Hello,

I wanted to communicate plans for our upcoming Email Gateway (Spam Filter) deployment to ensure you are aware of what is happening, and the timing of the transition.
If your agency currently utilizes this service, then there will be some changes that your users will need to be aware of.

What is happening?
ITS needs to replace/upgrade its aging email gateway platform.
ITS will transition the email filtering service from the current locally hosted product to a new cloud hosted service.
The new service is provided by Mimecast.

Why is this being done?
The existing email gateway runs on locally hosted hardware that needs to be upgraded/replaced.
The existing platform has limitations and constraints that will start to impact agency email delivery, for those agencies that use this service, so the new platform will overcome these limitations. In addition, the new service provides enhanced functionality that will improve the state's overall email security capability. Mimecast is FedRAMP compliant and on track for certification in September 2021.

When will it be done?
ITS will begin transitioning agencies over from the existing email gateway to the new email gateway starting from the beginning of March 2021.
A schedule for the transition will be published and reminders sent out prior to transitioning your agency to this service.

What changes should we expect to see?
When the transition is complete to the new system, there may be some email that was previously blocked as spam, that may come through until the new system filters are optimized and fine-tuned around our specific use.
The new system, Mimecast, has a very good reputation for filtering out "bad" email (Spam or other inappropriate types of email), however it uses different filtering technology that may take some time to "tune".
Also, when a user clicks a link in an email, they may initially be directed through the Mimecast service to verify the link prior to allowing the user to get to a given site. When this happens, the web link will have a Mimecast reference associated with it, and there will be a slight delay in getting to the site while the Mimecast verification happens.

Also, as many already know, a major source of Cybersecurity issues result from malware and other malicious content being delivered via email in the form of a file attachment or a link (URL). Many features are included in the Mimecast service to help circumvent this activity.

Some of these features include:

1. You will receive Anti-Spam Options for Quarantine Messages much like the Cisco Spam quarantine. However, the messages will look different. More information and examples will be provided to your agency before the transition.
2. All emails that contain attachments may be delivered with a "Safe file" first. The "safe file" is a .pdf version of the attachment that was sent to you. Once you determine it is safe and want the file in its original format, you can click the link within the email to download the original file.
3. Once you click a link in an email, or request the release of an original email attachment, you may be asked to enroll your device in the Mimecast Targeted Threat Protection service to continue. When prompted in the browser, enter your work email address, and hit "next". Mimecast will send you a one-time authentication code by email which you will enter into the browser dialog box where indicated. While this is typically performed once, it is possible you will have to re-register if something changes with your browser, or you change your computer to another computer or device. If asked to re-enroll frequently, please contact ITS to review what is happening.
4. You can find "How to Guides" and "Using Your Mailbox" at this link Mimecast for Outlook Guides

What if I have questions?
If you have any questions about this initiative, please provide details and your questions in an email to:
MimecastAdmin@its.idaho.gov