DOL Cybersecurity Tips

The Department of Labor (DOL) has published Cybersecurity tips to use when hiring service providers as well as tips for plan sponsors and participants. These are tips serve as a recommended course of action and not requirements. However, under the prudent man standard of care all tips from the DOL should be reviewed and carefully considered by plan sponsors.

Call to Action

Per the DOL, plan sponsors should ask the service provider about the following:

- Security Standards
- Security Practices
- Security Policies
- Audit Results
- Security Validation Process
- Security Levels Implemented
- Past Security Breaches
- Cybersecurity Insurance
- Cybersecurity Guarantee

Per the DOL, plan sponsors should consider the following actions:

- Establish a formal Cyber Security Program
- Conduct annual risk assessments
- Hire third party to audit security controls
- Define and assign information security roles and responsibilities
- Establish strong access control procedures
- If data stored in cloud or with third party conduct security reviews
- Conduct cyber security awareness training
- Implement secure system development life cycle
- Create effective business resiliency program
- Encrypt sensitive data
- Respond to cyber security events

Per the DOL, plan participants should consider the following actions:

- Register your account
- Regularly monitor your account
- Use strong and unique passwords
- Use multi-factor authentication
- Keep personal contact information current
- Close or delete unused accounts
- Do not use free Wi-Fi
- Beware of Phishing attacks
- Do not store login information in your email account
- Use up to date anti-virus software
- Report identify theft to your employer and the record-keeper

A Proud Member of
RPAG