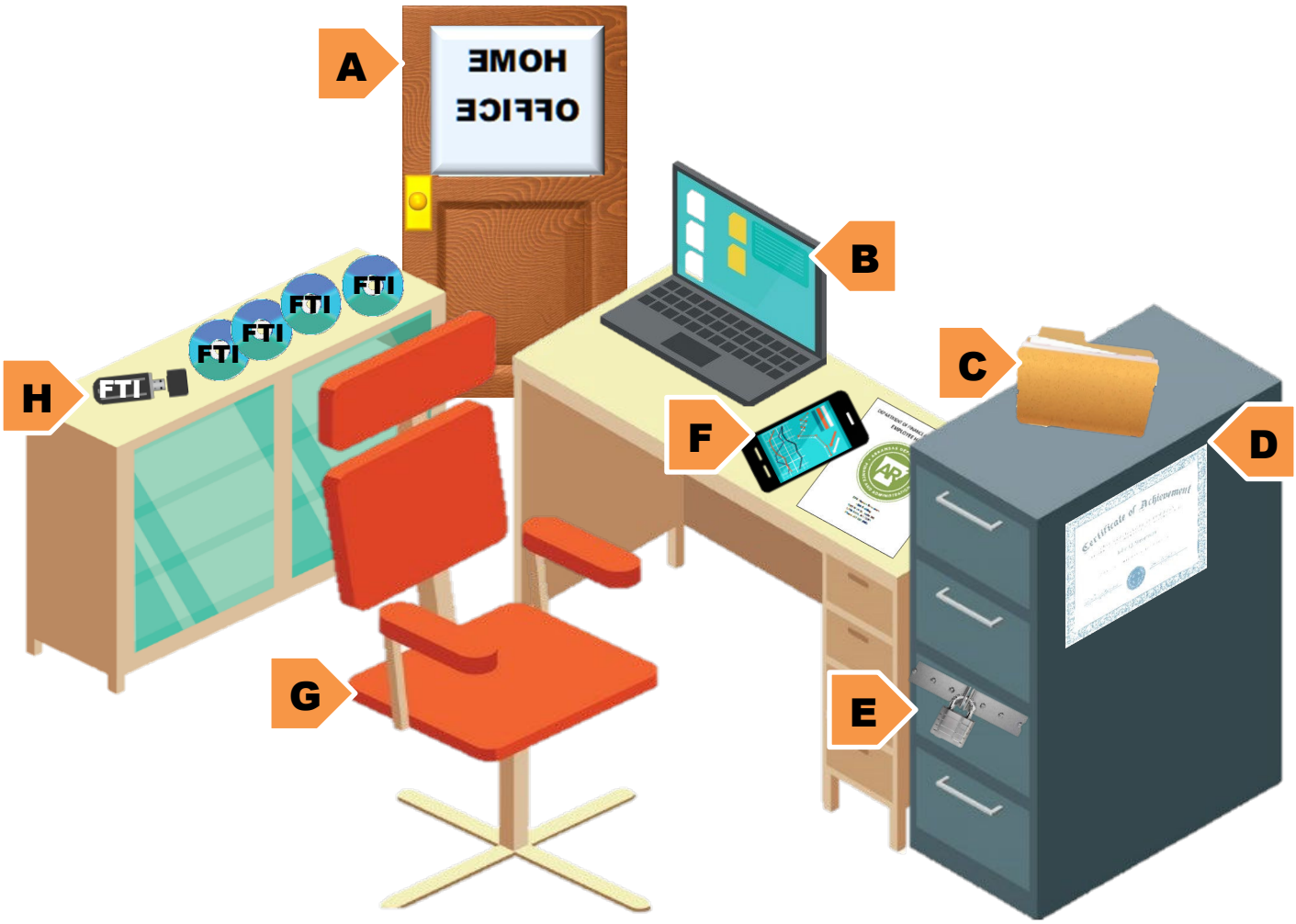
ALTERNATIVE WORK SITE
Remote Work

Purpose: Use this job aid to ensure that DFA employees who have access to Federal Tax Information (FTI) and are approved for a DFA Remote Work Agreement are compliant with the alternative work site requirements of the Internal Revenue Service Publication 1075 (IRS Pub. 1075), Tax Information Security Guidelines.



A. Dedicated room
B. DFA equipment
C. Records retention
D. Annual training
E. Locked storage
F. Security risks/breach
G. Confidential information
H. FTI labels

ALTERNATIVE WORK SITE
Remote Work

A. **Dedicate a specific alternative work site room, or area in a room, with appropriate space and facilities to perform your job functions when working remotely.** The area must be a location where you can ensure all devices, materials, and business conversations are confidential and stored properly both when and when not in use. You should consider the following when determining if the site is acceptable: electrical outlets, phone/cable receptacles, internet signal strength, noise, lights, door/cabinet locks, etc.

B. **Only use DFA approved security access control devices and DFA approved software to perform your job duties.** A DFA-authorized virtual desktop is permissible. *Control devices* include computers, laptops, cell phones, USB drives, CDs, or any other hardware or peripherals used to perform your job duties. You are responsible for regularly logging into the DFA network for OIS maintenance and alerts. You must complete yearly cyber security training.

C. **Comply with the DFA records retention schedule.** You must make DFA equipment that is located at the remote site available for inventory inspection or self-report as requested. You must create and maintain any FTI logs and usage reports as applicable to your access to FTI.

D. **Complete *DFA Disclosure Awareness* training.** You must complete the online training course before initially accessing FTI and annually thereafter if you have access to FTI. You are required to comply with the laws and guidelines explained and referenced in the course. S*ee the IRS Publication 1075.*

E. **Store FTI and confidential information to prevent a breach or unauthorized access.** When working remotely you must lock computers, tax documents, removable media, and smaller agency-owned equipment containing FTI or DFA confidential information in a file cabinet or desk drawers when not in use. When in use, the items must always be under your immediate protection. Non-DFA personnel should never have access to view, copy or remove FTI or DFA confidential information from the remote site.

F. **Report security issues immediately.** Call your DFA Manager or the DFA Office of Information Services (OIS) Help Desk at 501-683-2183 if security problems arise. Data security risks include a data breach, unauthorized access, tampering, etc. Technical security issues include compromised username/password credentials, faulty Windows idle log-off feature, phishing emails, etc.

G. **Safeguard and ensure the confidentially of all DFA information.** Always properly lock your computer and store DFA sensitive information and FTI when you are away from the computer and/or workstation, including brief absences.

H. **Label removable FTI media.** Label all removable devices containing FTI, such as USBs or CDs, as “FTI”. Keep FTI locked in a desk drawer or filing cabinet when not in use.