The New PCI Standards

What Every Government Needs to Know

BY BENJAMIN DAVIDSON

Governments that process, store, or transmit credit card information must adhere to Payment Card Industry (PCI) Data Security Standard compliance standards (PCI DSS). Being PCI compliant ensures the secure handling of customer payment card data, minimizes the risk of data breaches, and protects customers' trust. Governments that aren't compliant may face fines and additional expenses from their merchant services providers or even lose the ability to process payments with certain providers. GFOA has long recommended that governments ensure PCI compliance and have robust policies and procedures in place to evaluate and implement compliance, including conducting an annual PCI compliance review.

An annual review of the card brands accepted, the volume of card transactions, and the number and types of payment flows an entity uses, among other activities, will determine the government's scope of responsibility for PCI compliance. Governments should also understand any updates to PCI DSS.

On April 1, 2025, revised PCI compliance protocols, known as PCI 4.0, became mandatory.

GFOA members should familiarize themselves with these changes to ensure compliance with the updated standards. The 12 core PCI compliance requirements remain the same, but there are updated and new component requirements, as well as a shift in how an organization can achieve those requirements.

"For government entities, PCI compliance isn't just about securing transactions—it's about protecting public trust."

–**SCOTT DINGMAN**, COALFIRE SYSTEMS

Some of the key changes include:

- **Reporting changes** to the self-assessment questionnaire (SAQ) and the Report on Compliance (RoC) template, as well as focusing on ongoing monitoring and assessment rather than singular point-in-time assessments.
- **New requirements** include preventative measures against phishing, website, and skimming attacks; periodic review of access privileges, documentation requirements, vulnerability scans, and testing; and password and multi-factor authentication (MFA) requirements.
- **Updated requirements** include implementing security incidence response plans, monitoring access to sensitive areas, group and shared accounts authentication, and limiting invalid authentication attempts.
- **A focus on outcomes** rather than a prescriptive approach to implementing and validating PCI DSS. Using a customized approach comes with its own risks and challenges, however, and is better suited to more sophisticated entities.

Governments should talk with their merchant services providers for additional and specific information on the ways in which new and existing PCI compliance rules apply to the government. "For government entities, PCI compliance isn't just about securing transactions—it's about protecting public trust. A single data breach can compromise citizens' financial information, erode confidence, and lead to costly legal and regulatory consequences. Compliance ensures not only security but also the integrity of government operations," according to Scott Dingman, principal consultant at Coalfire Systems. "The latest PCI updates in 2025 represent a dramatic shift in how these entities are held accountable, manage risks, and report their compliance."

As governments work to ensure compliance with the updated PCI requirements, they should:

- Complete an internal assessment to better understand the necessary scope of PCI compliance. Governments may consider outsourcing this assessment to a qualified security assessor (QSA). The PCI Security Standards Council provides a list of QSA providers (at pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors).
- Talk with your merchant services provider, solution provider, and/or acquiring bank to determine the government's responsibilities and how the provider can help with evaluating scope and processes to ensure compliance.
- Have policies and procedures in place that include the updated standards, including reporting and infrastructure changes.
- Ensure PCI compliance certifications from third-party payment vendors.
- Use PCI standardizations rather than individual customizations within your payment card program.
- Include questions about aiding the entity with PCI compliance standards (for example, upgraded terminals) in merchant services RFPs.
- Bookmark PCI and GFOA resources on PCI compliance.
- Look to peers and PCI consultants/QSAs to help PCI compliance today and tomorrow.

Governments that Use Third-Party/Outsourced Payment Providers

The updated protocols may require limited changes for governments that outsource their payment card receivables; the government is still responsible for ensuring that its vendor systems are PCI compliant. Governments should talk with their payment processing providers to determine if any change or update to its processes are needed to remain compliant. At a minimum, governments should have the providers annually submit a written certification that they are PCI compliant.

Benjamin Davidson *is a consultant with GFOA's Research and Consulting Center.*

Want to learn more?

Attend the *Protecting Paperless Payments: Achieving PCI and Nacha Compliance* session at GFOA's annual conference, June 29–July 2, 2025, in Washington, D.C.