

Puerto Rico Outlines Minimum Cybersecurity Standards for Government Entities and their Contractors

ATTORNEYS

- Arturo J. García-Solá
- Rubén Méndez-Benabe
- Lizzie M. Portela-Fernández
- Ernesto N. Mayoral
- Adrián P. Goyco-Vera
- Isabel Torres-Sastre
- Ignacio Portela-Cabán

PRACTICE AREAS

- Data Privacy & Cybersecurity Practice Team

An McV Data Privacy & Cybersecurity Practice Team Alert

February 2, 2024

On January 18, 2024, the Governor of Puerto Rico signed into law the Cybersecurity Act of the Commonwealth of Puerto Rico, Act No. 40-2024 (“[Act 40](#)”). Act 40 introduces a comprehensive cybersecurity framework required to be adopted by the Executive Branch of the Commonwealth of Puerto Rico, its agencies, departments, public corporations (the “Government”), and any natural or legal person doing business or having contracts with the Government (the “Contractors”).

Accordingly, the Government and its Contractors are required to, among others:

- establish control mechanisms to stop inappropriate material, malware and other threats
- establish control mechanisms to protect the confidentiality and integrity of information, including the use of encryption in their systems
- establish policies regarding the adequate use of information systems
- report any cybersecurity incident within 48 hours; and
- comply with industry practice and standards when accepting credit cards payments in web portals.

Under Act 40, the Puerto Rico Innovation and Technology Service (“PRITS”) is entrusted with the responsibility of ensuring the secure administration of information resources and implementing regulations, standards, and procedures pertaining to the security of information technologies at the governmental level. PRITS, together with the Puerto Rico Bureau of Statistics, are mandated to publicly disclose cybersecurity incident statistics reported by governmental agencies on their respective websites. Act 40 also creates a Chief Information Security Officer of the Government position, which, among other functions, will oversee the Office for Cyber Incident Assessment. This Office is tasked with establishing cybersecurity protocols and overseeing compliance with Act 40.

Puerto Rico Outlines Minimum Cybersecurity Standards for Government Entities and their Contractors

Puerto Rico government agencies are required to confer with PRITS before engaging in any contract, amendment, or renewal with a Contractor. Act 40 empowers PRITS to terminate contracts that are found to be non-compliant with the established cybersecurity standards.

The Government has until July 18, 2024, to comply with the provisions of Act 40.

The content of this McV Alert has been prepared for information purposes only. It is not intended as, and does not constitute, either legal advice or solicitation of any prospective client. An attorney-client relationship with McConnell Valdés LLC cannot be formed by reading or responding to this McV Alert. Such a relationship may be formed only by express agreement with McConnell Valdés LLC.