WHITE PAPER:
CAPSTONE COMPLIANCE

Archiving and eDiscovery for U.S. Government Agencies

Capstone Compliance Using Symantec Archiving and eDiscovery Solutions

Who should read this paper

IT decision-makers, architects, records-management professionals and archiving administrators responsible for compliance with the Federal Records Management Directive of 2012, especially those using or considering Symantec archiving and eDiscovery products.

Symantec

Content

Capstone overview

Government agency email volume has outstripped the capabilities of paper-based records management. To modernize records management, and improve compliance with existing laws like the Freedom of Information Act, the Obama administration issued a directive for federal agencies to convert records to electronic formats, and assigned NARA to oversee compliance. The "Capstone" guidelines issued by NARA were designed to help federal agencies develop their compliance strategy by providing advice for electronic capture and management of email records. Bulletin 2013-02 summarizes the process for agencies considering whether and how to implement it.

While not a requirement, Capstone is an excellent way for agencies to meet the obligations outlined in the OMB memos: OMB – 12-18 [http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf], and the follow-up memo OMB – 14-16 [http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-16.pdf]. The latter memo reminds agency leaders that full compliance for email records is expected by the end of 2016.

To encourage adoption, Capstone was designed for easy implementation using technologies already in place, with flexibility in:

- Scope, whether agency-wide, or across selected groups, offices, or regions
- Capture of new email only, or with recapture of legacy email
- Deployment in stages or simultaneously across the agency
- End-user involvement in records classification and management

In September 2014, NARA published a follow-up report to section A 3.1 of their original guidance in the OMB – 12-18 memo that included an assessment of technology options for automation of electronic records management. They outline a range of options which are listed below:

- No Automation; manual management of electronic records
- Rules-based automation
- Business process and workflow automation
- Modular re-usable records management tools
- Auto-categorization

This paper describes how to achieve, maintain, and document Capstone compliance, utilizing a modular family of Symantec solutions that map to the above automation framework from NARA's September 2014 update. The Symantec solutions can be used all together, or as individual technology components, and include the Enterprise Vault archiving platforms and the Symantec eDiscovery Platform (powered by Clearwell). Since it's on-premises and cloud archiving platforms are very similar, "Enterprise Vault" will be used to refer to both, with differences noted as they come up and summarized in an appendix.

Implementing Capstone—key decisions

Capstone guidelines lay out a straightforward approach that gives agencies considerable flexibility. However, a few early decisions, as outlined below, have significant impacts on the coverage, resource consumption, and complexity of a records management solution.

Account types and retention periods

The most basic approach to Capstone compliance is user-based retention: agencies select user accounts for retention and capture all their email automatically. Accounts selected for indefinite retention are called "permanent accounts;" email in the remaining "temporary accounts," is deleted after a set period of time.

Capstone recommends permanent accounts for:

- Officials at the higher levels of agencies or component organizations
- Staff members in positions that regularly create or receive email presumed to be of permanent value
- Anyone else who creates or receives email of permanent value

NARA recommends that agencies consult the United States Government Policy and Supporting Positions (Plum Book), U.S. Government Manual, and other sources when assigning permanent account status.

Symantec Enterprise Vault can easily support this approach through what NARA refers to as *Rules-based Automation* technology to act on the email created by these account types and automatically retain it as required. If an agency uses Enterprise Vault, accounts are made permanent or temporary simply by assigning them to provisioning groups with different retention times (on-premises version), or assigning different retention times to individual accounts (cloud version).

Method of capture - journaling or mailbox archiving

NARA notes that email may be captured by either journaling or mailbox archiving and Enterprise Vault supports both methods.

Journaling is a form of archiving that implements what NARA calls *Business Process and Workflow Automation*, because it automatically forwards a copy of all mail sent or received on the server to a journal; Enterprise Vault then archives messages from the journal. Journaling captures all email in target accounts with no user intervention and no loss, and is easier to set up than mailbox archiving. Enterprise Vault supports journaling from on-premise email servers such as Microsoft® Exchange, and IBM Domino®, as well as any cloud-based email systems that support the Simple Mail Transfer Protocol (SMTP) such as Office 365, and Google gmail.

Mailbox archiving is the type of archiving described above for Capstone's user-based retention method. Again, this is what NARA calls *Rules-based Automation*, which archives messages after they have arrived in end users' mailboxes according to policies that specify how long they should be retained.

If desired, Mailbox archiving can be used in conjunction with a data classification feature that will include a policy context for the type of content in the mailbox (see the item below on culling non-records for more information on content-aware policy automation) so that non-records can be omitted from the archive. Journaling, on the other hand, retains everything for an account.

Regardless of how content reaches the archive, all items are indexed using full text and metadata, deduplicated, and their retention policy applied. The retention policy defines when the item will be deleted from the archive, and may also indicate its record type. Enterprise Vault maintains the data and keeps it readily accessible for the specified period, and then deletes as specified by retention policies.

Culling non-records from permanent accounts

Enterprise Vault has content classification features that NARA would describe as *Auto-categorization* that allow email retention policies to be content-aware. This is useful to weed out emails that do not need to be retained. Otherwise, by default, all messages sent or received by permanent accounts are treated as though they were records under Capstone. But some messages clearly do not merit permanent retention, because they contain only transitory, personal, or routine procedural content. High proportions of such non-record email may make 100 percent capture expensive, impractical, or undesirable; therefore NARA recommends culling (deletion) of non-records, especially when the process can be automated. Enterprise Vault provides three ways to do this:

With either method of capture, Symantec Data Classification Services (DCS) offers fully automated record capture together with culling of non-records. DCS can tag, delete, archive, and set retention periods for content based on:

- Analysis of content and metadata
- Predefined rules and keywords in subject and message body
- Proximity searches for combinations of words
- Senders and recipients
- Newsletter content

With the mailbox archiving method of capture, messages arrive with a default retention period assigned according to the user's account. Agencies may allow end users to manually override the default categories, for example to cull non-records. This is done by using Enterprise Vault Policy Manager to create "retention folders" with assigned retention categories. This allows end-users to change a message's retention period simply by dragging it into a folder with a different retention period—for example, a "personal" or "non-record" folder. User can configure their email clients to automate this process using rules that place messages in retention folders according to source email address and other criteria.

Finally, for messages already in permanent accounts, culling may be done retroactively by using the Enterprise Vault search tool to find messages with keywords and metadata that identify them as non-records, and then manually deleting them.

Declaring records in temporary accounts

By combining rules-based automation and auto-categorization, email to and from temporary accounts is excluded from Capstone retention by default. But Capstone acknowledges that some of this email may need to be retained, for example because it documents interactions with permanent account users. For this reason, it may be necessary to reclassify messages as records for permanent retention. Enterprise Vault accomplishes this using the same set of tools used for culling non-records.

Just as Data Classification Services help cull incorrectly classified non-records in permanent accounts, they can help identify actual records in temporary accounts. Reclassification is based on keyword proximity, sender or recipient, and other criteria, using pre-existing rule sets provided with the tool or custom rules defined by the agency.

And in the same way agencies can use Enterprise Vault Policy Manager to define non-record retention folders for users with permanent accounts, they can set up permanent retention folders for users with temporary accounts. Typically, zero-day archiving policies are applied to these folders, so the next scheduled archiving run captures messages in them.

FOI and eDiscovery considerations

Search, Retrieve and Discover

Email archived by Enterprise Vault can still be easily accessed after it's undergone the archiving process. This is automated through shortcuts in the user's email client, or through the Enterprise Vault Search feature, even after being processed by the Enterprise Vault rules engine. The Search feature will automate the identification and retrieval of messages by group topic or keyword and the shortcuts will allow the user to click on individual messages to bring them up as long as there is connectivity to the Enterprise Vault server. To retain a copy of archived messages on client computers so that they can be accessed even when disconnected from the Enterprise Vault server, Enterprise Vault offers IMAP email client caching technology – or Virtual Vault caching technology specifically for Windows clients.

For more complex information discovery requirements Symantec offers eDiscovery solutions which fall into the automation category that NARA calls *Process and Workflow Automation*. eDiscovery is extremely useful to help federal agencies comply with Freedom of Information Act (FOIA) and other situations that require collection of categories of email over a long period of time,. As the Capstone guidelines suggest, Symantec eDiscovery automation solutions are able to:

- Collect a large body of topic-related or categorized information on-demand
- Impose a legal hold that preserves relevant records when litigation is anticipated
- Review potentially relevant records, and export them in a suitable format

Agencies should also have a plan and method for destroying non-records and temporary records after they no longer need to be retained, a process called defensible deletion.

Legal hold

Every Symantec eDiscovery solution—Symantec eDiscovery Platform (powered by Clearwell), Enterprise Vault Discovery Accelerator, and Discovery.cloud—provides legal hold for archived content. Items designated for legal hold are preserved in a repository and cannot be deleted or expired until the hold is lifted.

The Symantec eDiscovery Platform (powered by Clearwell) can impose legal holds on a per-item, per-custodian, or per-case basis. Records identified as relevant to multiple cases will not be released until all holds have been lifted. The solution can also run scheduled searches that add new content to an existing hold. When a case closes, users can quickly release all holds associated with it, allowing items to revert to their originally scheduled expiration dates. Symantec eDiscovery applications require no additional storage and provide detailed reports specific to legal holds.

Collect, Review and Export

Symantec eDiscovery solutions give legal staff a controlled environment and expanded search capabilities for enterprise-wide searches.

Symantec eDiscovery Platform (powered by Clearwell) provides managed workflow for agency-wide searches to meet litigation, FOIA, regulatory, or investigative requirements. Searches can be based on custodian, date range, classification, and keywords, using Boolean fields and attachment types to shape results. Result sets can be quickly culled in the analysis phase using advanced search-within-search, conversation threading, and other capabilities offered in a guided review.

To accelerate the process and reduce storage waste, records are de-duplicated during review and export. Users can run preliminary and test searches to isolate proprietary content from case audit trails, or to export selected item sets for review by outside counsel.

Symantec eDiscovery Platform (powered by Clearwell) also provides Transparent Predictive Coding (TPC) which gives review teams highly accurate results from minimal input. TPC generates search criteria from a set of known actionable and non-actionable items, and then applies them to a larger body of content. TPC significantly reduces review time and cost, and both the way criteria are generated and their accuracy across the case are completely transparent to reviewers.

Defensible Deletion

Deletion is generally acceptable when it adheres to a pre-determined policy, is not done in reaction to an event and doesn't violate other retention requirements. Enterprise Vault and EV.cloud both conform to record retention schedules, enforcing expiry in accordance with them.

Transfer of records to NARA

Permanent records are transferred to NARA for long-term retention; upon transfer they belong to NARA and not the sending agency. Guidance on how to transfer records is provided here, and the proper formats for email transfer here. Guidance on transfers includes:

- Transfer of e-mail records as an identifiable, organized body
- Preference for the .eml format for individual messages, but acceptance of the .msg format
- Acceptance of the .pst format for aggregate email
- Transfer of e-mail attachments in their native formats, for example .pdf, .jpg, and common office automation formats

All Symantec eDiscovery solutions can export email in .eml or .msg formats, or as .pst collections, with attachments in their native format and optional export of metadata. Results can be burned to permanent media for transfer or storage. The production module of Symantec eDiscovery Platform (powered by Clearwell)provides a load file configurator for creation of a customizable load during export. Expanded export options support any output format and many metadata formats, including .csv, .dat, .edrm, and .xml, and Concordance®, Relativity®, and Summation® load files.

Solutions for Capstone compliance

The volume of data created today makes the change from paper to digital archiving inevitable. Capstone was introduced to make this change easy to implement using systems already in place. As shown in this paper, Enterprise Vault, EV.cloud and Symantec eDiscovery Platform (powered by Clearwell)provide the tools needed for a successful Capstone implementation. Using journaling, account-level retention period assignments, or mailbox archiving, all versions of Enterprise Vault supports complete or granular capture of email to satisfy Capstone requirements within an efficient, resource-sensitive archiving framework.

Symantec understands that agencies' deployment needs vary, and designs its solutions with the flexibility to best meet an agency's immediate and long-term information management goals: through on-premises installation, as an outsourced (managed) service, in the cloud, or using a hybrid model.

- *Symantec Enterprise Vault*—The widely deployed on-premises enterprise archiving solution that gives agencies a central platform to optimize storage, enable retention and defensible deletion, and improve search and eDiscovery across Exchange and SharePoint, Domino, file servers, and other content sources (see Appendix 1).
- *Symantec Managed Enterprise Vault*—A monitoring, management, and support service for agencies that want to retain data on premises while enjoying the benefits of remote management. Customers support is provided by the Symantec Business Critical Services team, experts in service delivery and Symantec archiving technologies.
- *Enterprise Vault.cloud*—A cloud-based archiving service that helps agencies store, manage, and discover critical information. Enterprise Vault.cloud securely and defensibly captures information in a single repository, and delivers a highly intuitive end user experience, with seamless access and rapid search functionality. Built-in collaborative workflow gives legal teams role-based access to the archive, expediting eDiscovery.
- *Symantec eDiscovery Platform (powered by Clearwell)*—Advanced eDiscovery capabilities available for deployment on premises or using hosted, public, or private cloud models.

Symantec's best-of-breed solutions are a fast, reliable path for government agencies to achieve, maintain, and document compliance with Capstone requirements.

Appendix 1: Enterprise Vault Content Sources

Enterprise Vault supports archiving of unstructured electronically stored information, including but not limited to email and associated attachments, files, Instant Messaging, Social Media, and SharePoint. Enterprise Vault and EV.cloud provide full-content indexing and "future proofing" for more than 400 data types. A complete list of supported file types can be found here, and a detailed list of supported applications and versions can be found in the Enterprise Vault Compatibility Guide located here. They include:

- Microsoft Exchange
- Domino
- SharePoint
- File System Archiving
- Social Media, Instant Messaging, and Unified Communications throught partner integrations with Actiance and Globanet
- Database archiving through partner integrations with Informatica

Appendix 2: Comparing on-premises and cloud versions of Enterprise Vault

Enterprise Vault—on-premises archiving

- Archives email plus file system and SharePoint records
- Integrates with 3rd-party solutions for social and structured database archiving
- Includes options to move older content to cloud or tape storage
- Allows archived items to be accessed through Virtual Vault, a .pst-style view of archived records, or replaced with shortcuts.

EV.cloud—cloud-based archiving

- Archives email plus SharePoint, Box, and SalesForce Chatter records
- Archives directly to the cloud, compliant with "Cloud First" initiatives
- Provides unlimited storage
- Reduces datacenter costs in accordance with Federal Data Center Consolidation initiatives

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 21,500 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: http://go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com