



ENTERPRISE MESSAGING

IRONPORT EMAIL ENCRYPTION

USER GUIDE

Version: 1.4

Date: 6/30/2014

SECURITY WARNING

The information contained herein is proprietary to the Commonwealth of Pennsylvania and must not be disclosed to un-authorized personnel. The recipient of this document, by its retention and use, agrees to protect the information contained herein. Readers are advised that this document may be subject to the terms of a non-disclosure agreement.

DO NOT DISCLOSE ANY OF THIS INFORMATION WITHOUT OBTAINING PERMISSION FROM THE MANAGEMENT RESPONSIBLE FOR THIS DOCUMENT.

Version History

Date	Version	Modified By / Approved By	Section(s)	Comment
9/15/2009	1.0	Daren McCormick	All	Initial Version
9/28/2009	1.1	C. Reber	All	Made extensive formatting and structure updates to the document. Basic content was not changed. Changed title and file name.
12/17/2009	1.2	Daren McCormick	All	Removed references to automatic encryption
6/13/2013	1.3	C. Reber	All	Updated links and team references. Blocked out phone # on screen shots.
6/30/2014	1.4	M. White C. Reber (QA Edits)	All	Updated to use with CRES Edited document to OA-OIT standards

Table of Contents

- 1 INTRODUCTION..... 4**
 - 1.1 PURPOSE/BRIEF OVERVIEW 4
- 2 SENDING ENCRYPTED EMAIL..... 5**
 - 2.1 SEND AN ENCRYPTED MESSAGE USING THE SEND SECURE BUTTON IN OUTLOOK 5
 - 2.2 SEND AN ENCRYPTED MESSAGE USING THE SUBJECT LINE FILTER..... 7
- 3 CISCO REGISTERED ENVELOPE SERVICE (CRES) REGISTRATION..... 8**
 - 3.1 CRES REGISTRATION PROCESS..... 8
- 4 RECEIVING AND OPENING ENCRYPTED MESSAGES..... 12**
 - 4.1 OPENING A MESSAGE USING THE STANDARD METHOD 12
 - 4.2 OPENING A MESSAGE USING THE OPEN ONLINE FEATURE 15
 - 4.3 RECEIVING MESSAGES WITH ENCRYPTED ATTACHMENTS 16
- 5 RESETTING A CRES ACCOUNT PASSWORD..... 17**
- 6 APPENDIX A – ADDITIONAL INFORMATION..... 20**
 - 6.1 SUPPORT..... 20
 - 6.2 REFERENCES 20

1 Introduction

1.1 PURPOSE/BRIEF OVERVIEW

The OA/OIT has selected Cisco IronPort as the solution for secure email for the "Commonwealth of Pennsylvania" agencies that are under the Governor's jurisdiction. The addition of the secure email solution addresses the needs of commonwealth email users who have valid business requirements for sending emails containing sensitive information securely to third parties or business partners.

Cisco IronPort interfaces with the commonwealth email systems and becomes an additional seamless feature within the Outlook email application.

This document provides the end user with knowledge of how to send and receive and encrypted messages.

2 Sending Encrypted Email

Encrypted email can be sent using the Cisco IronPort add-in for Outlook, manually entering specific text in the subject line (subject line filter) or automatically, through the use of data loss prevention (DLP) policies.

The following tasks must be performed to encrypt a message.

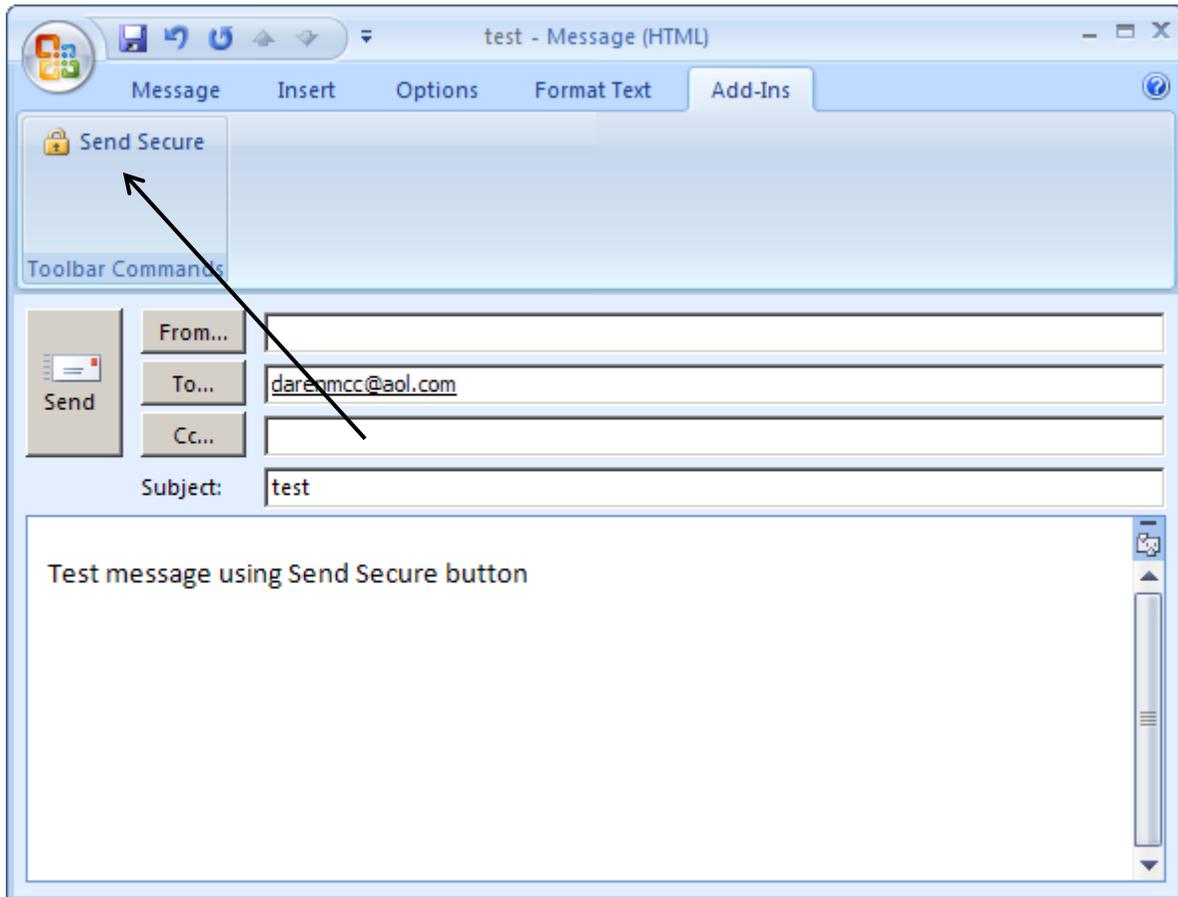
2.1 SEND AN ENCRYPTED MESSAGE USING THE SEND SECURE BUTTON IN OUTLOOK

The IT department deploys the Cisco IronPort add-in within Outlook for each agency that chooses to use this method for sending an encrypted message.

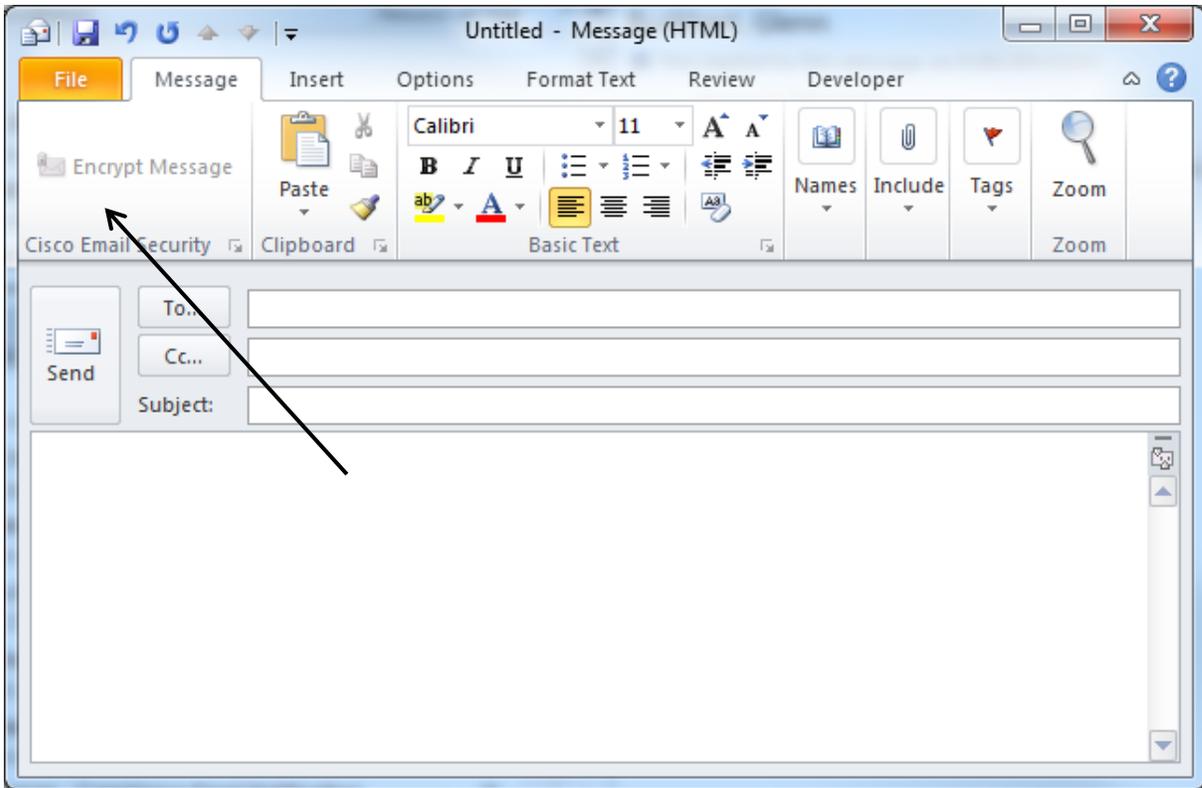
When installed, the add-in creates an "Encrypt Message" button on the Outlook ribbon of the new message window. To use this button, click it to toggle it on and click Send. This will prepend this text "[SEND SECURE]" to the subject line of your message.

There are different versions available depending on the installed version of Outlook. Each version looks slightly different.

- Example: Send Secure button displayed in Outlook 2007



- Example: Encrypt Message button displayed in Outlook 2010

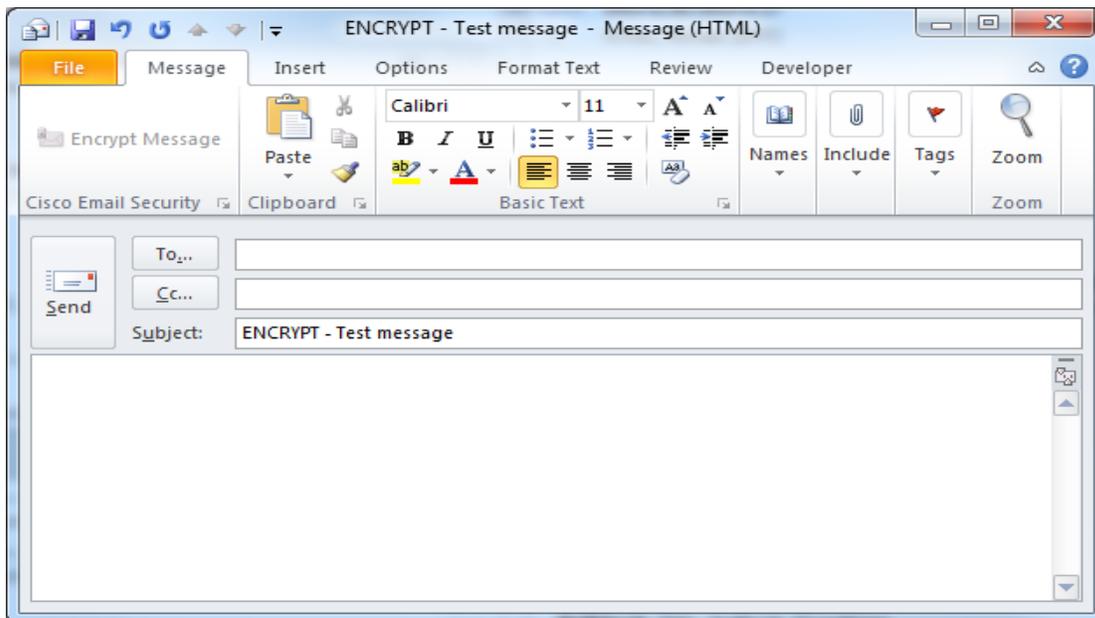


2.2 SEND AN ENCRYPTED MESSAGE USING THE SUBJECT LINE FILTER

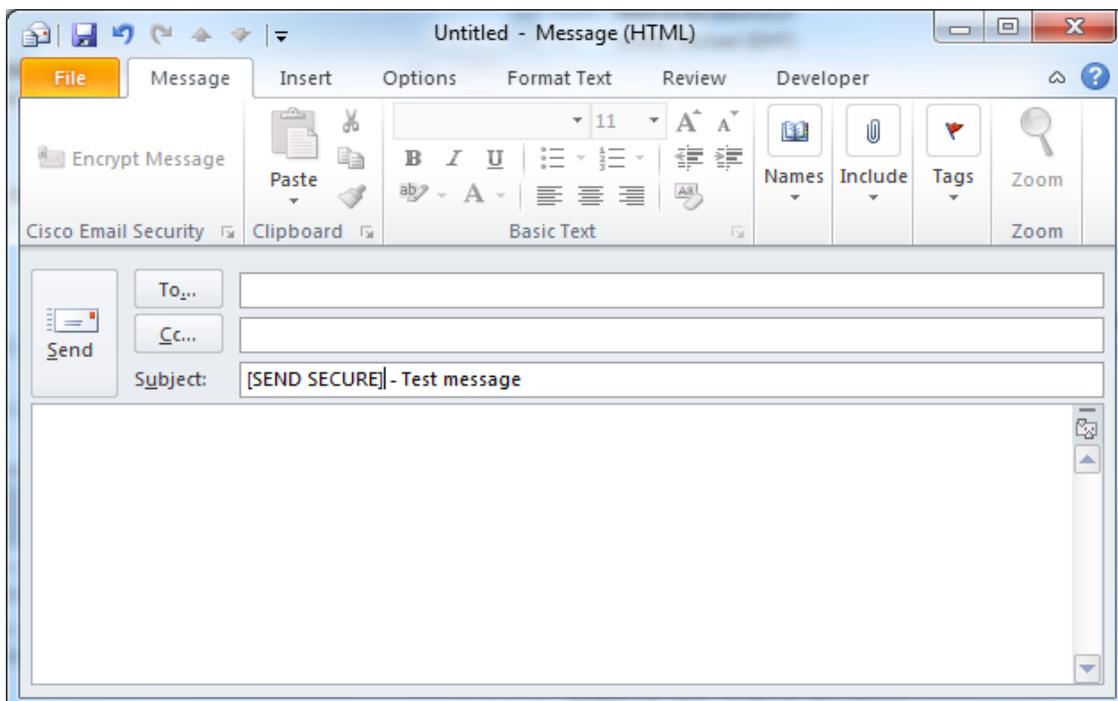
Messages can also be encrypted if either the word **"ENCRYPT"** or the text **"[SEND SECURE]"** is entered exactly as shown (including capitalization) in the message **Subject**.

This allows users to encrypt messages that do not have the Cisco IronPort add-in for Outlook installed on their workstations.

- Example: Manually type **ENCRYPT** (in all caps) as the first word in the Subject line.



- Example: Manually type **[SEND SECURE]** (in all caps) as the first word in the Subject line.



3 Cisco Registered Envelope Service (CRES) Registration

3.1 CRES REGISTRATION PROCESS

1. Upon receipt of the first encrypted message, you need to complete registration before you are able to open the message. Click the **REGISTER** button to go to the registration page.



2. Complete the **New User Registration** form and click **“Register”** when complete.

NEW USER REGISTRATION

To assure future messages from this service are not accidentally filtered out of your email, please add "DoNotReply@res.cisco.com" to your Address Book or Safe Sender List.

* = required field

Enter Personal Information

Email Address michael.white@pa.gov

Language The language setting will be stored for future login and email notifications.

First Name*

Last Name*

Create a Password

Password* Enter a minimum of 6 characters or numbers. Passwords are case-sensitive. Your password must contain both letters and numbers.

Confirm Password*

Personal Security Phrase* Enter a short phrase that only you will know. This phrase will appear on message envelopes when you log in. When you see your phrase, you know you are logging in to our secure site. [More info](#)

Enable my Personal Security Phrase.

Select 3 Security Questions
You will be asked these questions in the future if you forget your password.

Question 1*

Answer 1*

Confirm Answer 1*

Question 2*

Answer 2*

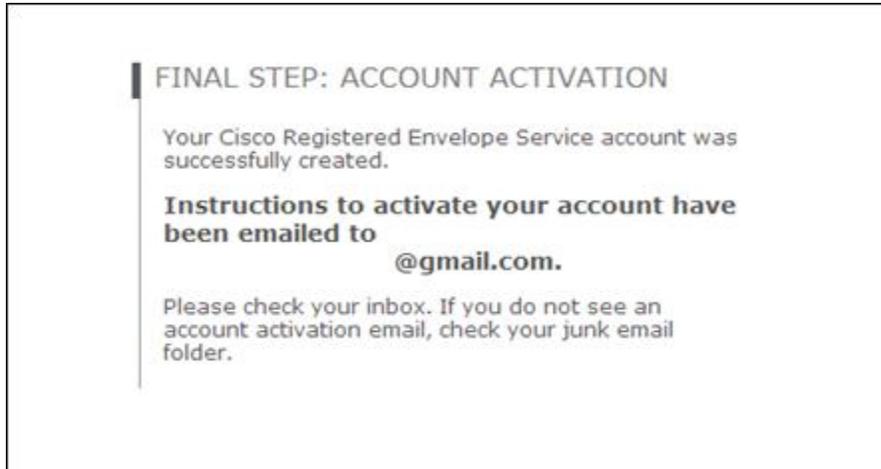
Confirm Answer 2*

Question 3*

Answer 3*

Confirm Answer 3*

3. After you complete the registration form, an activation message is sent to your registered email address.



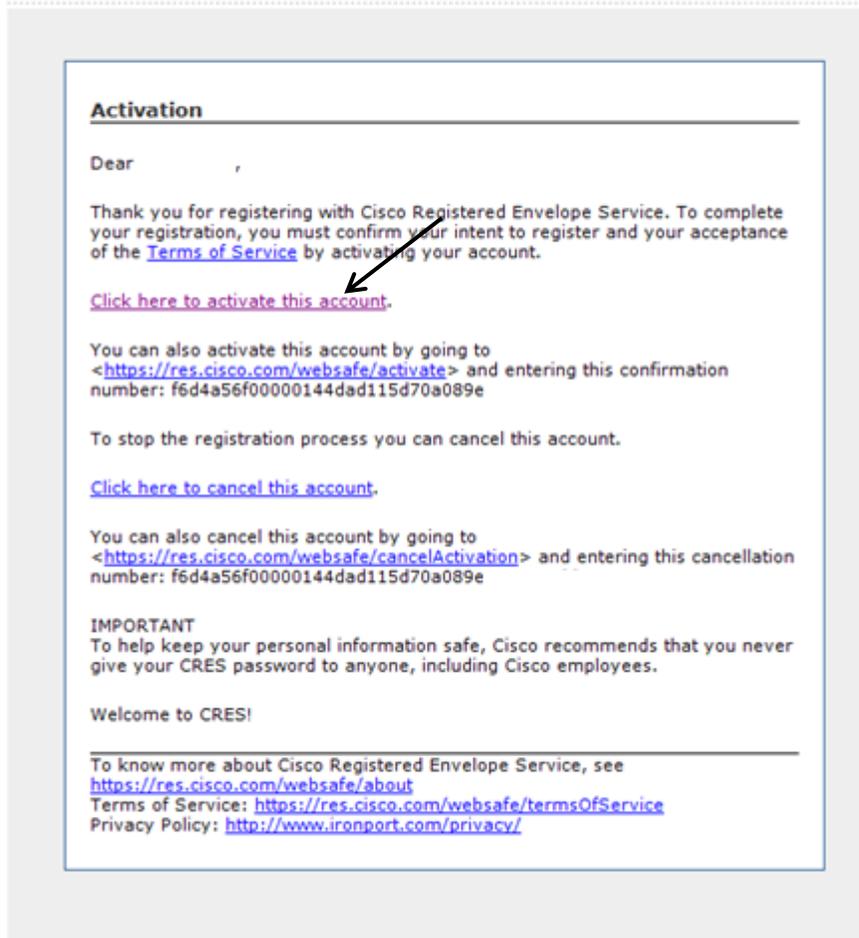
4. Open the activation message and select **"Click here to activate this account"** to complete activation of your CRES email encryption account.

Please activate with CRES

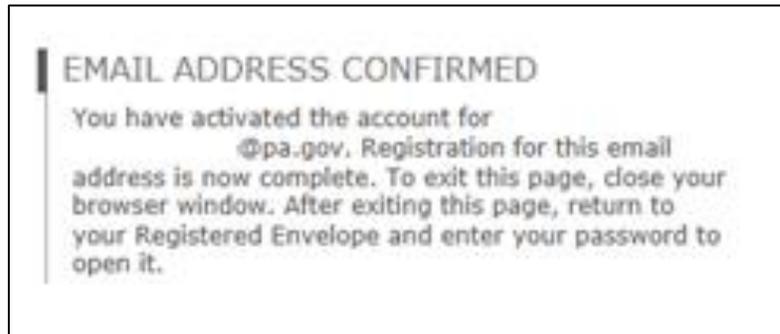
CRES Do Not Reply <DoNotReply@res.cisco.com>

Sent: Wed 3/19/2014 10:49

To: White, Michael (EMT)



5. After you activate your account, a confirmation message is sent to your registered email address. You can now return to your message and enter the password to open it.

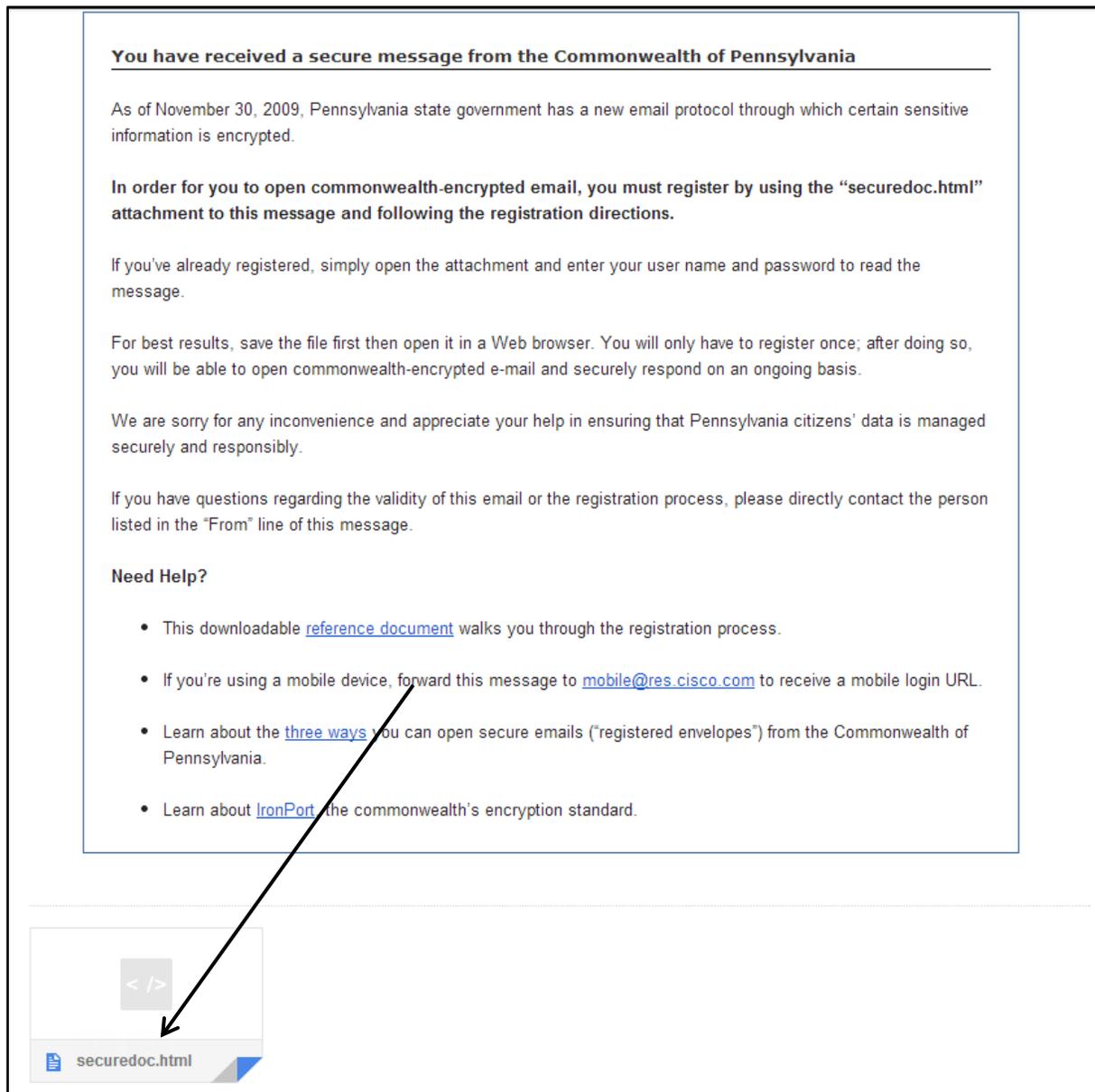


4 Receiving and Opening Encrypted Messages

4.1 OPENING A MESSAGE USING THE STANDARD METHOD

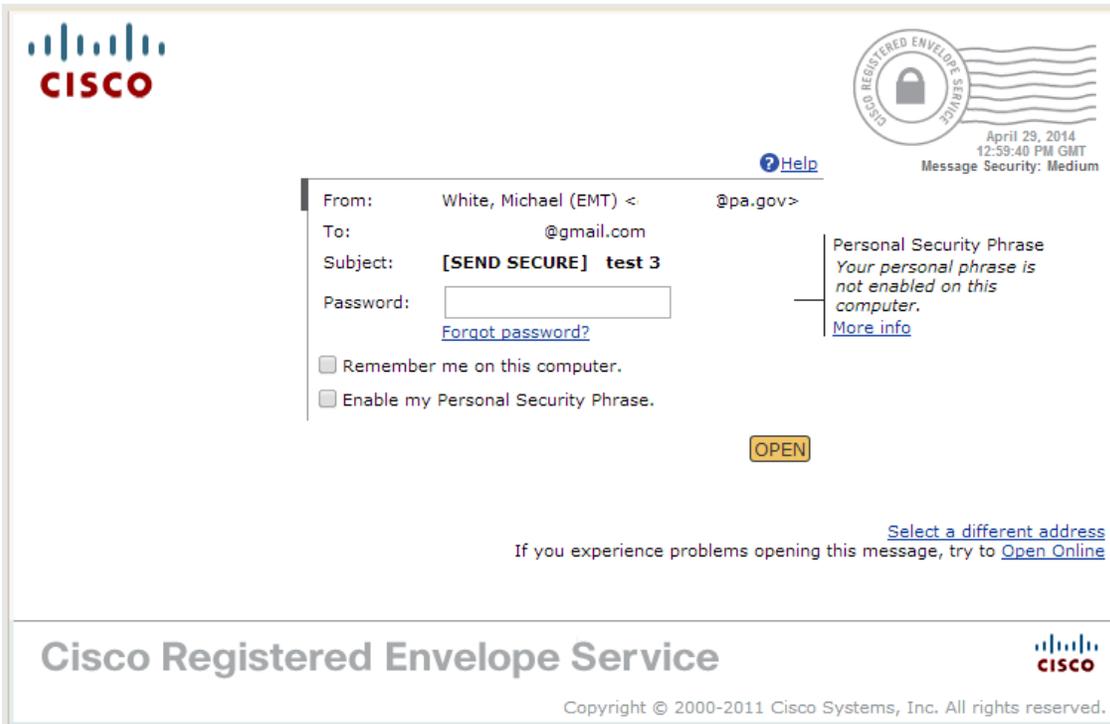
The external recipient receives a notification that they have received a secure message. Basic instructions for viewing the message are also displayed.

1. Click on the "securedoc.html" **attachment** to open the message.

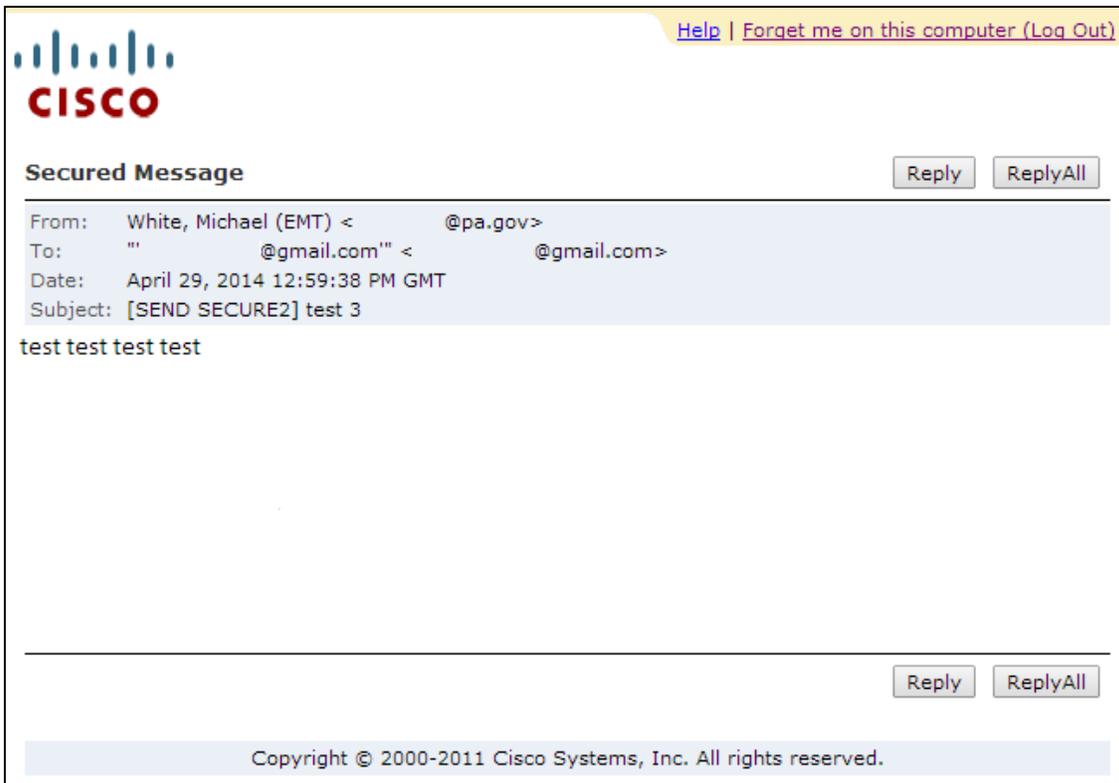


Note: You will be directed to complete registration upon opening the securedoc.html file if you have not previously done so.

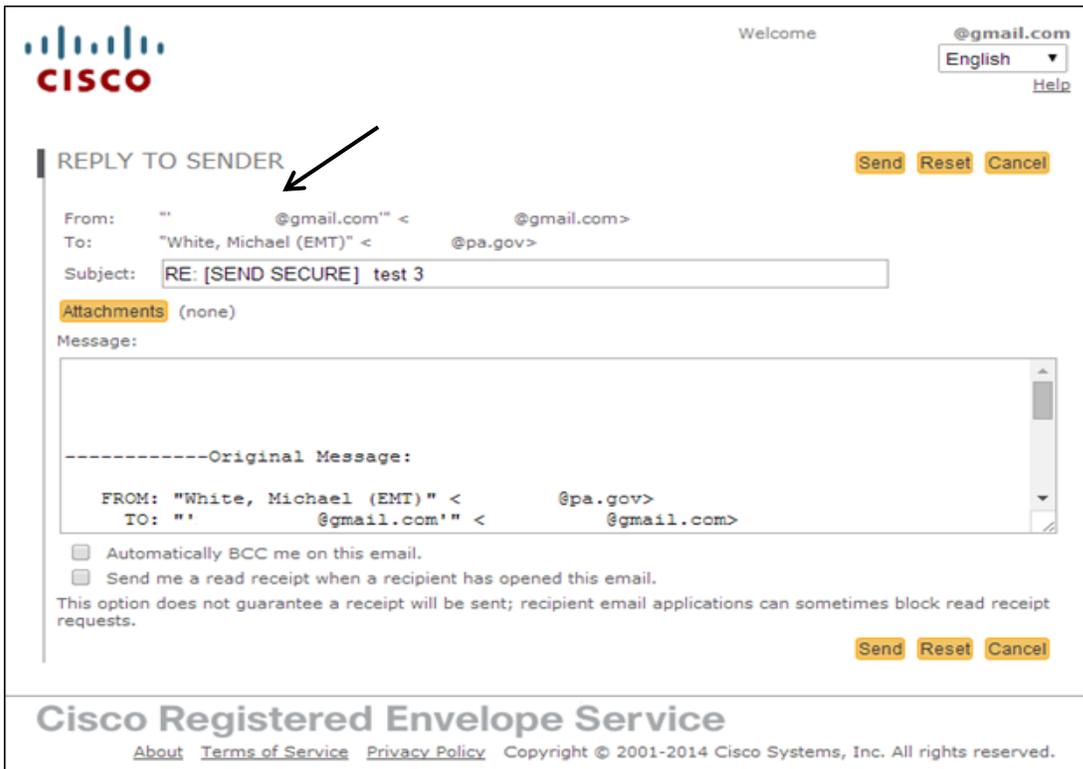
- 2. Enter the password you created during the registration process to open the message.



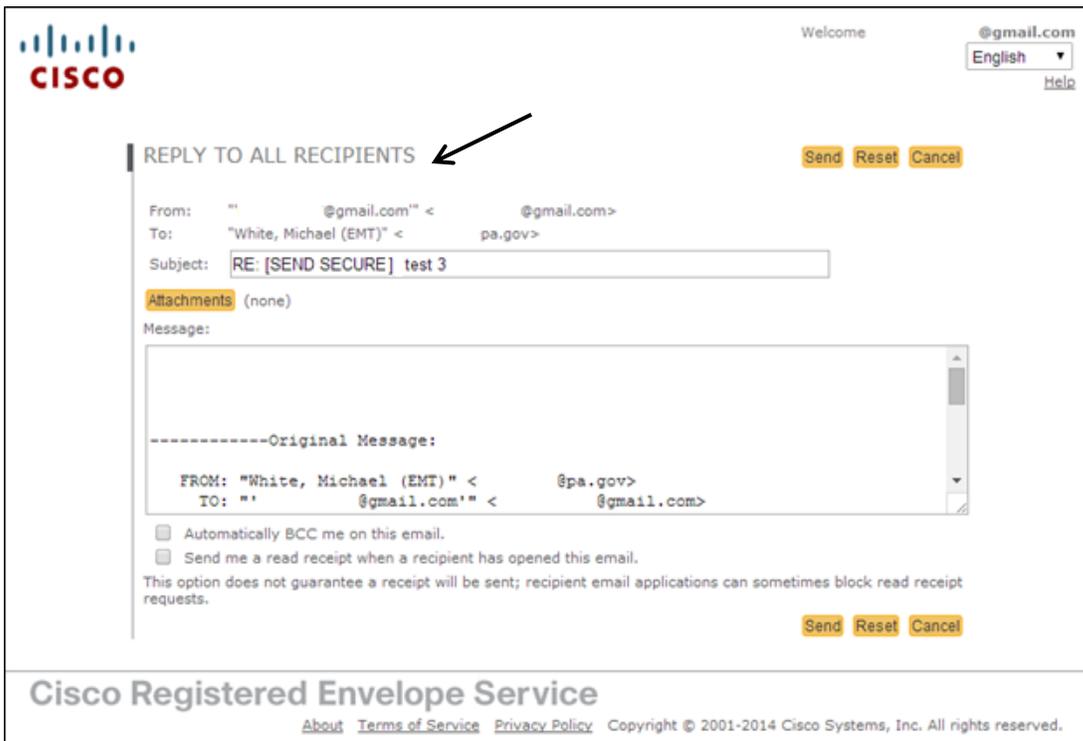
- 3. The message is decrypted and displayed and you are now able to reply to the message.



- 4. The "Reply" option generates an encrypted message addressed only to the message originator.



- 5. The "ReplyAll" option generates an encrypted message to the message originator and all other recipients of the message you received.



4.2 OPENING A MESSAGE USING THE OPEN ONLINE FEATURE

Use the **Open Online** method if you cannot open a message with the Standard method.

1. Enter your password and select "Open Online."

CISCO

CISCO REGISTERED ENVELOPE SERVICE

April 29, 2014
12:59:40 PM GMT
Message Security: Medium

[Help](#)

From: White, Michael (EMT) <@pa.gov>
To: @gmail.com
Subject: **[SEND SECURE] test 3**
Password:
[Forgot password?](#)

Remember me on this computer.
 Enable my Personal Security Phrase.

OPEN

[Select a different address](#)
If you experience problems opening this message, try to [Open Online](#)

Cisco Registered Envelope Service

CISCO

Copyright © 2000-2011 Cisco Systems, Inc. All rights reserved.

2. The message opens with the same "Reply" and "ReplyAll" options.

CISCO

[Help](#) | [Forget me on this computer \(Log Out\)](#)

Secured Message

Reply **ReplyAll**

From: White, Michael (EMT) <@pa.gov>
To: "" @gmail.com" <@gmail.com>
Date: April 29, 2014 12:59:38 PM GMT
Subject: [SEND SECURE2] test 3

test test test test

Reply **ReplyAll**

Copyright © 2000-2011 Cisco Systems, Inc. All rights reserved.

4.3 RECEIVING MESSAGES WITH ENCRYPTED ATTACHMENTS

Attachments are encrypted and decrypted along with the rest of the message.

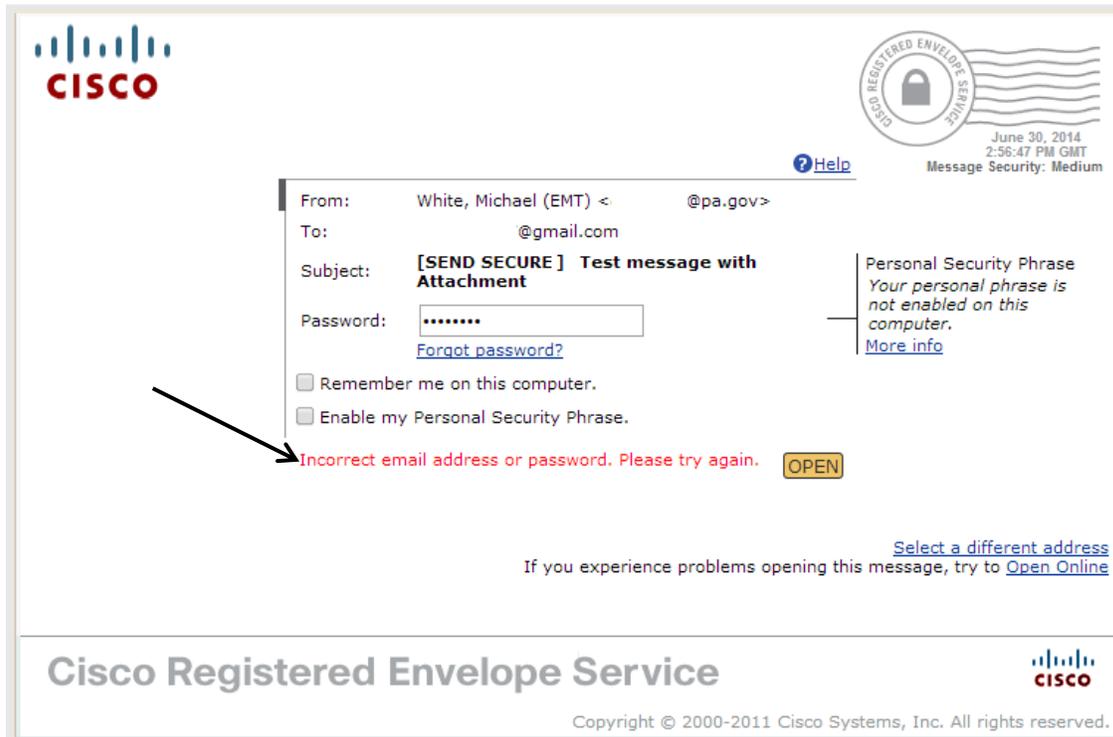
You will not see any attachments until you have successfully decrypted the message.



5 Resetting a CRES Account Password

If you have forgotten the password you created during the registration process, you can reset your password using the "Forgot password?" link.

1. If you provide incorrect credentials, you will get an error. Click "Forgot password?" to change your password.



2. Enter your Email Address or simply click "Continue" and an email will be sent to your registered email address to change your password.

FORGOT PASSWORD

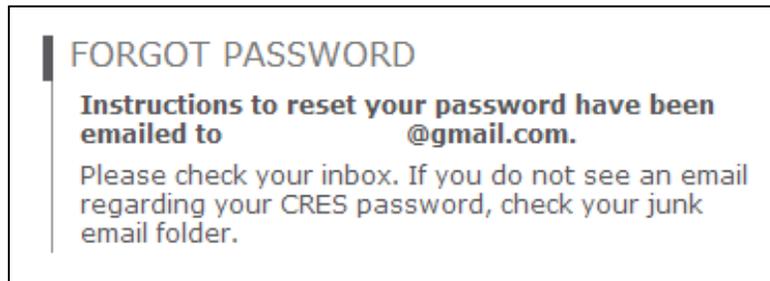
We'll email you a link to a page where you can easily create a new password.

To assure our messages are not accidentally filtered out, please add "DoNotReply@res.cisco.com" to your Address Book or Safe Sender List.

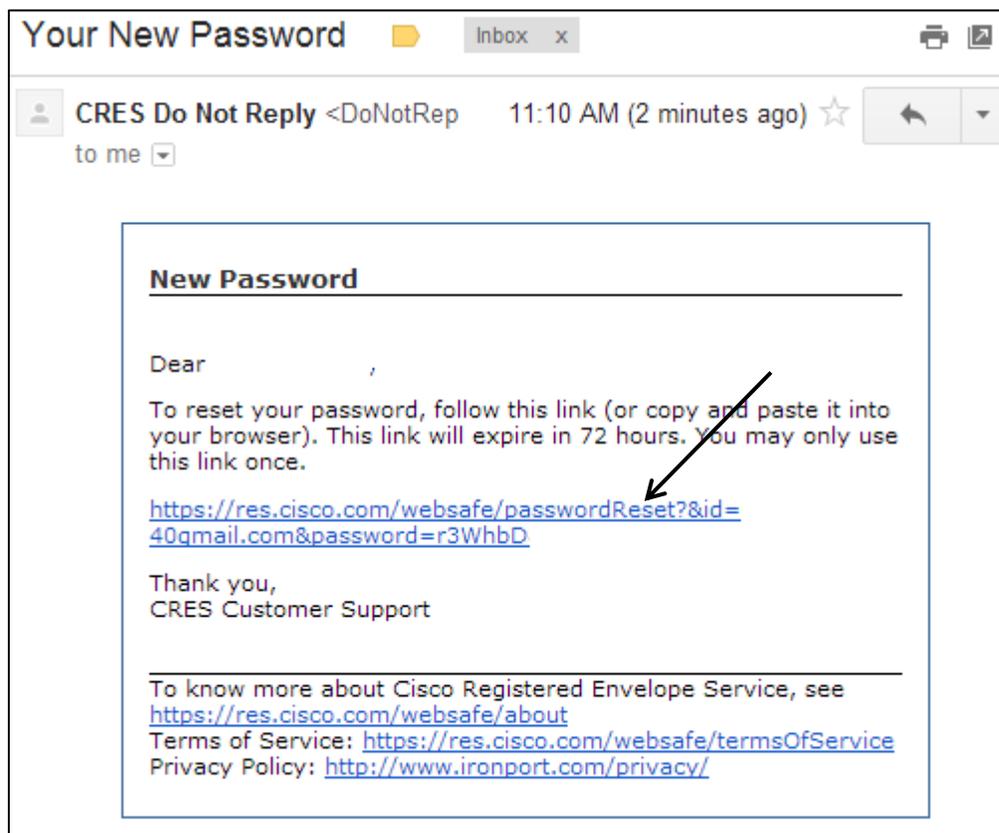
If you are authenticating using single sign on, please contact your Identity Provider for assistance.

Email Address

- A confirmation message is displayed directing you to check your inbox for the CRES password reset message.



- Go to your email account and open the CRES password reset message. Select the **password reset link**.



5. Answer the **security questions** that you completed during your initial registration and click "Continue."

SECURITY QUESTION

Please answer the following security questions to reset your password.

What is your father's middle name?

What is your oldest cousin's first name?

What is your mother's middle name?

[Continue](#)

6. Once you answer the questions correctly, you can create and confirm a new password. Click "Continue" when completed.

CREATE NEW PASSWORD

Enter a minimum of 6 characters or numbers. Passwords are case-sensitive. Your password must contain both letters and numbers.

New Password

Confirm Password

[Continue](#)

7. A confirmation message is displayed indicating that the password has been successfully updated. Click the link to return to the encrypted message where you can log in with the new password.

PASSWORD SUCCESSFULLY UPDATED.

Your password has been changed.

Return to the encrypted message envelope to log in and read your message or [click here to log in](#).

6 Appendix A – Additional Information

6.1 SUPPORT

To resolve issues with sending or opening encrypted emails, contact your local Agency IT administrative staff as you would for any other technical computer issue.

6.2 REFERENCES

Refer to the E-mail Encryption web page for additional information and for access to this user guide:

http://www.portal.state.pa.us/portal/server.pt/community/email_exchange/748/email_encryption/1355066