_			
	ra	m	
	··		

Sent:

Thursday, November 10, 2005 3:25 PM

To:

Subject:

Latest version

Attachments: ExchangeArchiveSOPv3.0.doc; CheckList.xls

Attached. Also a spreadsheet I put together for the Check List, which is also imbedded into the process document, use as you will.

And for those informed minds,

Crytonomicom and the Quicksilver.

STANDARD OPERATING PROCEDURES (SOP)

MS Exchange Electronic Mail Archival Process

for

The Executive Office of the President



Office of Administration

Office of the Chief Information Officer

November 2005

Document Information

Document ID	EOP-OA-OCIO-ExchangeArchiveSOP
Version	3.0
File Name	ExchangeArchiveSOP.doc
Revision Date	November 11, 2005
Owner	Information Systems & Technology, Office of
	Administration, Executive Office of the President
Description	Standard operating processes and procedures for the
	archiving of electronic mail messages and the auditing of
	the archival process.

DOCUMENT RECORD OF CHANGE

All changes to this document MUST be recorded using the below Record of Changes, which should list the page number, change comment, and the date. All changes must be signed off on by the person responsible for the changed area.

		Record of Chan	ges	
Page Number	Change	Comment	Date of Change	Signature
			·	
	-			
·				
·				
·				

Version 3.0 – November 11, 2005

Page 2 HOGR60A-021993

Table of Contents

1.0	Exchange Email Archival Process Functionality & Audit Check	4
1.1.	Monitoring	4
1.2.	Set Up	4
1.3.	Archiving (IS&T/SIS)	5
1.4.	Daily Verification	6
1.5.	Weekly Verification	8
	Roles and Responsibilities	

Version 3.0 – November 11, 2005

Page 3 HOGR6OA-021994

1.0 Exchange Email Archival Process Functionality & Audit Check

1.1. Monitoring

Monitor any and all servers that support both the Exchange email journaling process (currently) and the PST archive files (currently on a continuous basis to ensure that each server is still active and functioning. The following must be monitored:

CPU utilization – If CPU utilization is greater than 75% with a wait queue length greater than 3 for more than five minutes, generate an alarm.

System Memory – If virtual memory usage exceeds 90%, generate an alarm. If physical memory exceeds 75%, generate an alarm.

Storage Capacity - On the server maintaining the journal files, if any partitioned storage device reaches 80% capacity, generate an alert. If any partitioned storage device reaches 90% capacity, generate an alarm. On the server maintaining the PST files, if any partitioned storage device reached 70% capacity, generate an alert. Generate an alarm at 80% capacity.

Server Activity - If the server cannot be polled, generate an alarm.

Application Activity – On the server maintaining the PST files, ensure that the Mail Attender application is up and running. Generate an alarm if it is not. Note that this application should be defined as a Tier 1 application until the implementation of ECRMS makes it no longer a needed process.

Polling should be performed no later than 1 minute apart. Support personnel must respond to events that trigger alarms based on the priority of the alarm. Refer to the Service Level Monitoring document which defines the standards used within EOP for the monitoring of different tiers of systems. The email archival process is part of the Message systems within EOP and is classified as a Tier 1 system and must be monitored accordingly.

1.2. Set Up

Prior to the implementation of the email archival processes, perform the following steps:

- 1. Create twenty test email ids for each component, with two or more emails associated with each journal file. These will be used for the daily and weekly verification steps. These should be structured as XXXXX_TESTNN@XXXXXX.EOP.GOV, where XXXXX is the EOP component found in Table 1, and NN is a two digit sequential number starting with 01.
- 2. Create one email id that will be used to send test emails from. This should be created within the OA component. This email should be created as AUDIT_EMAIL_ID@OA.EOP.GOV. Associate this id with the first OA journal file.
- 3. Remove all PST files from the journal file server, currently
- 4. Ensure that all PST files on the PST server, currently directories, that is, as defined in section 1.2 item 5.
- 5. Configure the Mail Attender rules so that the following naming constructs are used:
 - a. A separate drive will be used for each year of mail messages.
 - i. E\$ 2002, 2003
 - ii. F\$ 2004

Version 3.0 - November 11, 2005

Page 4 HOGR6OA-021995

- iii. G\$ 2005 (minus PST files for OMB)
- iv. H\$ 2005 (OMB PST files)
- v. I\$ All Issues and Other files
- vi. J\$ 2006 (minus PST files for OMB)
- vii. K\$ 2006 (OMB PST files)

On a go forward basis there will need to be two drives for each subsequent year allocated similarly to vi and vii above.

- b. Within the appropriate drive, a directory will be created using the component acronym defined in Table 1.
- c. Within the component directory, a directory will be created with the four digit year.
- d. The file name will follow the following convention: MS_XXXXX_YYYYMMDD_NN_QQQQQQQPST. There is a one to one correlation between journal files and PST files.
 - i. MS indicates the file is a Message Store
 - ii. XXXXX is the component as found within Table 1
 - iii. YYYY is the four digit year of the date the PST is created
 - iv. MM is the two digit month of the date the PST is created
 - v. DD is the two digit day of the month of the date the PST is created
 - vi. NN is the two digit sequence number starting from 01 of the PST file created for each journal file within that component, incremented by 1.
 - vii. QQQQQQ is the name of the journal file that was used to create the PST file, to uniquely identify the multiple PST files created by the process.

This naming convention will be used for all files created on the PST server. For example, G\$:/ONDCP/2005 will hold PST files for ONDCP created in 2005, and MS_ONDCP_20051028_01_ONDCP01PST is the PST file created for ONDCP from journal ONDCP01.

6. Ensure that all of the journal files have been flushed out to the greatest extent possible before this process is implemented.

The Mail Attender process will key off of the message received date, and will be based on the time in the Eastern Time zone for consistency. Once the messages are place in the appropriate PST file, the journal file will be flushed of all of the archived messages. Note that the Mail Attender rules will be configured to process all messages for the previous day and prior, to ensure that all messages are accounted for in the event of Mail Attender processing problems.

1.3. Archiving (IS&T/SIS)

Start the electronic message archiving process daily at 12:01am:

Determine and save the number of messages within the journal file for the preceding day and
prior using the MailStats software. This will initially be a manual process; the count should be
kept in a spreadsheet associated with the journal name and the file name of the PST that is
created. When automated, this number will be stored within the Inventory Daily Process
database.

Version 3.0 - November 11, 2005

Page 5 HOGR60A-021996

- 2. Execute the Mail Attender procedure. The rules that Mail Attender uses will be configured to process all messages from the previous day and before. If the preceding step is manually implemented, start this procedure manually upon completion of Step 1. If the preceding step is automatic, start this procedure at the conclusion of Step 1 in the same script file that processes Step 1.
- 3. In the initial manual process, update the daily spreadsheet with the date and time the Mail Attender process ran, the from directory path and name of the journal file, the to directory path and name of the resulting PST file, the earliest received date and time found within the PST file, the latest received data and time found within the PST file, the size of the PST file, and the number of messages found within the PST file. This information is derived from the Mail Attender log file. When this step is automated, this information will be stored within the Inventory database via an automated procedure. This process inventory database will be used for independent verification during the Independent Verification and Validation (IV&V) process.

1.4. Daily Verification

After the Mail Attender process has run, the email archival process functionality should be verified using the following checklist (the group responsible for the step is indicated in ()'s after each step):

- 1. On the journaling server, ensure that no PST files are resident on any storage device associated with the server. (IS&T/SIS)
- 2. On the PST server, ensure that no PST files are resident on the C:\ system drive, and that all PST files are stored within the appropriate directory based on the defined naming conventions. This should be an automated process and run once per day, at the conclusion of the PST file creation facilitated by the Mail Attender software. (IS&T/SIS)
- 3. Count the number of PST files created on the PST server after the Mail Attender process is run. For the current Exchange 2000 environment, the number of PST files created per component must be greater than or equal to the exact number of journal files that are being flushed. When there are more PST files created for any individual journal file, send an alert to the operations support personnel. If there are fewer files, than send an alarm as an FYI to the operations support personnel for review. Do not store more than one journal file into any given PST file. For Exchange 2003 there must be a one to one correlation between journal files and created PST files. When there are not an equal number, send an alarm to the operations support personnel.

This will initially be a manual process, and can be determined by analyzing the daily spreadsheet of journal files and created PST files created in the previous archiving step. The Mail Attender process will limit the size of the PST files to 1.729 Gigabytes; after this is reached, Mail Attender will create another PST file with the appropriate name, with an increment of 1. Do not archive more than one journal file into any PST file. (IS&T/SIS)

Version 3.0 - November 11, 2005

Page 6 HOGR6OA-021997 The current number of journal files is 59, broken down into the following components:

EOP Component	# of Journal Files
CEA	2
CEQ	2
NSC	4
OA	5
ODNITT*	2*
OMB	8
ONDCP	3
OPD*	<i>1</i> *
OSTP	2
OVP	3
PFIAB	2
USTR	10
WHO	15

Table 1 – EOP Components and corresponding number of journal files

- *NOTE The above table shows the component journal files that are currently defined. Steps for adding and deleting journal files must be defined when journal files are no longer needed, or additional journal files for a specific component are needed, or a new component is added with its corresponding journal files. This will result in changes to the Inventory database (when implemented) and/or the spreadsheet used in the manual verification process.
- 4. Using the information found in step 1 of this archive process and initially using the spreadsheet from previous days/weeks processing, re calculate the average journal size for that day of the week for that PST file from the corresponding day of the week over the last six (6) weeks, and update the greatest and smallest PST sizes for that day of the week for that PST file. These should be maintained in the spreadsheet as well. (IS&T/SIS)
- 5. Using the information found in step 1 of this archive process and initially using the spreadsheet from previous days/weeks processing, re calculate the average number of messages for that day of the week for that PST file from the corresponding day of the week over the last six (6) weeks, and update the greatest number of emails and the smallest number of emails for that day of the week for the PST file. (IS&T/SIS)
- 6. Sign off on the daily process check list (found in Appendix A) and forward to IA, along with the spreadsheet information generated from the previous steps.
- 7. Using the checklist and spreadsheet forwarded from IS&T, compare the PST file size from the current day's PST files with the average daily PST size for that PST file for that day of the week. If there is more than a 20% plus or minus difference for that file, generate an alert. Note that holidays will affect these numbers and should be accounted for as best as possible. As an alert, the basis for this difference should be investigated as quickly as possible. This initially will be a manual process. (IA)
- 8. Compare the PST message count from the current day's PST files with the average daily PST message count for that PST file for that day of the week. If there is more than a 20% plus or minus difference for that file, generate an alert. Note that holidays will affect these numbers and should be accounted for as best as possible. As an alert, the basis for this difference should be investigated as quickly as possible. This will initially be a manual process. (IA)

Version 3.0 – November 11, 2005



Page 7 HOGR60A-021998

- 9. Verify that the overall email archival process ran correctly by performing a search for email generated on the preceding day (note that the first day this process is run there will be no emails from the preceding day to check). Follow the following steps:
 - a. Generate a test email in the afternoon of each day to be sent to a random number of test emails for a specific component each day from the originating audit test email id. Record the component and addresses that the email will be sent to. Within the subject and body of the email, include the phrase "Archival Test Message NN, created date YYYYMMDD", where NN is the two digit sequential test number starting with 01 (maintained within the database supporting this audit process) and YYYY is the four digit year of the date the email is sent, MM is the two digit month of the date the email is sent, and DD is the two digit day of the date the email is sent.
 - b. Send the email generated in step 1 to the addresses defined in Step 1.
 - c. The following afternoon, perform a standard search looking for the pattern "Archival Test Message NN, created date YYYYMMDD" using the information from the previous day's test email. The number of emails for the targeted component should match the numbers determined in Step a above. If this is an exact match, the archival process is working correctly. If there is any deviation, the process has not worked correctly and an alert should be generated for immediate checking by IS&T and IA.
- 10. Fill out the daily check list with the results of these steps, and sign the appropriate area of responsibility. This form is defined at the end of this document. Disseminate and store appropriately. Additionally, forward the daily check list to the Federal Records Management Group at FAX:

 to the attention of the FRMG Manager. (IA)

This concludes the daily functionality check for the archival process.

1.5. Weekly Verification

Verify the email archival process functionality on a weekly basis.

- 1. Generate a test email on Friday of each week to be sent to a random number of TEST email addresses within a random set of components from the originating audit test email id. Record the components and addresses that the email will be sent to. Within the subject and body of the email, include the phrase "Archival Test Message NN, created date YYYYMMDD", where NN is the two digit sequential test number starting with 01 (maintained within the database supporting this audit process) and YYYY is the four digit year of the date the email is sent, MM is the two digit month of the date the email is sent, and DD is the two digit day of the date the email is sent.
- 2. Send the email generated in step 1 to the addresses defined in Step 1.
- 3. On the following Monday, perform a standard search looking for the pattern "Archival Test Message NN, created date YYYYMMDD" using the information found in the preceding week's test email. The number of emails per component should match the numbers stored from Step 1. If this is an exact match, the archival process is working correctly. If there is any deviation, the process has not worked correctly and an alert should be generated for immediate checking by IS&T and IA.
- 4. When all checks and audits of the email archival process are complete for the week, the Federal Records Management Group must certify that the integrity of the email archival process is intact, for external audit purposes. The daily check list should be signed off in the correct location that the results have been certified for the week. Once this check list is complete, it should be disseminated and stored as appropriate. (FRMG)

Version 3.0 - November 11, 2005

Page 8 HOGR6OA-021999

2.0 Roles and Responsibilities

The email archival process requires extremely detailed measures and management oversight to ensure that errors in the archival process, such as gaps in the timelines of email files, missing and misnamed files, etc. does not occur. This is extremely important due to the nature of the emails and the critical role they play in the checks and balances of the Executive Office of the President.

The roles and responsibilities for these processes include:

Role/Process	Responsibility	Frequency
Active Email Archiving and Tracking	Information	Daily
	Systems and	
	Technology (IS&T)	
Reconciliation of Counts and Size	Information	Daily
	Assurance (IA)	
IV&V (ensuring the tracking	Information	Weekly
spreadsheet/database is complete with no	Assurance (IA)	
gaps/holes for dates/components and 100%		
compliance on all procedures)		
Records Management Certification (checking	Federal Records	Weekly/Monthly
that IA validation has been complete and that	Management Group	
correct number of test emails are archived	(FRMG)	
properly)	·	

Version 3.0 – November 11, 2005

Page 9 HOGR6OA-022000

Check List - Page 1

Da	te:	
1.	Use Mail Stats and record the number of messages per journal file	
2.	Run Mail Attender Procedure	
3.	Update daily spreadsheet with (see third page)	
	3.1. Date and time Mail Attender ran (start/end times)	
	3.2. Journal File Name / PST file name	
	3.2.1. Journal message count/earliest received date/latest received date	
	3.2.2. PST message count/earliest received date/latest received date/file size	
4.	Ensure no PST files are resident on the Journal server's storage devices	
5.	Ensure that no PST files are resident on the PST server's C drive	
6.	Ensure that all PST files within any given directory share the same component in	
	their filename as in the directory path	
7.	Check the number of PST files created.	
	7.1. If less than the number of journal files, alert operations staff that Mail Attender	
	did not run properly	
	7.2. If greater than, ensure that no improperly named files were created, and that	
	one of the journal files was excessively large for the day, resulting in multiple	
	PST files being created	
8.	Calculate average PST message count for that journal for day of week over 6 weeks	
9.	Sign check list, forward with spreadsheet to IA	
n	AII V Signed Ry	IS&T

Version 3.0 - November 11, 2005

Page 10 HOGR6OA-022001

Check List Page 2

10. Compare daily PST file size with average PST file size	
10.1. If 20% difference, alert IS&T and IA	
11. Compare daily PST message count with average PST message count	
11.1. If 20% difference, alert IS&T and IA	, ·
12. Create and send daily test emails (single component)	
13. Run daily audit search check for previous days emails	
13.1. If messages not found, alert IS&T, IA, and FRMG	
14. Sign check list, forward with spreadsheet to FRMG	
DAILY Signed By: Signature:	IA
Weekly Audit Check	
15. Create and send weekly test emails (all components)	
16. Run weekly audit search check for previous days emails	
16.1. If messages not found, alert IS&T, IA, and FRMG	
17. Sign check list	
WEEKLY Signed By: Signature:	FPMC

Version 3.0 – November 11, 2005

Page 11 HOGR6OA-022002

	Page 1		PST PST 1st Message Last Message																							
ck List			PST Msg Count																	-					Page 12	
SOP for Exchange Email Archival Check List			PST PST File Name Size																							
SOP for Exchange			PST Directory Path																							
			JOURNAL Last Message																							
at			JOURNAL 1st Message																							
e of the Presider			JOURNAL Msg Count																						mber 11, 2005	
Executive Office of the President	Archive Process Daily Stats	Date: Day of the Week: Weekend? (Y/N) Holiday? (Y/N) Start Time:	JOURNAL File Name	CEA01 CEA02	CEQ01	NSC01	NSC02 NSC03	NSC04	OA02	OA03	OA04	OA06	ODNITT01	ODNITT02 OMB02	OMB03	OMB04	OMB05 OMB06	OMB07	OMB08	OMB09	ONDCP01	ONDCP02	OPD01	; } ; ;	Version 3.0 - November 11, 2005	
																					Н	OG	R60	DA-02	2003	

			_																															
	Page 2	PST Last Message																																
		PST PST Msg Count 1st Message																																
ck List		PST Msg Count																																
ival Che	•	PST Size																																
e Email Arch		PST File Name																																
SOP for Exchange Email Archival Check List		PST PST Directory Path File Name																																
		JOURNAL Last Message																																
Ħ		JOURNAL 1st Message																																
of the Presider		JOURNAL Msg Count																																
Executive Office of the President	Archive Process Daily Stats	JOURNAL File Name	OSTP01	OSTP02	OVP01	OVP02	OVP03	PFIABO1	PFIABUZ HOTEGA	USIRO1	USTR02	USTR03	USTR04	USTR05	USTR06	USTR07	USTR08	USTR09	USTR10	WHO01	WHO02	WHO03	WHO04	600H/W	WIIO00	00 M	000L/W	WHOOS	200	- 6101	WHO 12	WHO I	WHO15	2

Page 1		PST e Last Message		
		PST 1st Message		
		PST Msg Count		
		PST Size		
		PST File Name		
		PST PST Directory Path File Name		
•		JOURNAL Last Message		
		JOURNAL 1st Message		
	1/31/2008 Thursday	JOURNAL Msg Count		
Archive Process Daily Stats	Date: Day of the Week: Weekend? (Y/N) Holiday? (Y/N) Start Time: End Time:	JOURNAL File Name	CEA01 CEA02 CEQ02 NSC01 NSC03 NSC04 OA02 OA05 OA05 OA06 ODNITT01 OMB02 OMB03	OMB06 OMB07 OMB08 OMB09 ONDCP01

~
•
<u> </u>
10

Archive Process Daily Stats

	PST Last Message												
	PST 1st Message												
	PST Msg Count												
	PST Size												
	PST File Name												
	PST Directory Path	0 0	0 .	0 0	0	0				00	0		
*	JOURNAL Last Message	4 · ·						·					
	JOURNAL 1st Message												
1/31/2008 Thursday	JOURNAL Msg Count												
Date: Day of the Week: Weekend? (Y/N) Holiday? (Y/N) Start Time: End Time:	JOURNAL File Name	ONDCP02 ONDCP03 OPD01	OSTP01 OSTP02	OVP02 OVP03	PFIAB01 PFIAB02	USTR01 USTR02	USTR03	USTR05	USTR07	USTR09	USTR10	WHO01 WHO02	WHO03 WHO04

Φ
₽
10

	PST Last Message	
	PST PST Msg Count 1st Message	
	PST Msg Count	
	PST Size	
	PST File Name	
	PST PST Directory Path File Name	00000000
	JRNAL JOURNAL lessage Last Message	
1/31/2008 Thursday	JOURNAL JOU Msg Count 1st M	
Date: Day of the Week: Weekend? (Y/N) Holiday? (Y/N) Start Time: End Time:	JOURNAL File Name	WHO05 WHO06 WHO07 WHO11 WHO12 WHO13 WHO15

HOGR6OA-022007

Archive Process Daily Stats