A. Overall Program	1. Well-documented program. DOL is looking for a formal, well-documented cybersecurity program. The guidance identifies specific policies and procedures that should exist and 18 areas that should be covered.
	2. Clear roles The DOL is looking for clearly defined and assigned information security roles and responsibilities. The guidance requires cybersecurity programs to be managed at the senior executive level and executed by qualified personnel.
B. Annual Duties	3. Annual risk assessment Prudent annual risk assessments that identify, estimate, and prioritize information system risks.
	4. Annual third party audit Reliable annual third party audit of security control, that should assess the organization's security controls and provide a clear, unbiased report of existing risks, vulnerabilities, and weaknesses. The organization must then document how it addresses identified weaknesses.
	5. Annual training The DOL is looking for annual cybersecurity awareness training for all personnel. Training should be at least annual, emphasize identity theft, and reflect risks identified by the most recent risk assessment.
C. Nuts & Bolts of Security	6. Access controls The DOL is looking for strong procedures to control access to plan systems and information. This includes controlling authentication and authorization. The guidance identifies 8 best practices in this area: 1. Limit access to systems, assets, and facilities. 2. Limit access privileges based on role of the user and adhere to the need-to-access principle. 3. Review access privileges at least every three months. 4. Require use of unique, complex passwords. 5. Use multi-factor authentication (MFA) wherever possible. 6. Monitor for activity of authorized users and detect unauthorized access, use of, or tampering. 7. Implement procedures to ensure that any sensitive information about a participant or a beneficiary in the service provider's records matches the information the plan maintains about the participant. 8. Confirm the identity of the authorized recipient of funds.
	7. Technical controls Best security practices for technical security include: 1. Hardware, software, and firmware kept up to date. 2. Vendor-supported firewalls, intrusion detection, and prevention appliances/tools. 3. Current and regularly updated antivirus software. 4. Routine patch management (preferably automated). 5. Network segregation. 6. System hardening (e.g., minimizing security vulnerabilities by removing non-essential programs). 7. Routine data backup (preferably automated).

	8. Data storage Data classification, storage, and destruction is an important security measure. If retirement plan data is stored or managed by a third party, should ensure that party is subject to appropriate security. The guidance identifies 4 best practices for the third party including: 1. Requiring a risk assessment. 2. Defining minimum cybersecurity practices. 3. Periodically assessing based on potential risks. 4. Ensuring that guidelines and contractual protections address: (a) the provider's access control, including the use of multifactor authentication; (b) the provider's encryption policies and procedures, and (c) the provider's notification protocol for event which directly impacts a customer's information.
	9. Encryption Data should be encrypted using current industry standards. The guidance does not specify the precise type of encryption or the scope of data that must be encrypted. Instead, it appeals to industry standards and prudence. While not in the guidance, one might look to current privacy rules, such as state law definitions of personally identifiable information (e.g., full and partial SSNs, birthdate, address, and other individualized data), in selecting what information must be encrypted.
	10. Secure Software Development Life Cycle (SDLC) process If an organization develops its own systems or applications, a secure SDLC process should be implemented to ensure security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort.
D. Incident Response	11. Business resiliency Organization should have a business resiliency program (business continuity plan, disaster recovery plan, and incident response plan) that: 1. Defines the processes for responding to an event; 2. Reasonably defines resiliency program goals; 3. Defines documentation and reporting requirements regarding cybersecurity events and response; 4. Defines roles, responsibilities, and authority levels; 5. Describes external and internal communications and information sharing, including protocols to notify the plan sponsor and affected user(s) if needed; 6. Identifies remediation plans for any identified weaknesses in information systems; 7. Includes after action reports (re: how plans will be evaluated and updated following an event); and 8. Is annually tested based on possible risk scenarios.
	12. Responses to incidents/breaches When a cybersecurity breach or incident occurs, procedures should require appropriate action be taken quickly to protect the plan and its participants, such as: 1. Informing law enforcement; 2. Notifying the appropriate insurer; 3. Investigating the incident; 4. Giving affected plans and participants the information necessary to prevent/reduce injury; 5. Honoring any contractual or legal obligations with respect to the breach, including complying with agreed upon notification requirements; and 6. Fixing the problems that caused the breach to prevent its recurrence.