A Survival Guide for Federal Records Management Compliance

Who should read this paper

This Solution Brief provides an overview for business decision makers in Federal Agencies that are charged with setting policy and supervising implementation for compliance with the Federal Capstone guidelines, and longer term mandates for all government records, as set forth by the National Archive Records Agency (NARA).
### A Survival Guide for Federal Records Management Compliance

#### Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>An Unfunded Mandate With a Ticking Clock</td>
<td>1</td>
</tr>
<tr>
<td>NARA's Capstone Automation Guidelines</td>
<td>1</td>
</tr>
<tr>
<td>Long Term Information Governance Responsibilities</td>
<td>2</td>
</tr>
<tr>
<td>What it Means to Agency IT Departments</td>
<td>2</td>
</tr>
<tr>
<td>Capstone and Beyond – How Should IT Organizations proceed?</td>
<td>3</td>
</tr>
<tr>
<td>Getting Started</td>
<td>3</td>
</tr>
<tr>
<td>More About Policy</td>
<td>3</td>
</tr>
<tr>
<td>Other Considerations</td>
<td>3</td>
</tr>
<tr>
<td>Symantec Technology Solutions Profile</td>
<td>4</td>
</tr>
<tr>
<td>Archiving</td>
<td>4</td>
</tr>
<tr>
<td>Data Classification and eDiscovery</td>
<td>4</td>
</tr>
<tr>
<td>Broad Support for Other Record Types</td>
<td>4</td>
</tr>
</tbody>
</table>
Executive Summary

President Barack Obama issued a directive in 2011 to reform federal records management. The directive put the responsibility for managing and defining implementation guidelines, under the Office of Management and Budget (OMB) and the National Archive Records Agency (NARA). The directive’s policies were published in a 2012 memo OMB-13-12 giving Federal Agencies a timeline to move from paper based records management to digitized formats – and even digitize existing paper records. [http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf]

This guide discusses a practical approach to achieving agency compliance using a modular set of solutions as recommended in NARA guidelines. The modular approach balances cost, compliance, and longevity, enabling agencies to meet short-term deadlines, while investing in systems that will deliver long term flexibility and value for all federal information governance objectives.

An Unfunded Mandate With a Ticking Clock

While the directive has laid out discrete timelines for compliance it does not come with any funding provisions. Nevertheless, in September, 2014 the OMB and NARA issued joint memorandum OBM-14–16 reminding the heads of federal agencies that the compliance deadline is December 31, 2016 for all federal agencies to manage both permanent and temporary email records in an electronically accessible format. [http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-16.pdf]. All records (not just email) are required to be kept in electronic formats by the end of 2019.

NARA's Capstone Automation Guidelines

Many agencies originally responded to the presidential directive with manual printing, scanning and filing processes and some continue the practice to this day. While compliant today, this approach is characterized by NARA as inefficient, inaccurate and a laborious diversion of resources from most agency main missions.

**Long Term Information Governance Responsibilities**

While focusing on short term Capstone deadlines, it’s important not to lose sight of the long-term directive goals for all government records (not just email), which NARA lists as:

- First, Federal agencies will require electronic recordkeeping to ensure transparency, efficiency, and accountability.
- Second, agencies are required to demonstrate compliance with Federal records management statutes and regulations, including those that require due diligence to secure personally identifiable information, and ensure citizen access to records, such as the Healthcare Information Portability and Accountability Act (HIPAA) or the Freedom of information Act.

Therefore, agencies need technology solutions which both ensure records are electronically retained, and in addition ensure records are properly protected and efficiently discovered, reviewed, retrieved and delivered when needed.

**What it Means to Agency IT Departments**

It will fall upon Information Technology departments to ultimately put automation systems in place to support the agency mission. While NARA is specifying the core requirements, they are not specifying exactly how Agency IT Departments should deploy solutions to meet those requirements.

A key recommendation of Capstone is to define rules for classifying potentially important email records of government employees to enable more purposeful identification of emails that should be kept versus unimportant “chatter” between workers. Using a role-based classification scheme will help establish consistent decision criteria for what to save and what to discard.

A Capstone target role may include any or all of the following:

- Officials at or near the top of an agency or an organization subcomponent. These are generally senior executives – but can be others.
- Key staff members that may be in positions that create or receive presumptively permanent email records
- Any individual, based on agency business processes, that create or receive permanently valuable email

The compliance responsibilities for the email of these individuals are summarized below:

- Ensure all email records are scheduled
- Prevent the unauthorized access, modification, or deletion of declared records
- Ensure all records in the repository are retrievable and usable
- Consider whether email records and attachments can or should be associated with related records
- Capture and maintain required metadata

Presumably, the approach you take will automate the capture of relevant email messages, and the migration of those messages into long-term record storage repositories. Capstone implementation guidelines do NOT require on a specific technology approach. If you already have

a technology solution in place you are free to continue using that solution. If you are not currently utilizing technology you are free to acquire something that works best for your agency.

**Capstone and Beyond – How Should IT Organizations proceed?**

**Getting Started**

To get started with Capstone you must determine the scope of your email that will be subject to record keeping regulations. Is managing at the account level suitable for your agency – or will you have to retain all employee email. Here are some of the questions you should ask yourself:

- Must my implementation manage email for the entire agency or only some groups?
- Should the email be managed for all offices and regions – or only certain ones?
- Will I need to apply the solution to legacy email or just to email moving forward?

The decisions you make with regard to these questions are the basis of your email management policies. Note that if you plan a new solution for data created this day forward you will need to have a separate plan for legacy as well. For example, you may have to scan existing printed records to meet the Capstone deadline, at the same time you deploy new technology to capture future email electronically as it’s created.

**More About Policy**

An official of the Federal Office General Council recently gave a presentation in which 3 key requirements were outlined for Capstone compliance and it’s critical that the technology you use can support these requirements:

1. Categorize and schedule email based on the position and/or work of the email account owner
2. Schedule all of the email belonging to selected officials as permanent
3. Schedule all other email accounts as temporary to be preserved for a set period of time based on agency needs

Capstone allows for culling (any activity, whether automated or manual, that removes non-record and/or transitory material from an email account). Culling is encouraged by NARA, especially when automated, to reduce capture of non-record and transitory material. Culling will enhance the accessibility and usefulness of the complete set of records.

Obviously, you’re not going to retain everything. Capstone recommends identifying ‘non-records’ even for individuals targeted for Capstone. Classification can be done automatically, or through manual identification by the user, but time has taught the industry that manual data classification systems typically fail. Such systems are too dependent on human behavior and can’t keep up with the data volume that email systems generate.

**Other Considerations**

One of the considerations that an email record retention policy must anticipate under Capstone is how the agency will be able to execute on a request for information under a regulation such as the Freedom of Information Act or a legal subpoena requiring a litigation hold. The solution you deploy must be capable of executing appropriate e-discovery and legal hold processes if a request is made of the agency. What will be the access request procedure and how will the discovery for that process be done? In the case of a legal hold, what group of records might the hold require to be preserved that would otherwise have been deleted? Make sure your plan takes these issues into account.
Symantec Technology Solutions Profile

There is no prescribed technology solution or platform that NARA mandates. But as has been discussed, there are policy and procedural requirements you have to meet. You should expect large volume of data to manage and over time the volume will probably accelerate if history is any indication. NARA acknowledges in their A31 report that a modular solutions approach, as opposed to a complex and cumbersome monolithic systems, will be the easiest to deploy, and adapt over a long-term governance lifecycle.

In a modular approach, one of the fundamental technology tools you should use, if you are not doing so already, is an automated email archiving solution. An electronic archiving system provides an automatic mechanism for moving email records requiring long term storage into the system you use for long term retention as the presidential directive mandates. The best archiving solutions will also have sophisticated classification and discovery suggested by NARA, as well as the ability to automate retention for files and other records, as required for full compliance by the 2019 deadline.

Archiving

Many government agencies already use Symantec’s Enterprise Vault or Enterprise Vault.cloud archiving solutions. Both solutions provide capabilities needed for Capstone compliance and can be set up to automatically capture email via journaling which will capture all messages for designated Capstone “record creators” in a manner which prohibits their modification. Capabilities such as Retention Folders will allow staff to manually make retention decisions when desired.

Data Classification and eDiscovery

Symantec Enterprise Vault also has classification capabilities that can tag email from non-designated accounts that must be retained for agency business purposes or a formal request for information. Several advanced automated eDiscovery options will enable agency employees to efficiently search records to find information for research, hold information for legal needs, and export discovered data to various formats for use outside the archive.

Broad Support for Other Record Types

Beyond Capstone, Enterprise Vault provides the capability to use metadata based rules to set retention categories on Microsoft SharePoint servers and File Servers, Instant Messaging, Web content and other forms of both structured and unstructured data to assist with other issues that are among the Presidential Records Management Directive requirements beyond the Capstone 2016 email milestones.

In short, Symantec has a history of technology and best practice experience with archiving and e-discovery solutions that are appropriate for agencies to deploy – or leverage if already deployed – in order to meet Capstone guidelines. For more information about on-premises Symantec archiving and e-discovery solutions visit the Symantec website at http://www.symantec.com/enterprise-vault or visit http://www.symantec.com/enterprise-vault-cloud for information on cloud based archiving solutions.
**About Symantec**

Symantec protects the world’s information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at [www.symantec.com](http://www.symantec.com) or by connecting with Symantec at [go.symantec.com/socialmedia](http://go.symantec.com/socialmedia).

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