DOL Cybersecurity Guidance Questionnaire

In April 2021, the U.S. Department of Labor (DOL) issued guidance on best practices for maintaining cybersecurity, including tips on how to protect the retirement benefits of America's workers.

As a result of this guidance, I am kindly requesting for your response on each of the following tips and best practices as a service provider to our retirement plan(s).

Tips for hiring a service provider

1. **DOL tip:** Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.

   Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. You can have much more confidence in the service provider if the security of its systems and practices are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.

   Service provider response:

2. **DOL tip:** Ask the service provider how it validates its practices, and what levels of security standards has it met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.

   Service provider response:

3. **DOL tip:** Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendors' services.

   Service provider response:

4. **DOL tip:** Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

   Service provider response:

5. **DOL tip:** Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participant's account).

   Service provider response:

6. **DOL tip:** When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards—and beware of contract provisions that limit the service provider's responsibility for IT security breaches. Also, try to include terms in the contract that would enhance cybersecurity protection for the plan and its participants, such as:

   Information Security Reporting – The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.

   Service provider response:

   DOL tip: Clear Provisions on the Use and Sharing of Information and Confidentiality – The contract should spell out the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse.

   Service provider response:

   DOL tip: Notification of Cybersecurity Breaches – The contract should identify how quickly you would be notified of any cyber incident or data breach. In addition, the contract should ensure the service provider's cooperation to investigate and reasonably address the cause of the breach.

   Service provider response:

   DOL tip: Compliance with Records Retention and Destruction, Privacy and Information Security Laws – The contract should specify the service provider's obligations to meet all applicable federal, state, and local laws, rules, regulations, directives, and other pertaining governmental requirements.

   Service provider response:

   DOL tip: Insurance – You may want to require insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability, and privacy breach insurance, and/or fidelity bond/blanket crime coverage. Be sure to understand the terms and limits of any coverage before relying upon it as a protection from loss.

   Service provider response:

Cybersecurity program best practices

1. **DOL tip:** Have a formal, well-documented cybersecurity program.
   Service provider response:

2. **DOL tip:** Conduct prudent annual risk assessments.
   Service provider response:

3. **DOL tip:** Have a reliable annual third-party audit of security controls.
   Service provider response:

4. **DOL tip:** Clearly define and assign information security roles and responsibilities.
   Service provider response:

5. **DOL tip:** Have strong access control procedures.
   Service provider response:

6. **DOL tip:** Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
   Service provider response:

7. **DOL tip:** Conduct periodic cybersecurity awareness training.
   Service provider response:

8. **DOL tip:** Implement and manage a secure system development life cycle (SDLC) program.
   Service provider response:

9. **DOL tip:** Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
   Service provider response:

10. **DOL tip:** Encrypt sensitive data, both stored and in transit.
    Service provider response:

11. **DOL tip:** Implement strong technical controls in accordance with best security practices.
    Service provider response:

12. **DOL tip:** Appropriately respond to any past cybersecurity incidents
    Service provider response:

Service provider name:

Date of completion:

Contact name:

PQ13022B-01 | © 2023 Principal Financial Services, Inc. | 2831431-042023 | 04/2023