Background: In FY25, CCISD used SLCGP funding to complete an independent external penetration test (“black box” testing) that evaluated whether an outside attacker could gain access to district systems. The tester was not able to move into internal accounts or systems, and the primary findings were limited to four vulnerabilities tied to a third-party system, which the vendor addressed.

Building on that successful assessment, CCISD now proposes an FY27 application to conduct an internal, credentialed penetration test, using controlled CCISD test credentials and, as appropriate, district devices, to more realistically evaluate what could occur after initial access and to identify internal attack paths and improvement priorities.

Federal Pass-Through Grants (DHS via Texas OOG/PSO)	Generals (Deliverables / Requirements / Flexibility / Restrictions)	Amount
State and Local Cybersecurity Grant Program (SLCGP) – Objective 2: Assessment & Evaluation (FY25 – Completed) To understand CCISD’s cybersecurity posture and identify areas for improvement through independent testing and structured assessment activities.	**Deliverables:** Third-party penetration testing, periodic external exposure (“attack surface”) checkups, technical findings reports, prioritized recommendations, and follow-up validation insights to support improvement planning. **Have to:** Manage a vendor-led assessment process; maintain documentation for procurement, deliverables, and grant compliance; provide the required match through in-kind personnel time; use results to inform district prioritization and reporting. **Get to:** Obtain an independent “safety inspection” of CCISD’s digital environment to identify real-world weaknesses and prioritize fixes based on risk. **Length:** 11/1/2024 - 10/31/2025. **Cost / Match:** Awarded **$54,753.50**; matched **$10,954.86** (in-kind personnel); total project cost **$65,708.36**.	$54,753.50
State and Local Cybersecurity Grant Program (SLCGP) – Objective 2: Assessment & Evaluation **(FY27 – Proposed Application)** Application due 02/12/2026; earliest start 09/01/2026; up to 12 months To evaluate CCISD’s cybersecurity posture through independent, structured testing that identifies exploitable vulnerabilities and internal attack paths, clarifies how far an intruder could progress after initial access, and delivers prioritized, actionable recommendations to guide district risk reduction efforts.	**Deliverables:** Internal penetration test deliverables including scope/rules of engagement, testing results, prioritized findings, and recommended actions; documentation to support planning and risk reduction. **Have to:** Meet eligibility and submission requirements (governing body resolution and required certifications/assurances); provide a 30% match; maintain SAM/UEI; meet state requirements for cybersecurity training certification; participate in required post-award CISA services and join TX-ISAO. **Get to:** Conduct a more realistic evaluation of internal risk by simulating what could happen after initial access, strengthening how CCISD prioritizes improvements and validates protections. **Cannot:** Use funds for prohibited costs (e.g., ransomware payments, spyware, cybersecurity insurance premiums, construction/renovation, or non-cybersecurity purposes). Funds must remain focused on Objective 2 assessment/evaluation activities. **Length:** Up to a 12-month project period, beginning on/after 09/01/2026 (subject to FEMA/CISA approval). **Looking ahead:** FY27 refines the FY25 approach by adding credentialed internal testing; testers would be granted controlled, time-limited CCISD credentials and may use district devices on the network. This better simulates real-world conditions and helps CCISD understand what a threat actor could potentially accomplish after gaining initial access.	TBD