BEST PRACTICE IN ACTION:
Department of Labor Cybersecurity Guidance

In April of 2021, the Department of Labor (DOL) announced new guidance relating to cybersecurity best practices for plan sponsors, plan fiduciaries, plan service providers, and plan participants. The guidance came in three forms: (1) a tip sheet for plan sponsors and plan fiduciaries hiring plan service providers, (2) a tip sheet for plan participants and beneficiaries accessing online accounts, and (3) a summary of twelve best practices for plan fiduciaries and plan service providers safeguarding nonpublic plan data.

Always your partner in compliance, ERP has taken swift action to align its own cybersecurity processes with DOL best practices. ERP recognizes the importance of protecting data stored and accessed on its system—particularly nonpublic, sensitive data relating to ERISA-covered benefit plans. ERP will work to *identify* internal and external cybersecurity threats, *protect* the data stored and accessed on its systems, and *address* the many facets of cybersecurity risk mitigation.

ERP has implemented and continually monitors a comprehensive cybersecurity program that is tailored to the DOL's twelve best practice prongs, as summarized below.

1. A Formal, Well Documented Cybersecurity Program.
ERP's cybersecurity program evidences well-documented information security policies, procedures, guidelines, and standards to protect the security of its IT infrastructure and the data stored on its system. Under the leadership of its Chief Information Security Officer (CISO), the procedures detailed in the program enable ERP to identify risks to its assets, information, and systems; protect its assets, data, and systems; detect and respond to cybersecurity events; recover from any cybersecurity events; disclose the event as appropriate; and restore normal operations and services. ERP intends that the program be approved by ERP senior leadership, reviewed internally at least annually, and reviewed regularly by an independent third party to confirm compliance.

2. Prudent Annual Risk Assessments.
ERP recognizes that routine risk assessments are a foundational element of any shrewd cybersecurity program. ERP intends to implement reasonable processes to (1) identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized; (2) establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks; (3) describe how its program will mitigate or accept the risks identified; and (4) facilitate the revision of controls resulting from changes in technology and emerging threats.

3. Reliable Annual Third Party Review of Security Controls.
ERP intends to have an independent third party regularly assess ERP's internal security controls—particularly those related to benefit plan data. Following such review, ERP intends to implement reasonable processes to address any weaknesses and to retain documentation related to both the identified risk and its associated correction.

4. Cleary Defined and Assigned Information Security Roles and Responsibilities.
ERP's cybersecurity program will be managed at the senior executive level by its CISO and implemented by qualified personnel.

5. Strong Access Control Procedures.
ERP allows only authorized personnel and devices to access its nonpublic data, including nonpublic benefit plan data. ERP maintains reasonable procedures to ensure robust access control, focusing primarily on authentication and authorization. These procedures may include limiting access to systems, limiting access privileges, reviewing access privileges regularly, requiring complex

passwords, using multi-factor authentication wherever possible, and reviewing stored benefit plan data for accuracy.

6. Service Provider Oversight.
ERP intends that all assets or data stored in a cloud or managed by a third party service provider be subject to appropriate security reviews and independent assessments. ERP aims for reasonable oversight processes, which may include requiring a risk assessment of third party service providers, defining minimum cybersecurity practices for third party service providers, periodically assessing third party service providers, and ensuring that guidelines and contractual protections address certain minimum security standards.

7. Personnel Training.
ERP recognizes the importance of verifying that its personnel are aware of—and implement—cybersecurity best practices. To this end, ERP intends to provide regular cybersecurity awareness training to all personnel to set clear cybersecurity expectations, educate its personnel about cybersecurity principles, highlight the importance of fighting identity theft, and emphasize current trends in cybersecurity best practices.

8. Secure System Development Life Cycle (SDLC) Program.
ERP does not currently develop systems, software, or applications. If it does so in the future, it intends to take reasonable steps to ensure that such development meets acceptable SDLC standards.

9. Business Resiliency Program.
Business resiliency is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. ERP is implementing processes to ensure business continuity, disaster recovery, and incident response in the event of a cybersecurity event. ERP's program focuses primarily on defining internal processes and documentation requirements, delineating responsibility and roles in the event of a cybersecurity event, and describing response protocols and remediation goals. ERP intends to test its program regularly to assess possible risk scenarios.

10. Data encryption.
ERP intends to implement reasonable processes to encrypt and protect sensitive benefit plan data at rest and in transit.

11. Strong Technical Controls Implementing Best Security Practices.
The program has robust technical control processes, focused primarily on hardware asset management, software and firmware management, virtual perimeter security and network segregation, antivirus software, routine patch management, system hardening, data backup, and data classification.

12. Responsiveness to Cybersecurity Incidents or Breaches.
In the event of a cybersecurity incident, ERP will take action. This may include informing law enforcement, notifying the appropriate insurer, investigating the incident, giving affects plans and participants the information necessary to prevent or reduce injury, honoring any contractual or legal obligations with respect to the breach, and fixing the problem to mitigate risk of a future breach.

ERP Retirement Services, Inc.
Edward Repper
erepper@erpretirement.com