TIAA Cybersecurity – An Overview of Our Alignment to the DOL's Cybersecurity Guidelines

TIAA Global Cybersecurity & Fraud Management

In April 2021, the United States Department of Labor (DOL) released cybersecurity guidelines that detail best practices for cybersecurity program management, tips for hiring a retirement plan service provider with strong cybersecurity practices, and online security tips for plan participants. The DOL's guidelines were issued in response to a March 2021 report from the Government Accountability Office (GAO) titled Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans.

TIAA fully supports both the GAO and the DOL for thoroughly addressing a topic of such great importance. We have long made cybersecurity and the protection of participant, plan and financial information a top priority and our processes are aligned and compliant with the DOL guidelines.

The second piece of guidance, Cybersecurity Program Best Practices (updated April 2024) details best practices for maintaining a strong cybersecurity defense. In addition to providing a framework for recordkeepers and other service providers responsible for plan-related IT systems and data, these tips and best practices are a valuable reference for retirement plan fiduciaries when evaluating the cybersecurity practices of service providers.

The following is a summary of TIAA's current controls and practices aligned with the DOL's recommended best practices.

1. Have a formal, well-documented cybersecurity program.

Teachers Insurance and Annuity Association of America (also "TIAA") has a formal, well-documented cybersecurity program. TIAA is an insurance company regulated by the New York Department of Financial Services. As such, TIAA is required to maintain a written, risk-based cybersecurity program ("Cybersecurity Program") pursuant to the Gramm Leach Bliley Act of 1999 ("GLBA"), the Fair Credit Reporting Act ("FCRA") as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), the respective regulations promulgated thereunder, including the Federal Financial Institutions Examination Council (FFIEC) Examination Guidance and the NY DFS Cybersecurity Regulation, and applicable state privacy laws, including but not limited to 201 CMR 17.00 et. seq. Our Cybersecurity Program is also mapped against the International Organization for Standardization/the International Electrotechnical Commission (ISO/IEC 27002) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is consistent with the DOL's "Cybersecurity Program Best Practices."

Within TIAA's Cybersecurity Program, the privacy and security of our clients' information is the top priority. TIAA combines technology, people, and process to protect client data and to identify, prevent, defend against, and respond to anticipated threats. TIAA's Cybersecurity Program is documented in enterprise policies, control standards, and standard operating procedures that reflect the procedural aspects of operations.

The policies, standards, and operational components of our Cybersecurity Program are regularly reviewed by internal stakeholders, assessed by internal and external auditors, and examined by regulators.

For more information, please see the following resources:
Cybersecurity Program Video
TIAA.org Security Center
TIAA's Plan Sponsor Resource page
TIAA's Retirement Industry Leadership and Innovation page

2. Conduct prudent annual risk assessments.

TIAA operates a robust enterprise risk management framework with explicit first, second, and third lines of defense. Cybersecurity operates within that risk framework and performs detailed risk assessments on TIAA's Information Technology ("IT") assets (including, but not limited to, business applications, servers, databases, network devices, end user devices, and suppliers). Risk classification occurs at least annually, and subsequent control assessments are performed with varied frequency based on inherent risk ratings. Emerging risks and technologies are also consistently evaluated, and new assessment capabilities are developed and put into operation as needed.

Risk assessment details are formally documented, and any findings are reviewed in accordance with TIAA's enterprise risk management framework and managed accordingly.

Within the enterprise risk management framework, TIAA additionally conducts various vulnerability assessments and employs external parties to perform targeted penetration and vulnerability assessments against our systems and networks. TIAA regularly updates its computing environment with security vulnerability patches and other similar safeguards to address identified risks.

3. Have a reliable annual third-party audit of security controls.

TIAA's Cybersecurity Program is risk-based, consistent with regulatory obligations and examination guidance applicable to financial institutions, industry standards and the DOL guidance. This risk-based approach requires the adoption, implementation and review of controls to minimize risks to customer information and includes the Federal Financial Institutions Examination Council (FFIEC) booklets, International Organization for Standardization/the International Electrotechnical Commission (ISO/IEC 27002), National Institute of Standards and Technology (NIST), as applicable.

TIAA is regularly assessed by internal and external auditors and engages a nationally recognized accounting firm to issue Statement on Standards for Attestation Engagements No. 18 (SSAE18) (formerly SSAE16, SAS70) SOC1 and SOC2 reports for Defined Contribution Retirement Recordkeeping annually. The reports include a transparent view of TIAA's business operations, as well as our cybersecurity, and IT availability controls.
With regards to cybersecurity, the most recent SOC2 covers the period of 10/1/2023 to 9/30/2024 and has an unqualified opinion and zero exceptions. TIAA is happy to provide its SOC2 results to clients, upon request.

4. Clearly define and assign information security roles and responsibilities.

TIAA's management, in particular the Board of Directors and Senior Executive Management, is responsible for overseeing the execution and delivery of TIAA's Cybersecurity Program through TIAA's Chief Information Security Officer (CISO). The CISO role is a dedicated executive position with principal responsibility for overseeing TIAA's Cybersecurity Program as dictated in TIAA's IT policies, standards, and operating procedures.

The CISO also chairs TIAA's Information Security Leadership Committee (ISLC) which has been established with representation from Technology, Legal, Operations Risk, Compliance, Business Operations, Internal Audit, and others to:

- Create enterprise strategic planning for security priorities
- Recommend and approve IT policies and standards for enterprise adoption
- Ensure cross-functional collaboration on all security incidents
- Identify, select and adapt controls based on identified threats, risks and cost-benefit analysis
- Provide guidance and leadership for protecting information from unauthorized access, destruction, modification, and disclosure
- Initiate and monitor associated risk action plans, progress against plans, and supporting performance and operational metrics
- Leverage and implement IT risk best practices across all business areas
- Coordinate corporate security initiatives at the senior leader level
- Ensure representation from all business areas to provide a firm-wide approach to information security

5. Have strong access control procedures.

TIAA's Cybersecurity Program maintains a comprehensive identity and access management program that provides oversight on the following related controls for TIAA's workforce:

- Systems access and entitlements are granted on a need-to-know basis. Only the minimum level of access required for successful job completion is permitted.
- Systems access and entitlements are reviewed by management on a recurring basis and revoked when job functions change or upon separation from TIAA. Initial access and entitlements are only provisioned with appropriate management approvals.
- Password requirements are based on industry best practices.
- Multi-factor authentication is required to access TIAA's network.
- TIAA's participant websites implement risk-based adaptive multi-factor authentication to secure user authentication and sensitive transactions; users can elect to always use a one-time PIN or biometrics (on TIAA's mobile app and IVR) to authenticate.

6. 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.

TIAA operates a robust enterprise risk management framework with explicit first, second, and third lines of defense. As part of that framework, TIAA operates an explicit Supplier Risk Management function that oversees initial and recurring risk assessments of suppliers. Suppliers are assessed against TIAA's policies and standards before engagement and risks are documented, classified, and managed. Suppliers are reassessed on a recurring basis.

TIAA's contracts with suppliers address cybersecurity concerns as stated in the DOL guidelines.

7. Conduct periodic cybersecurity awareness training.

TIAA operates an enterprise-wide cybersecurity training and awareness program that drives a culture of security accountability across TIAA's workforce. The program aims to ensure TIAA's workforce understands comprehensive security is the responsibility of every employee at TIAA, and not just the responsibility of cybersecurity professionals or technological controls. TIAA's workforce is educated to recognize attack vectors, maintain vigilance, and on how to report any potential threats.

TIAA's workforce is required to complete formal risk management and cybersecurity training upon joining the company and also on a recurring basis. TIAA further provides targeted online training to certain employees based on their role or at-risk behaviors. Examples of this more targeted formal training can include extensive training on secure coding for employees operating in software development roles and specialized training for privileged users. Training completion is monitored, recorded and reported to management.

TIAA also conducts recurring phishing email simulations across TIAA's workforce. Phishing continues to be an effective attack vector for malicious parties, and this program drives vigilance and accountability around these dangers. Phishing simulation results are reported to TIAA's Board of Directors to ensure proper visibility and oversight. TIAA additionally sponsors recurring cybersecurity-related enterprise communications and enterprise-wide events that remind employees of their security responsibilities. TIAA's phishing awareness program was awarded a 2022 CSO50 award for innovation and TIAA's broader cybersecurity program has been awarded a CSO50 award in other areas every year since.

Within TIAA's Cybersecurity Program, TIAA further ensures its cybersecurity workforce undergoes continuous training on security tools, emerging threats and cybersecurity concepts. TIAA has a strong academic relationship with New York University (NYU) and has a significant number of employees pursuing cyber-related graduate degrees at the school, the most of any of NYU's current industry partners.

8. Implement and manage a secure system development life cycle (SDLC) program.

TIAA's software development teams adhere to a policy-based secure systems development life cycle (SDLC) methodology to manage software development and ongoing systems maintenance. This methodology, and associated governance activities, ensure proper software development procedures. These procedures include, but are not limited to, planning, analysis, design, development, testing, and user documentation, and further include analysis, design, implementation, and testing of security requirements. Using a risk-based approach, the methodology requires software development teams to collaborate with Cybersecurity Architects and cybersecurity subject matter experts to help ensure security policy and standards are included. Developers additionally deploy integrated vulnerability scanning tools and use a risk-based approach to remediate findings accordingly. Developers are required to undergo formal training on secure coding and tools.

TIAA's policies and standards dictate security features and functionality that must be included in appropriate transaction-based software to ensure alerts, logging, and additional user validation (i.e., multi-factor authentication for certain transactions) are in place, per regulatory guidance. As part of TIAA's enterprise risk management framework, business applications (regardless of source or hosting) are assessed for risk against all applicable policies and standards on a recurring basis.

TIAA additionally conducts network, host, and application vulnerability and risk assessments, and employs external parties to perform targeted penetration and vulnerability assessments against systems and networks. TIAA regularly updates its computing environment with security vulnerability patches and other similar safeguards to address identified risks.

9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

TIAA has well-documented business continuity and disaster recovery programs and plans that are regularly reviewed and tested. Business-critical functions are required to have procedures in place to make sure business operations can continue in an emergency. TIAA's business continuity plan covers operational criteria including, but not limited to:

- Backing up and recovering data
- Building redundancy into all critical systems
- Maintaining geographically diverse business center locations, personnel, processes and technology
- Minimizing financial, operational and credit risk exposures
- Establishing alternate ways to communicate with our participants
- Confirming emergency contacts and alternate business facilities for our employees
- Arranging emergency procedures with critical business partners, such as banks
- Communicating with and reporting to regulators
- Ensuring participants have prompt access to their accounts and funds

10. Encrypt sensitive data, stored and in transit.

TIAA’s Cybersecurity Program implements a comprehensive data loss prevention program that defines data classification parameters, educates TIAA’s workforce on those parameters, provides tools to support data classification efforts, and implements numerous controls to reduce the risk of any unauthorized data exposure. These controls include, but are not limited to, encryption of sensitive data in storage, encryption of sensitive data in transit, encryption of portable employee devices, and network monitoring.

The controls implemented by TIAA’s data loss prevention program are dictated by TIAA’s IT policies and standards.

11. Implement strong technical controls in accordance with best security practices.

TIAA’s Cybersecurity Program implements numerous layers of comprehensive technologies to prevent, detect, and respond to malicious activity and to protect client data and company assets from anticipated threats. TIAA implements the latest in firewall, intrusion prevention, antivirus, backup, and other technologies. Recurring scanning is conducted to identify vulnerabilities in hardware, software, and firmware models, and versions and stringent patching requirements are enforced, monitored, and reported to management.

12. Appropriately respond to cybersecurity incidents.

TIAA implements and maintains a multi-disciplinary, enterprise-wide incident response program based on the banking regulators’ “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.” In the event of an incident or breach, there are procedures in place to investigate, contain, and mitigate the impact and risk to clients and the enterprise, as well as to restore capabilities or services that were impacted. As part of our incident response plan, if there was a breach of customer data, TIAA follows all applicable state and federal regulations regarding notification of affected individuals and regulators; TIAA also offers credit monitoring, identity theft repair and insurance at our expense. It is also TIAA’s practice to reinstate a participant’s account for any financial losses that may occur due to unauthorized access to the account, through no fault of their own. For more details please read the Customer Protection Policy details on TIAA.org.

TIAA