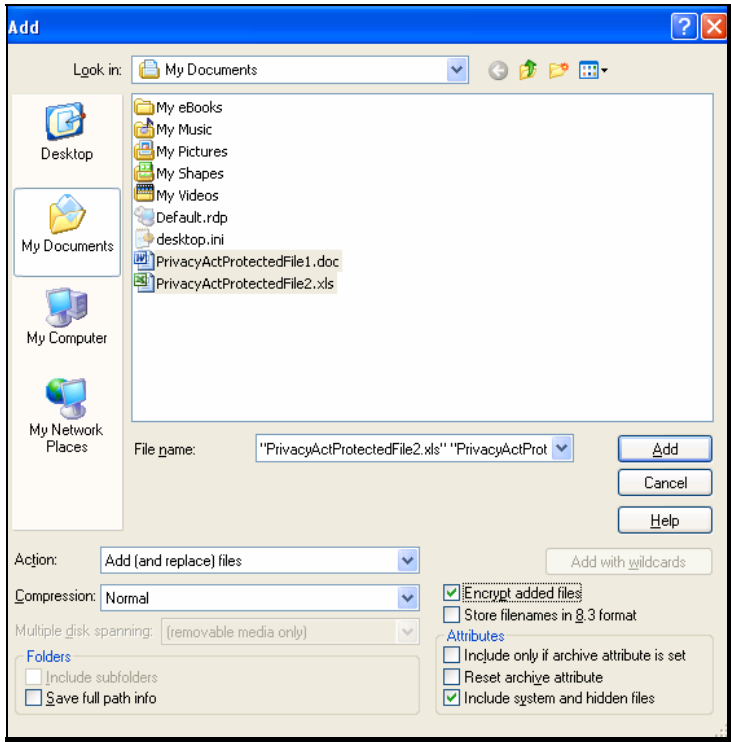
cc:
Dave Combs, Chief Information Officer
Jerry Williams, Deputy Chief Information Officer

Instructions for Using WinZip to Encrypt Sensitive (Privacy Act Protected) Data

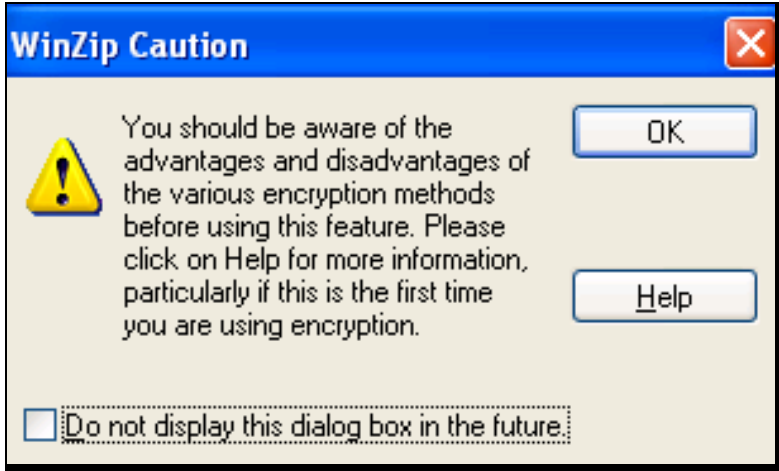

The following instructions are for using WinZip.

Step	Action
1	<p>From the Start Menu on user's computer, select WinZip 9.0 SR-1.</p>  <p>The screenshot shows the Windows XP Professional Start menu. The 'Programs' folder is expanded, and 'WinZip' is selected. The 'WinZip 9.0 SR-1' application is highlighted in the sub-menu. The taskbar at the bottom shows the Start button, a clock, and several open applications including 'Read Receipts - Micro...', 'C:\Documents and Se...', and 'Adobe Acrobat'.</p>
2	<p>CLICK "New" icon to create a new WinZip archive.</p>  <p>The screenshot shows the WinZip application window. The title bar reads 'WinZip'. The menu bar includes 'File', 'Actions', 'Options', and 'Help'. The 'Actions' menu is open, displaying several icons: 'New' (a folder with a plus sign), 'Open' (a folder with a magnifying glass), 'Favorites' (a folder with a heart), 'Add' (a folder with a plus sign), 'Extract' (a folder with a minus sign), 'Encrypt' (a folder with a lock), 'View' (a folder with a magnifying glass), 'CheckOut' (a folder with a magnifying glass), and 'Wizard' (a folder with a star). Below the menu bar is a table with columns for 'Name', 'Type', and 'Modified'.</p>

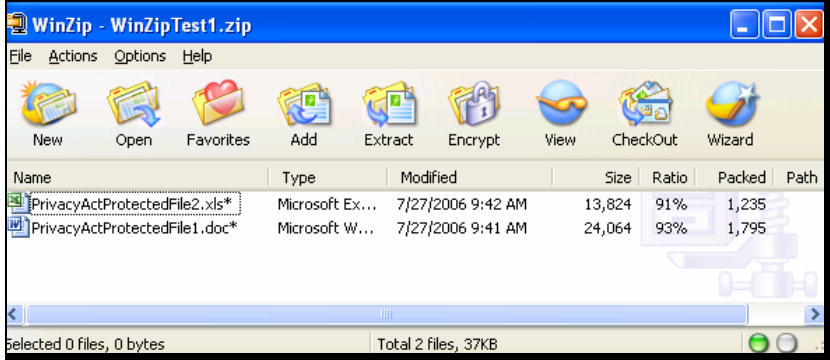
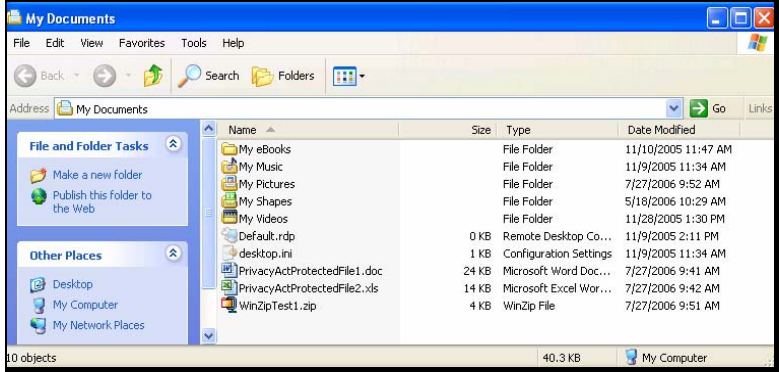
Instructions for Using WinZip to Encrypt Sensitive (Privacy Act Protected) Data (Continued)

Step	Action
3	<p>Enter a filename for user’s encrypted file such as “WinZipTest1” in the “File name:” box and CLICK “OK”.</p> 
4	<p>Select the files user wants encrypted, such as “PrivacyActProtectedFile1.doc” and “PrivacyActProtectedFile2.xls” as shown in the following screen print, check the box for “Encrypt added files”, and CLICK “Add”.</p> 

Instructions for Using WinZip to Encrypt Sensitive (Privacy Act Protected) Data (Continued)

Step	Action
<p>4 Cntd</p>	<p>A dialog box is displayed to suggest that the user read the WinZip Encryption Help File. This is highly recommended unless user is an experienced user. CLICK “Help” or “OK”, as appropriate.</p>  <p>The image shows a 'WinZip Caution' dialog box with a yellow warning icon. The text reads: 'You should be aware of the advantages and disadvantages of the various encryption methods before using this feature. Please click on Help for more information, particularly if this is the first time you are using encryption.' There are 'OK' and 'Help' buttons. At the bottom, there is a checkbox labeled 'Do not display this dialog box in the future:' which is currently unchecked.</p>
<p>5</p>	<p>CLICK radio button for “256-Bit AES encryption (stronger)”, enter a password, enter a password again, and CLICK “OK”.</p>  <p>The image shows an 'Encrypt' dialog box. It contains a note: 'Note: the password will be applied to files you subsequently add to or extract from the current archive, and will be automatically cleared when the archive is closed.' Below the note are two password input fields: 'Enter password:' and 'Re-enter password (for confirmation):', both containing masked characters. There is a checked checkbox for 'Mask password'. Under 'Encryption method', three radio buttons are shown: 'Zip 2.0 compatible encryption (portable)', '128-Bit AES encryption (strong)', and '256-Bit AES encryption (stronger)', with the last one selected. There are 'OK', 'Cancel', and 'Help' buttons, along with an 'Information on encryption methods' button.</p> <p>Note: The password used should be at least 8 characters long, have both capital and lower case letters, and should have at least 1 number or special character in the middle of the password. For additional details on choosing passwords, contact user’s local help desk.</p>

Instructions for Using WinZip to Encrypt Sensitive (Privacy Act Protected) Data (Continued)

Step	Action																																												
6	<p>WinZip will display the contents of the encrypted file user created in steps 4 and 5.</p> <p>Example: The file name in this screen print is “WinZipTest1.zip”.</p> <p>WinZip can now be closed; CLICK “X” in the upper, right-hand corner.</p>  <p>The screenshot shows the WinZip application window titled "WinZip - WinZipTest1.zip". The menu bar includes File, Actions, Options, and Help. The toolbar contains icons for New, Open, Favorites, Add, Extract, Encrypt, View, CheckOut, and Wizard. Below the toolbar is a table listing files:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Modified</th> <th>Size</th> <th>Ratio</th> <th>Packed</th> <th>Path</th> </tr> </thead> <tbody> <tr> <td>PrivacyActProtectedFile2.xls*</td> <td>Microsoft Ex...</td> <td>7/27/2006 9:42 AM</td> <td>13,824</td> <td>91%</td> <td>1,235</td> <td></td> </tr> <tr> <td>PrivacyActProtectedFile1.doc*</td> <td>Microsoft W...</td> <td>7/27/2006 9:41 AM</td> <td>24,064</td> <td>93%</td> <td>1,795</td> <td></td> </tr> </tbody> </table> <p>The status bar at the bottom indicates "Selected 0 files, 0 bytes" and "Total 2 files, 37KB".</p>	Name	Type	Modified	Size	Ratio	Packed	Path	PrivacyActProtectedFile2.xls*	Microsoft Ex...	7/27/2006 9:42 AM	13,824	91%	1,235		PrivacyActProtectedFile1.doc*	Microsoft W...	7/27/2006 9:41 AM	24,064	93%	1,795																								
Name	Type	Modified	Size	Ratio	Packed	Path																																							
PrivacyActProtectedFile2.xls*	Microsoft Ex...	7/27/2006 9:42 AM	13,824	91%	1,235																																								
PrivacyActProtectedFile1.doc*	Microsoft W...	7/27/2006 9:41 AM	24,064	93%	1,795																																								
7	<p>The encrypted file (shown in this screen print as “WinZipTest1.zip”) is now properly protected and may be transported by e-mail, CD Rom, floppy disk, or other unsecure media/means, as appropriate.</p>  <p>The screenshot shows the "My Documents" folder in Windows Explorer. The address bar shows "My Documents". The left pane shows "File and Folder Tasks" and "Other Places". The main pane displays a list of files and folders:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Type</th> <th>Date Modified</th> </tr> </thead> <tbody> <tr> <td>My eBooks</td> <td></td> <td>File Folder</td> <td>11/10/2005 11:47 AM</td> </tr> <tr> <td>My Music</td> <td></td> <td>File Folder</td> <td>11/9/2005 11:34 AM</td> </tr> <tr> <td>My Pictures</td> <td></td> <td>File Folder</td> <td>7/27/2006 9:52 AM</td> </tr> <tr> <td>My Shapes</td> <td></td> <td>File Folder</td> <td>5/18/2006 10:29 AM</td> </tr> <tr> <td>My Videos</td> <td></td> <td>File Folder</td> <td>11/28/2005 1:30 PM</td> </tr> <tr> <td>Default.rdp</td> <td>0 KB</td> <td>Remote Desktop Co...</td> <td>11/9/2005 2:11 PM</td> </tr> <tr> <td>desktop.ini</td> <td>1 KB</td> <td>Configuration Settings</td> <td>11/9/2005 11:34 AM</td> </tr> <tr> <td>PrivacyActProtectedFile1.doc</td> <td>24 KB</td> <td>Microsoft Word Doc...</td> <td>7/27/2006 9:41 AM</td> </tr> <tr> <td>PrivacyActProtectedFile2.xls</td> <td>14 KB</td> <td>Microsoft Excel Wor...</td> <td>7/27/2006 9:42 AM</td> </tr> <tr> <td>WinZipTest1.zip</td> <td>4 KB</td> <td>WinZip File</td> <td>7/27/2006 9:51 AM</td> </tr> </tbody> </table> <p>The status bar at the bottom indicates "10 objects" and "40.3 KB".</p> <p>Notes: Passwords should never be written down, e-mailed, or shared with unknown individuals.</p> <p>Because of recent emergence of some viruses and worms that use the WinZip (.zip) file extension, some USDA and other e-mail systems may filter out WinZip (.zip) file attachments, preventing them from being forwarded as e-mail attachments.</p>	Name	Size	Type	Date Modified	My eBooks		File Folder	11/10/2005 11:47 AM	My Music		File Folder	11/9/2005 11:34 AM	My Pictures		File Folder	7/27/2006 9:52 AM	My Shapes		File Folder	5/18/2006 10:29 AM	My Videos		File Folder	11/28/2005 1:30 PM	Default.rdp	0 KB	Remote Desktop Co...	11/9/2005 2:11 PM	desktop.ini	1 KB	Configuration Settings	11/9/2005 11:34 AM	PrivacyActProtectedFile1.doc	24 KB	Microsoft Word Doc...	7/27/2006 9:41 AM	PrivacyActProtectedFile2.xls	14 KB	Microsoft Excel Wor...	7/27/2006 9:42 AM	WinZipTest1.zip	4 KB	WinZip File	7/27/2006 9:51 AM
Name	Size	Type	Date Modified																																										
My eBooks		File Folder	11/10/2005 11:47 AM																																										
My Music		File Folder	11/9/2005 11:34 AM																																										
My Pictures		File Folder	7/27/2006 9:52 AM																																										
My Shapes		File Folder	5/18/2006 10:29 AM																																										
My Videos		File Folder	11/28/2005 1:30 PM																																										
Default.rdp	0 KB	Remote Desktop Co...	11/9/2005 2:11 PM																																										
desktop.ini	1 KB	Configuration Settings	11/9/2005 11:34 AM																																										
PrivacyActProtectedFile1.doc	24 KB	Microsoft Word Doc...	7/27/2006 9:41 AM																																										
PrivacyActProtectedFile2.xls	14 KB	Microsoft Excel Wor...	7/27/2006 9:42 AM																																										
WinZipTest1.zip	4 KB	WinZip File	7/27/2006 9:51 AM																																										

Note: Before using WinZip to encrypt data, read the following notes from the WinZip Help File that provide additional important information on encryption safety. User’s help desk is available to assist if user has any additional questions.

Instructions for Using WinZip to Encrypt Sensitive (Privacy Act Protected) Data (Continued)**Winzip 9.0 Notes From Help File**

Encryption provides a measure of safety for your sensitive documents, but even encrypted documents can be compromised (regardless of whether they were encrypted by WinZip or by other encryption software). Here are *some* of the ways this can occur. This is by no means an exhaustive list of potential risks; it is intended only to give you an idea of some of the safety issues involved with sensitive documents.

- If a keystroke monitor or other malicious code (such as a virus) is running on your computer, your password may be recorded when you type it. Be sure to check frequently for viruses and follow other recommended computer safety procedures.
- If you extract an encrypted file and then delete the file, it may be possible for someone to later "undelete" the file using file recovery software or the Recycle Bin.
- When you open or view a file from an archive (by double-clicking it), WinZip must extract the file to a temporary location so that the associated program can open it. If you subsequently close WinZip without first closing the program that is using the file, WinZip may not be able to delete the temporary copy of the file, thereby leaving it on disk in unencrypted form. The associated program may also make one or more backup copies of the decrypted file, and WinZip will not be able to delete these. In addition, as described above, it may be possible for someone to later recover deleted files using file recovery software or the Recycle Bin.
- When you "move" files to a Zip file by choosing the **Move** action in the Add dialog, WinZip moves the files into the Zip file by compressing them and then deleting the original files from the disk. It may be possible to recover the original, unencrypted files from the disk.
- After adding or extracting encrypted files, some or all of the unencrypted file contents may remain in your computer's memory or the page swap files on disk. A malicious user may be able to retrieve this unencrypted information.
- WinZip does not encrypt Zip file comments or, as described above, information about encrypted files such as their names, dates, etc. Any user with access to the Zip file can view this information without a password.

You may be able to eliminate some of these exposures using specialized software such as virus scanners, disk erasers, etc.