**BO23. CYBERSECURITY - THE CHALLENGES FACING FAAS (Q&A)  
  
Question:**Can we have the Partner Connect links for the slide. The ones listed have IFAP.

**Response:**SME - Lossing - Presentation slides are available on the FSAConferences.ed.gov website. The sessions will immediately go on-demand after airing until March 2, 2022. After that, they will be posted on the FSAConferences.ed.gov website.  
  
**Question:**  
Has there been any research into moving to biometric access for FSA systems? I could imagine facial recognition or other biometric access systems eventually since they are harder to spoof.

**Response:**SME – Maxwell – FSA does not currently have any plans to move to biometric access to our systems.  
  
**Question:**  
Is this why the latest update to EdConnect will not allow files to be downloaded to a shared server?  
**Response:**SME - Lossing - Can you clarify the question. I'm not sure I understand your issue with downloading files.  
**Question:**  
When we downloaded the last update to EdConnect, it will not under any circumstance allow us to have a directory for downloading files that is on a shared server. It forced us to use our C: drive to download files. Is that part of this effort to prevent issues? I reached out for assistance and tried everything to no avail.  
**Response:**SME - Lossing - EdConnect may have some policies or controls that limit how files are downloaded. I don't have any insight as to why this is an issue. I'd recommend reaching out to the help desk for additional assistance.  
SME – Maxwell – Here is a link to the Electronic Announcement on Partner Connect as well as contact information.   
<https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2021-09-10/mandatory-saig-software-upgrade-upgrade-edconnect-85-and-updated-tdclient-software-oct-23-2021-ea-id-general-21-56>  
If you have questions about the EDconnect or TDClient software, please contact CPS/SAIG Technical Support at 1-800-330-5947 or by email at [CPSSAIG@ed.gov](mailto:CPSSAIG@ed.gov)  
  
**Question:**  
Are password managers potentially okay (obviously there are some that are more secure than others)?  
**Response:**SME-Lossing- FSA does not have a policy or current guidance on password managers. Consult your IT or security dept. for approved, secured password managers.  
  
**Question:**  
SAIG and G5 are already multifactor. Which other systems will be changed over?

**Response:**SME-Lossing- FSA foresees that all Federal systems will need to use multifactor in the future.

**Question:**Are there any other school use FSA systems besides those two?  
**Response:**SME-Lossing- There are a variety of other systems that a school may use when interacting with FSA.  
**Question:**  
Can you give examples? I want to know which staff this might impact.  
**Response:**  
SME - Lossing - We can take this question back within FSA and try to find a list of systems that a school may use. Please email us at FSASchoolCyberSafety@ed.gov and we will get back to you. SME - Lossing - We can take this question back within FSA and try to find a list of systems that a school may use. Please email us at [FSASchoolCyberSafety@ed.gov](mailto:FSASchoolCyberSafety@ed.gov) and we will get back to you.  
  
**Question:**If a school uses outlook, can they send PII to other members unencrypted, if IT can confirm the data sharing is secured or does anything sent via email not considered secured regardless of any security measures?  
**Response:**  
SME – Maxwell – FSA advises that PII should not be sent unencrypted. FSA recommends sending PII using secure methods such as WinZip encrypt and password protected. When sending PII external to your organization over public internet, encryption is a must.  
SME-Lossing- Any emails with PII sent external from the institution must be encrypted.