

# Aftermath of a DOL Cybersecurity Audit

## Elham (Ellie) Fayyazi

Chief of Criminal  
Investigation Division,  
Employee Benefits Security  
Administration (EBSA)  
United States  
Department of Labor  
Washington, D.C.

## Julie Tracy, CISSP

Manager, Cyber Advisory  
Withum  
Indianapolis, Indiana



The opinions expressed in this presentation are those of the speaker. The International Foundation disclaims responsibility for views expressed and statements made by the program speakers.

International Foundation  
OF EMPLOYEE BENEFIT PLANS 

# Agenda

- Developing your program
  - Assessing the program
  - Assessing your vendors and their program
- DOL requests and preparing for audit
  - What does the DOL expect to see from you?
  - Preparation for the audit

# Agenda

- Audit findings and outcomes
- Lessons learned
- Updated DOL Guidance—September 2024

# The Fund's Cybersecurity Program

- *Every* Fund should have a Cybersecurity program in place
- *Every* Fund should be managing their third-party vendors



# The Fund's Cybersecurity Program

- *Every* Fund should have annual security awareness training (including the Trustees)
- *Every* Fund should be reporting to the Trustees on their cybersecurity program



# Developing the Fund's Cybersecurity Program

- What if you don't have a program?
  - Don't panic...Well panic a little
  - Get help to put a program in place that meets the DOL guidance and is appropriate for your Fund



# Assessing the Fund's Cybersecurity Program

- The one thing you cannot do yourself
  - Independent auditor assesses security controls that provide a clear, unbiased report of existing risks, vulnerabilities and weaknesses



# Assessing the Fund's Vendors



- *Risk* assessment of third parties
- Minimum cybersecurity practices
- Periodic assessing third parties based on *risk*



# DOL Requests and Preparing for an Audit



# The Request List



- Document request or subpoena will be sent for items related to:
  - Cybersecurity policies and procedures
  - Segmentation of networks
  - Encryption.

# The Request List



- Document request or subpoena will be sent for items related to:
  - Third-party audits
  - Third-party assessments
  - All other documentation that substantiates compliance with DOL guidance.

# How to Prepare for Audit

- Preparation starts well before an Audit is ever scheduled or a request list is received
- Make sure that your cybersecurity program is aligned with DOL guidance



# After the DOL Audit

# Audit Findings and Outcomes



- The current goal is to help plans meet fiduciary duties by implementing a robust cybersecurity program
- Ensure plan understand their own environments
- Monitor service providers

# Audit Findings and Outcomes

- If potential fiduciary breaches are identified
  - Voluntary correction of identified items
- No voluntary remediation of items, DOL will consider the following:
  - Issuing VC letter
  - Filing suit against breaching fiduciaries



# Lessons Learned

# Key Takeaways

- Be prepared for a cybersecurity audit well in advance of receiving a request list
  - Implement the DOL cybersecurity guidance
  - Understand the Plan's risks
  - Understand your fiduciary responsibility
- Keep documentation related to cybersecurity program organized and up to date

# Key Takeaways

- Review and update cybersecurity program annually
- Remediate any findings from DOL cybersecurity audit in a timely manner
- Review updated DOL cybersecurity best practices (September 2024)

Your Feedback  
Is Important.  
Please Scan  
This QR Code.

Session Evaluation

