Docket No: ED-2025-SCC-0581
Submitted via *regulations.gov*

On behalf of the National Council of Higher Education Resources (NCHER) guaranty agency (GA) members, thank you for the opportunity to provide initial comments and questions to the proposed revision to the Guaranty Agencies Security Self-Assessment and Attestation. The GAs share the Department of Education's commitment to data security; however, due to the government shutdown the GAs have not had the opportunity to discuss these changes with the Department of Education/Federal Student Aid. The GAs respectfully request the Department avoid changing the established rules of engagement or expectations partway through an active audit cycle. Mid-year cycle adjustments can create confusion for both the auditors and auditees and can undermine the consistency and comparability that make these reviews most effective. We value our working relationship and appreciate the Department's continued partnership to ensure strong oversight and compliance. If new requirements or interpretations are being considered, the GAs welcome the opportunity to review and plan for those changes ahead of the of the next audit cycle to ensure a smooth and transparent transition. The initial list of questions and concerns include but are not limited to the following issues.

The Department has provided responses in **bold**:

- Will the CIS AWS Foundations benchmark controls apply to all FISMA levels?
    - **Please clarify what is meant by "FISMA levels". From the Assessment Team's perspective, the FISMA levels are the system security categorizations defined by FISMA as Low, Moderate, and High. The CIS AWS Foundations benchmark controls will apply to any FISMA level if the system is leveraging an AWS Infrastructure as a Service (IaaS) cloud service model.**
- What is meant by automated versus manual?
    - **The Automated controls involve writing scripts or programming language to deploy the stated configuration(s) in the environment (e.g., Terraform, CloudFormation, etc.). The Manual controls involve deploying the configuration(s) manually via the console GUI. These identifiers are not necessary for the Cloud Assessment and have been removed from the control text.**
- CIS has recently released v6.0.0 of the CIS AWS Foundations benchmark. V5.0.0 is no longer available for review. Will v6.0.0 be sufficient as a benchmark and will FSA update their requirements to align with v6.0.0?
    - **The Cloud Assessments have not yet moved to CIS AWS Foundations Benchmark v6.0.0 but systems should securely configure their IaaS environment in accordance with the most recent benchmark. The Cloud Assessor has the ability to align different versions of the CIS AWS Foundations Benchmark checks to determine compliance.**

- AWS Security Hub has the ability to perform automated compliance checks based on CIS AWS Foundations benchmark controls. The most recent version of the AWS foundations benchmark available in Security Hub is v3.0.0. Will evidence from SecurityHub, which reflects v3.0.0, be sufficient to satisfy the FSA review?
    - **CIS AWS Foundations Benchmark v3.0.0 SecurityHub exports can satisfy the Cloud Assessment. As previously mentioned, the Cloud Assessor has the ability to align different versions of the CIS AWS Foundations Benchmark checks to determine compliance.**

- CIS AWS Foundations benchmark specifies specific steps to demonstrate compliance. Will FSA expect evidence to be produced in alignment with these steps?
    - **While the CSPM export typically identifies whether the control is compliant or not, there may be instances where the control is missing from the CSPM reports or has been identified as non-compliant when it actually is. In those instances, the Cloud Assessor will conduct a shoulder surfing session of the environment with the system SME's to validate whether the control is compliant. If a shoulder surfing session cannot be accomplished, evidence (e.g., screenshots) will be requested to validate compliance.**