

In light of recent communications regarding authentication of patron identification on library computers, the U.S. Government Printing Office (GPO) would like to take this opportunity to address some of the common security issues we are seeing more frequently in depository libraries.

The overall goal of the depository program is to provide the public no-fee access to U.S. Government information regardless of format. That said, GPO recognizes the necessity of securing computer networks. Balancing the need for network security and no-fee access to depository electronic information can be accomplished.

For libraries that utilize log-ins or authentication, the [Federal Depository Library Handbook](#) states,

*“Libraries may provide guests the ability to log-in at a workstation or staff may log them in at authenticated stations. At a minimum, if all workstations providing Internet access require authentication, users should be directed to public service desks for assistance through mediated searching.”*

On a similar thread, libraries that employ filters, *“must allow users the option to use workstations without filtering software or provide the capability of turning off the filter while users are searching FDLP information resources... At a minimum, if your library is unable to deactivate filtering in a rapid manner, you must provide mediated searching for depository users.”*

Keep in mind that language on public workstations, Web pages, and signage should promote access to government information rather than dissuading or limiting access.

As technologies evolve, the depository community and GPO will continue to work together to find that balance point between library user needs and network security requirements.

For additional information, please see:

- [Federal Depository Library Handbook, Chapter 4. Public Services](#)
- [FDLP Internet Use Policy](#)
- [Depository Library Public Service Guidelines for Government Information in Electronic Formats](#)

If you would like to discuss your library's situation with GPO, please feel free to contact us at (202) 512-1119.