OFFICE OF INFORMATION TECHNOLOGY

One government, empowered by innovative technical collaboration

Multi-Factor Authentication FAQs

Update

V 05/20/22.1

***Note* These FAQs are not all inclusive. For a more comprehensive list of information, SOA employees may visit the** Azure MFA for end users - SOA 0365 Information Portal - SOA Wiki (state.ak.us) (State of Alaska Network only) **or** OIT Strategic Partner Services Delivery - MFA: Getting Started with Multi-Factor Authentication (servicenowservices.com).

1. What is Multi-Factor Authentication (MFA)?

   A = Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful impersonation attack.

2. Why is MFA important?

   A = The main benefit of MFA is it will enhance the state of Alaska's security by requiring our staff to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like an authenticator app or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

3. Are Alaska state employees subjected to seizure of their personal cell/mobile device if used for MFA?

   A =Using a personal device for MFA—whether by means of a text, call back, personal email, or mobile app—does not subject that device to a public records request because the device would at most contain (at the time of the request) an expired code that had been used for logging into a state system: i.e., a transitory record that is no longer persevered or appropriate to preserve for its informational value or as evidence of the agency's organization or operation.

   Also, using a personal device neither increases nor decreases the risk that the device would be subject to search or seizure in a criminal matter—unless an issue in the criminal matter was about access to a state system that was accessed using MFA. Per Alaska statue 12.35.020 and 12.35.025, warrants may be issued for search and/ or seizure of any property, personal or work, if used in conjunction with the commission (or the intent of commissioner) of a criminal act.

4. Will MFA on my personal cell phone disrupt configuration?

   A = If text-back or call-back MFA is used, no changes are made to your cell phone.

If the MFA application is installed on your device, then your mobile device will utilize the application. The application is the most secure and easiest MFA method to use, and it should not disrupt your mobile phone configuration.

5. How is MFA handled with a shared mailbox accessed by more than one person?

   A = When using a correctly configured shared mailbox, employees authenticate as themselves using MFA and then access the shared mailbox. This is the same security process as accessing a shared network folder.

   It is against good security practices and state policy (ISP-178) to share passwords. Shared mailboxes that provide access to multiple employees using their own credentials are available to any group who needs them.

6. Which MFA option is the lowest impact to my personal cell/mobile device?

   A = Text-back and call-back do not require any changes to your device.

7. Well, I'm not sure what to do. My cell phone is ancient, and I have constant space issues so I'm not sure I will be able to download an app.

   A = Use the text-back or call-back which does not require you to install an app.

8. Does MFA only apply if the Office 365 user is using a VPN?

   A = No it does not. MFA applies to all O365 applications such as email/outlook, Teams, Word, Excel, PowerPoint, etc. regardless if logged in to VPN or not.

9. Does a user need to setup MFA if they only access their state O365 applications from a State laptop/desktop?

   A = O365 MFA is required regardless of device used for work.

10. Are there plans to implement O365 MFA to log into laptops?

   A = OIT is exploring the use of O365 MFA to login to laptops.

11. How is the requirement for MFA impacted by the availability of SOA-provided or subsidized smart phones?

   A = A state provided/subsidized device is not required.

12. I have no work cell phone, no work desk phone, or I use a shared work phone in the office… how do I access work email?

   A = If you are uncomfortable with the option of using a personal cell phone with call-back or text-back, MFA please consult your administration team for a solution.

13. Can a report be provided to agencies for users who have not gone through the steps to activate MFA?

   A = Yes, management can receive reports for who has and has not enabled O365 MFA.