Notes from the 9/20/2022 Exit/Offboarding meeting

Comments below in **red** are from Jack Tonkay prior to the meeting. Notes for the meeting are below Jack's comments and his links for CD Employees.

USDA Computer Network

- Access to historical CD documents for new employees
  - Where to store the CD information
    - (Authorized & approved storage locations for official USDA files/data
      - Computer (Documents – backed up to OneDrive)
      - OneDrive
      - Teams
      - SharePoint
      - Share Drives
      - External Media (Flash drives/External Hard Drives)
  - (myFPAC Recommended Virtual Collaboration Tools)

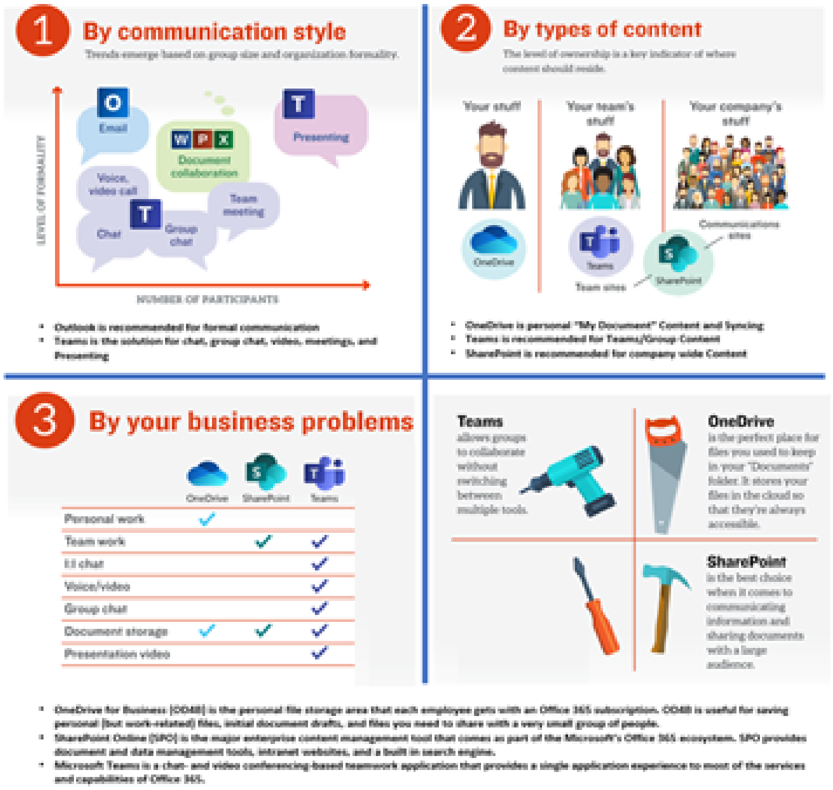
    Recommended Virtual Collaboration Tools (usda.gov)
  - (Collaboration Tools Overview)
    - (SharePoint allows you to share and manage content, knowledge, and application to empower teamwork, quickly find information and seamlessly collaborate across the organization
    - OneDrive lets you store your files in one place, share them with others, and get to them from any device connected to the internet
    - Microsoft Teams is a customizable chat-based team workspace for groups, meetings, calls and collaboration activities in Office 365

Integrations

Microsoft Office (Word, Excel, PowerPoint, and OneNote) is built into SharePoint Online through Office online. FPAC employees can create new Office documents directly in a library or create new files in the desktop app and save or upload them to OneDrive, Microsoft Teams, or SharePoint.

Usage Guidelines

USDA Office 365 offers a variety of communication and collaboration tools to simplify the way we work today. Below are four infographics that provide guidance on how to choose the right tool for your use based upon communication style, type of content, and business problem.



1 By communication style

Trends emerge based on group size and organization formality.

- Outlook is recommended for formal communication
- Teams is the solution for chat, group chat, video, meetings, and Presenting

2 By types of content

The level of ownership is a key indicator of where content should reside.

- OneDrive is personal "My Document" Content and Syncing
- Teams is recommended for Teams/Group Content
- SharePoint is recommended for company wide Content

3 By your business problems

	OneDrive	SharePoint	Teams
Personal work	✓		
Team work		✓	✓
1:1 chat			✓
Voice/video			✓
Group chat			✓
Document storage	✓	✓	✓
Presentation video			✓

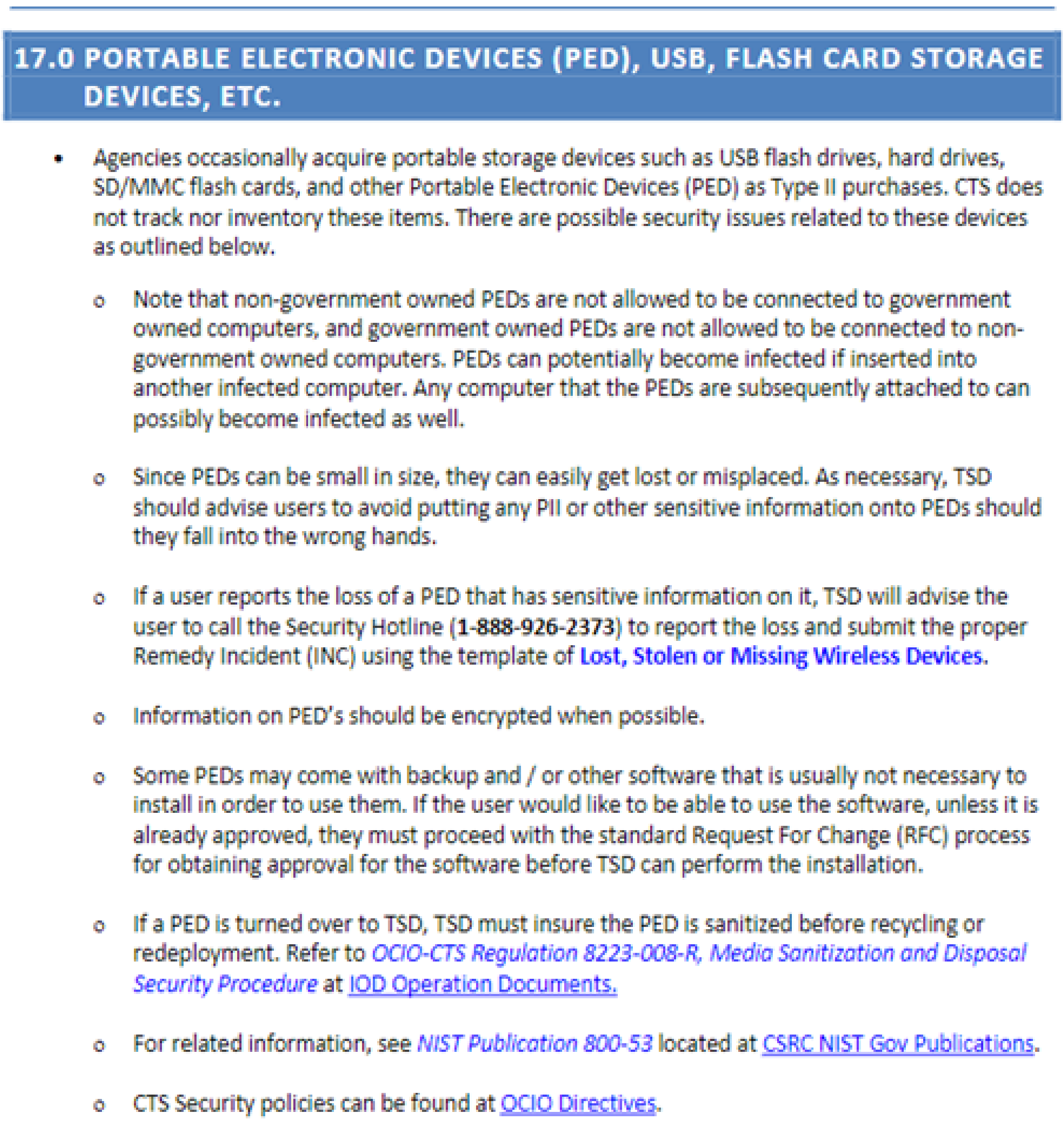
Teams allows groups to collaborate without switching between multiple tools.

OneDrive is the perfect place for files you used to keep in your "Documents" folder. It stores your files in the cloud so that they're always accessible.

SharePoint is the best choice when it comes to communicating information and sharing documents with a large audience.

- OneDrive for Business (OD4B) is the personal file storage area that each employee gets with an Office 365 subscription. OD4B is useful for saving personal (but work-related) files, initial document drafts, and files you need to share with a very small group of people.
- SharePoint Online (SPO) is the major enterprise content management tool that comes as part of the Microsoft's Office 365 ecosystem. SPO provides document and data management tools, intranet websites, and a built in search engine.
- Microsoft Teams is a chat- and video conferencing-based teamwork application that provides a single application experience to most of the services and capabilities of Office 365.

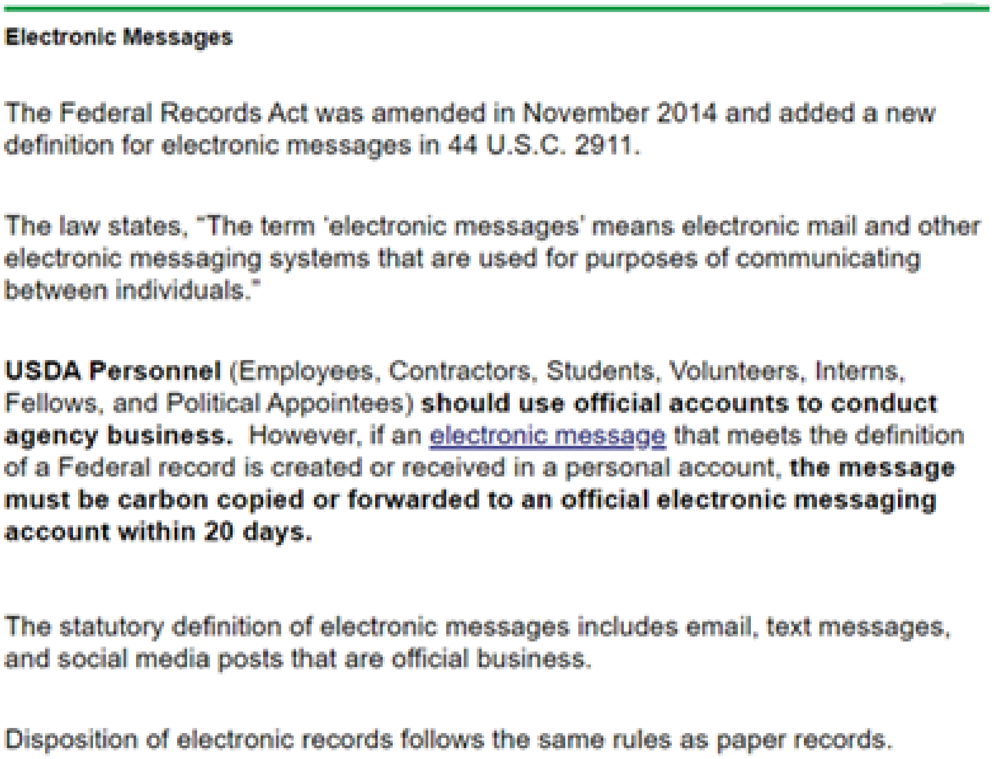
- External hard drives/USB flash drives-need to be approved by IT
    - (NRCS receives IT "Technical Approval" (AD-700) prior to purchase. The "use" of external **government owned** H/D's and USB Flash drives" do not require TSD approval.



17.0 PORTABLE ELECTRONIC DEVICES (PED), USB, FLASH CARD STORAGE DEVICES, ETC.

- Agencies occasionally acquire portable storage devices such as USB flash drives, hard drives, SD/MMC flash cards, and other Portable Electronic Devices (PED) as Type II purchases. CTS does not track nor inventory these items. There are possible security issues related to these devices as outlined below.
  - Note that non-government owned PEDs are not allowed to be connected to government owned computers, and government owned PEDs are not allowed to be connected to non-government owned computers. PEDs can potentially become infected if inserted into another infected computer. Any computer that the PEDs are subsequently attached to can possibly become infected as well.
  - Since PEDs can be small in size, they can easily get lost or misplaced. As necessary, TSD should advise users to avoid putting any PII or other sensitive information onto PEDs should they fall into the wrong hands.
  - If a user reports the loss of a PED that has sensitive information on it, TSD will advise the user to call the Security Hotline (**1-888-926-2373**) to report the loss and submit the proper Remedy Incident (INC) using the template of **Lost, Stolen or Missing Wireless Devices.**
  - Information on PED's should be encrypted when possible.
  - Some PEDs may come with backup and / or other software that is usually not necessary to install in order to use them. If the user would like to be able to use the software, unless it is already approved, they must proceed with the standard Request For Change (RFC) process for obtaining approval for the software before TSD can perform the installation.
  - If a PED is turned over to TSD, TSD must insure the PED is sanitized before recycling or redeployment. Refer to *OCIO-CTS Regulation 8223-008-R, Media Sanitization and Disposal Security Procedure* at IOD Operation Documents.
  - For related information, see *NIST Publication 800-53* located at CSRC NIST Gov Publications.
  - CTS Security policies can be found at OCIO Directives.

- Email access in case of shutdown
  - Gmail vs. MACD email address as backup?
    - (Gmail is outside of the USDA domain and not an authorized means of transmitting and storing official government data/information)



Electronic Messages

The Federal Records Act was amended in November 2014 and added a new definition for electronic messages in 44 U.S.C. 2911.

The law states, "The term 'electronic messages' means electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals."

USDA Personnel (Employees, Contractors, Students, Volunteers, Interns, Fellows, and Political Appointees) **should use official accounts to conduct agency business.** However, if an electronic message that meets the definition of a Federal record is created or received in a personal account, **the message must be carbon copied or forwarded to an official electronic messaging account within 20 days.**

The statutory definition of electronic messages includes email, text messages, and social media posts that are official business.

Disposition of electronic records follows the same rules as paper records.

- LincPass– (Specific LincPass issues are outside the scope of responsibility for TSD - Contact agency POC or visit HSPD-12 website for further information USDA HSPD-12 Information
  - Why does it take so long for some to get a LincPass and some have it so much faster, and what can people dS to speed the process up?
  - How do a person get a LincPass?
  - What options when selecting your agency, CDs aren't listed, and we don't work for USDA
  - What Training do you have to complete every year to avoid losing the LincPass?

- DNRC has a contract with MACD on tech stuff–could be a source for purchasing external drives (More information soon on this topic)
- Wendy Jones said that when she started, contacts list for the CD was retrievable, but any emails specific to the previous employee were gone. Get an external hard drive, save files to that. Use alternative email address that any new admin can access, for all of the day-to-day CD official business. Can be forwarded to the USDA email address.
  - (Agency/customer decision on authorized storage/backup)
- Julie Goss-Why, if the CD owns the computer, is the system wiped to send on to the next person? Wendy said that from the IT perspective, once the user is gone, the data is gone. This breaks all kinds of records retention rules.
  - (per TSD SOP/directives IT performs a full "re-imagine" of all computers prior to redeployment to another individual (Information Security, Computer Security & Network Security parameters). Only information stored on the computer physical

hard drive is lost. All information backed up on OneDrive, SharePoint, Teams, and network servers is preserved.

Data storage on USDA Computers

- Get an external hard drive approved by IT by going through your DC, or use cloud storage
    - (The use of a government sources/owned external H/D does not require IT approval. Encryption of external devices is a limiting factor for shared use.)
- DON'T store CD files only on the USDA computer's hard drive-store it on the shared drive. The hard drive is completely wiped (email and all) between CD Employees. (although, I've received mixed information on this. One IT person said that anything on the "personal user drive"--what used to be the H drive and is now OneDrive–is deleted between employees.
    - (Files & folders backed up to OneDrive are not lost when an employee departs).
- Because there's some time before a new employee can access files on the shared drive, back all of them, as well as the CD Calendar, email history, internet bookmarks that are work related, and contacts list up to the external hard drive, and/or an alternate computer (QuickBooks computer?). Consider using a secondary computer for the bulk of the Conservation District work.
    - (File retention and sharing is an agency/customer decision. Outlook calendars & email are not saved to individual computers (by default), they're located on the USDA Exchange Server under the users O365 profile. Internet bookmarks are saved to the users personal setting for the respective internet browser e.g. Microsoft Edge, Google Chrome, Firefox and should be shared as needed by the agency. QuickBooks is a Commercial Off the Shelf (COTS) application (outside the scope of TSD guidance). A "secondary computer" is available in the form of a network servers. Customers can request permissions to their respective server(s) by submitting a System Authorization Access Request (SAAR) through their agency POC.
- USDA Phone Systems–whole different problem

    Submit a ticket through the District Conservationist

    If you are on the USDA Network, your phone will run through the computer, if you aren't, it will be plugged into the wall.
- The two models of Cisco Voice over Internet Protocol (VoIP) phones, (7945 & 8841) are connected to the USDA network through an ethernet cable, generally plugged directly into a network outlet in the wall. Network connections to USDA computers can then be plugged directly into the VOIP phones. This is the standard configuration for VOIP phones and network computers. If commercial "dial up" phones are being used, they connect through the service carrier Plain Old Telephone (POTS) lines and have no capability for programing or configuring by TSD.

HELPFUL LINKS:

CEC Customer SharePoint Site:
Client Experience Center - Customer Site - Home (sharepoint.com)

How to Request CEC Help:
How to Request Help (sharepoint.com)

Customer Service Notifications:
Customer Service Notifications and IT Newsletters (sharepoint.com)

Agency SharePoint Administrators:
Agency SharePoint Points of Contact

CEC Customer Site – Security:
Security (sharepoint.com)

CEC Customer Site – Security Policies:
Security (sharepoint.com)

Notes from today's meeting:

The meeting opened with Jack introducing himself. His group supports all federal agencies in the Montana Wyoming group (12 IT specialists) and 1600 customers. Tier 1 Help Desk directs most of their work.
Service level agreements dictate timeliness of support. CEC technical support staff has responsibilities that they have to initiate like specialized software, technical vulnerabilities, etc.

Chris Evans asked about the timeliness of new CD employees getting access to CD information.
Jack referred to the above 6 authorized and approved storage locations. Unless the employee is creating different folders, all of the CD information should be in those locations. All of the CDs that were spot checked had been migrated to one drive. Teams and Sharepoint are the 2 collaboration tools that are available as best tools that should have the data that you want, when you want it. This takes front end work by current CD staff to determine storage locations and formats. Jack mostly recommends Teams, sharepoint requires some coordination. External media are available to CDs, but the CEC doesn't really approve their use. **When you plug in one of these, they should require data encryption (bit locker). Any USB device <u>will automatically be encrypted</u> for using LincPass or PIN. CAUTION: If the CD staff use one of these, and plug them into the network, they will automatically be encrypted. (This makes me think that if you as a CD staffer uses one, make sure that the information is transferred to a non USDA computer WHILE YOU ARE AT THE CD).**

USDA agency personnel-from the time an employee starts there are tools that can be used to get access to files within a few days for up to 30 days (to get lincpass). Route the request for a 30 LincPass exemption through the NRCS District Conservationist who will then contact the Management Strategy Office. Kyle Tackett says that if your NRCS staff doesn't know what this is, or that it's a real thing, to either contact him, or have the NRCS people contact him.

Kay Webb asked about a locked flash drive from when she started–Jack said that there is no way to retrieve that information.

Radley-How does a CD Employee get onboarded to the USDA Computer network? Official training available to access the tools on the network?-Jack said that's not really a CEC issue, everything they do is directed by the supporting agency (NRCS). Kyle made a note of Radley's comment with the idea that something should likely be done to consistently onboard new CD employees to the USDA network. Jack said that he can offer that USDA provides a tool called **software center**. Anyone authorized on the network has access to that software center. Users can go out and search that to find approved software that they can then install themselves. Soil Scientists have specific software that they have to use, so it's available to them, but not to others. Just type in software center in the windows search tool on their network computer .

Kay Webb-lincpass exemption-does it give access to everything? No, the exemption gets them into the computer. For access to shared drives etc, there has to be a separate request made. It's called a **SAAR**– System authorization access request. Once an employee gets in, they have access to those drives etc. Only the LincPass 30 day exemption has an expiration and multiple 30 day exemptions may be requested.
2nd question-jumping ahead-teams account-she doesn't use the government authorized email for her Teams she uses the alternate CD email. Can she have a SAAR to request a bypass? Jack said no, but that there's a dial in number with a pin that can be used instead of an email.

Bryan Vogt-one of the things he's had an issue with is that they have 2 computers that are linked up, CD owned, but on the USDA network that require a LincPass. When an employee leaves, is any data stored on the individual laptop accessible?
Answer-maybe, but probably not. It is the supporting agency's (NRCS) responsibility to work with employees on where they should store information. Agency needs to ensure that there are best practices on records management.

Computer/OneDrive-Agency must request that the data be retrieved
Combined solution-primary means of sharing data should be Teams, sharepoint and shared drives. CD Employee needs to ensure that the CD data is backed up to one of the those 3 locations (maybe all?). **New employee would have access to any of those locations with a SAAR and the 30 day Lincpass exemption.**

EMail-There is no way to import gmail or an email supported by MACD to Outlook on USDA network but the Government email could be forwarded to outside source probably. Jack said he'd look into that.

In the event of a government shutdown-take the laptop with you, using home network if approved by policy. Access to your computer in the event of a shutdown (if a desktop system) could be through remote means, but that would need to be set up ahead of time.

Rad commented that backing up documents in the government's system is primarily for the CD/USDA collaborative documents, but that CD records can be hosted on the cloud at the CD's expense or in another storage system.

Reimaging computers-agency staff who leave, their computers go to a central depot for "sanitizing" and to be used anywhere in the agency. **For CDs, because we buy our own equipment, make sure when someone leaves the office, contact IT and send computers to bozeman so it doesn't get comingled with NRCS equipment.**

Julie Goss asked about turnaround for getting the CD computer back once a new employee is hired. Jack said that there is no set timeline-as CD employees we would fall under the NRCS agreement, probably around 2 weeks.
If a CD employee's supervisor knows that an employee is leaving at the end of the month, relevant information should be backed up a week or so in advance. Then the question is when to send the computer to Bozeman. There is potential for loaners in the interim while waiting on return of the sanitized computer.

When an employee is working on a computer that's not on the usda network, accessing the CD information is going to be a problem. There is no way to just "call in" to the USDA network from an outside computer to access those records.

Also, if the CD gets a new computer, what do they do with the old one that's sanitized? (this question never was asked, I'm sorry. I will follow up with Kyle and Jack and ask.)

Can we speed up LincPass-Kyle says they're a pain for NRCS too, that they just take a while. He recommended that CDs rely on that 30 day exemption. NRCS pays for the computer seats and what comes with that is a LincPass. CDs need to be cautious on setting expectations for incoming CD employee. Evans noted that using Google drive for daily CD records could be a solution as gap filler. Bit locker pin is critical for new employee to use the USDA computer. Then lincpass pin. Radley asked if he can use his LincPass pin to log into their old admin computer. How do they know the bit locker? The old person can pass that along. If that doesn't happen, put in a ticket with Tier One help desk to reset the pin.

There will be a followup meeting after the 1st of the NRCS Fiscal Year to address more issues that aren't in Jack Tonkay's specialization. Kyle Tackett will work with Chris Evans on that.

Send CD computers to Bozeman prior to new employee use–clearly ID that as a CD employee computer so it doesn't go off to the centralized depot, which would cause it to be lumped in with all of the federal computers.. Brad Perry's contact information is:
Brad Perry
IT Specialist
OCIO/CEC/TSD
United States Department of Agriculture
Montana/Wyoming Group
10 East Babcock
Bozeman MT 59715

Office phone: (406) 587-6860
Mobile Phone: (406) 451-5137

Jack ITT commented-supervisors put a stack of paper in front of new employees for onboarding, it's really important to not overlook some of the required forms (security agreements etc.) and pay attention to the usda security awareness training. Acceptable use policies etc. Good information that everyone should be aware of. Don't make light of it.