(H. B. 1530)

(No. 40-2024)

(Approved January 18, 2024)

AN ACT

To create the "Commonwealth of Puerto Rico Cybersecurity Act"; establish as a public policy principle that providing data security to the Government is essential to support innovation processes and promote the sustainable economic development and growth of all sectors of Puerto Rico; create the position of Chief Information Security Officer within the Puerto Rico Innovation and Technology Service ("PRITS") and establish its powers and duties, in order to ensure the implementation of the public policy established herein; establish the Agencies' duty to collaborate with PRITS and the Chief Information Security Officer; create the Cyber Incident Review Office within PRITS; direct PRITS to adopt and promulgate regulations in all agencies pursuant to the provisions of this Act; establish employer-employee relationship relating to the use of its systems; and for other related purposes.

STATEMENT OF MOTIVES

Contrary to what people may think, cybersecurity has existed since the creation of the Internet. The only difference is that, in the last 24 to 36 months, there has been a significant increase in the number of attacks, infiltration strategies, and unauthorized accesses to information systems that have compromised the Island's security and businesses through the use of ransomware, and information theft or manipulation.

Cybersecurity is a subset of information security that aims to protect information in interconnected systems. There are other concepts related to cybersecurity such as cybercrime, cyber threats, or cyberspace, whose main and common feature lies in their existence in the network.

The World Economic Forum and the United Nations (UN) have stated that cybercrime is among the greatest risks to humanity together with natural disasters

and climate change and, in addition, the COVID-19 pandemic which have aggravated the online risks for all industries within a short period.

The crisis caused by the COVID-19 pandemic in early 2020 has highlighted our dependence on an essential infrastructure which most citizens are unaware of or barely notice. Our daily lives revolve around more digital activities each day; therefore, we are more vulnerable to cyber threats. Food supply chains, transportation, payments and financial transactions, educational activities, government transactions, emergency services, and even the water and electric power supply systems, among countless other activities, currently operate using digital technologies.

The COVID-19 pandemic helped us reflect on how the expansion of information and communications technologies, Internet connectivity, and cybersecurity has progressed in Puerto Rico. Society's increased dependence on the Internet during the crisis highlights the need to focus on the lessons learned in order to anticipate an ever-changing society and economy as well as guarantee cybersecurity at the national level.

In a more general sense, cyber attacks have increased in both frequency and complexity during the last decade. The low cost and minimum risk entailed by these crimes have played a key role in their increase. By simply using a computer and having internet access, cyber criminals can cause significant damage while remaining relatively anonymous.

Both people and institutions are vulnerable to the uncertainty and unpredictable nature of cybercrime; therefore, efforts to tackle these threats are essential. Such efforts should be multidimensional in nature because a variety of factors are required to build a resilient society. Policies and legal frameworks should conform to, and all interested parties from the civil society, as well as the public and private sectors, should work towards creating a culture that is cyber

aware and training qualified professionals to develop a cybersecurity strategy. For such reasons, this is an ongoing and complex effort.

The increasing number of cyber attacks has aroused greater interest in cybersecurity worldwide. For example, online searches for the word "cybersecurity" in one of the most well-known search engines increased from 20 to 100 between March 2016 and June 2019. In other words, there has been an growing interest in cybersecurity among Internet users. Furthermore, users who look into cybersecurity tend to search for the courses and training opportunities available in this field. There is a growing awareness of the importance of cybersecurity and more people are looking for ways to increase their cybersecurity literacy.

Cybersecurity policies are essential to safeguard the rights of citizens online, such as the right to privacy and property, as well as to increase citizen's trust in digital technologies so that they may feel comfortable using them. Cybercrime already makes up approximately half of all crimes against property worldwide. In the aggregate, these figures become even more significant because the economic impact of cybercrime could exceed 1% of the Gross Domestic Product in some countries. In the case of attacks against critical infrastructure, this figure could reach up to 6% of the GDP.

The damage caused by insider threats can be difficult to detect because such threats can encompass a broad range of behaviors and motives. A threat can arise from a disgruntled employee who aims to interrupt operations, a staff member who seeks to earn extra money by selling data, or a well-intentioned co-worker who, in order to save time, simply disregards a security policy implemented by the business.

Puerto Rico is still not properly prepared to face the cyber attacks being carried out. The Island suffered over 926 million cyber attack attempts in 2021 and

more than 12.4 million attacks had been confirmed by mid-2022. However, identifying a cyber threat is just the first step. Taking action against cyber threats and cybercrime poses an even greater challenge for the Island. The truth is that we have limited resources to investigate cybercrimes. Furthermore, prosecuting such crimes is an even greater challenge. In many instances, the law itself is part of the problem: one-third of all countries (including Puerto Rico) do not have a legal framework in place for cybercrimes.

On February 1, 2021, Puerto Rico created the Government Information Security Office upon contracting the Chief Information Security Officer (CISO). Said Office is responsible for providing centralized cybersecurity services to the Government through collaboration agreements with federal agencies and external service providers, as well as protecting and strengthening the security of the Government's data and information systems by implementing controls, monitoring, and quick cyber incident response.

Having well-trained professionals has become essential to design and implement the cybersecurity policies and measures necessary to ensure the Island's resilience to ever more sophisticated and complex cyber attacks.

From a cybersecurity standpoint, people erroneously acknowledge that the subject of cybersecurity can only be left to experts and, in a more in-depth technical sense, perhaps it is. However, cybersecurity is an essential matter that all executives and managers should oversee, and it should be included as an educational requirement for all users of systems and technologies such as computers and mobile devices. Users should be wary of information being extracted by the applications on their mobile devices, particularly when those applications play a key role in their work. Applications like Google Drive, Dropbox, or One Drive are a few examples of these types of applications.

The development of a comprehensive cybersecurity strategy shall enable the Island to take a more integral approach that shall allow it to better understand and respond to cybersecurity challenges. Likewise, this strategic planning shall allow the Island to prioritize its cybersecurity goals and investments.

Countries must be prepared to rapidly adapt to the changing environment that surrounds them and to make decisions based on an ever-changing threat landscape. Improving our readiness level shall require a comprehensive and sustainable cybersecurity policy supported by assertive public actions, as well as the allocation of financial resources and trained human capital necessary to implement it.

Protecting the digital space is an ever-increasing challenge. We must be proactive and more effective at developing and implementing laws that help mitigate Puerto Rico's cybersecurity problems. All citizens have a digital life that must be protected; therefore, the Government has to serve as a shield that protects the information of its citizens and safeguards their privacy so they feel safe in the digital world.

In light of the foregoing, this Legislative Assembly is convinced that the time has come to create a regulatory framework in order to formulate a robust and comprehensive cybersecurity public policy that brings about and promotes economic development within a secure and trustworthy environment. This Act is approved for such purposes.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF PUERTO RICO:

Section 1.- Title.

This Act shall be known as the "Commonwealth of Puerto Rico Cybersecurity Act."

Section 2.- Applicability.

The provisions of this Act shall apply to the Executive Branch including all departments, boards, instrumentalities, commissions, bureaus, offices, agencies, administrations or bodies, political subdivisions, public corporations, and municipalities. It shall likewise apply to every natural or juridical person doing business or having contracts with the Government including, but not limited to, private persons performing public services and duties, but only with respect to the public services and duties being performed; any public or private administration exercise in which public resources or funds were committed or invested (directly or indirectly), or in which any public servant exercised his authority with regards to the data collected as a result of such activities.

Section 3.- Public Policy.

It is hereby established as the public policy of Puerto Rico:

1. To establish minimum cybersecurity standards and principles based on the "zero trust architecture" concept in order to enable the Government to incorporate cybernetic and electronic technologies into Government operations so as to transform and streamline intragovernmental relations, and government relations with the general public, as well as with local and foreign businesses, thus making the Government more accessible, effective, and transparent, in a secure and reliable manner;

2. To establish as policy that all covered agencies, or natural or juridical persons, as well as their agents, insurers, or guarantors are prohibited from making any Ransom Payments in response to a Ransomware attack and that they shall collaborate with the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, as provided in the State and Local Government Cybersecurity Act of 2021. As an exception, and on a case-by-case basis, a Ransom Payment may be considered in the case of:

a. Critical infrastructure; or

b. Imminent risk of death;

If a Ransom Payment is made due to any of the aforementioned reasons, upon consultation with the Office, it shall not be deemed a violation of this Section.

3. To protect and maintain the confidentiality, integrity, and availability of the data stored and/or maintained by the Government's Information Resources and the related infrastructure assets, whether the data is at rest (stored), in-transit (being sent or received), or being created or transformed (processed);

4. To increase efforts to coordinate and improve the security of government networks and critical infrastructure as well as protect the data contained therein;

5. To enhance the capabilities and efforts to block, detect, prevent, protect from, and respond to threats against Information Resources and Government Data;

6. To ensure a stable and secure Information Technology (IT) environment through the implementation of measures as are appropriate to mitigate cybersecurity risks by preventing, reducing, and limiting data loss or the degradation of the Government's Information Resources, and by implementing corrective measures and protocols that ensure that any imminent attack shall be addressed and resolved swiftly;

7. To protect the right to privacy of citizens without limiting their right to peaceful coexistence online;

8. To stop and punish persons misusing any type of Information Technology to commit criminal acts;

9. To comply with the basic cybersecurity guidelines established by the President of the United States, the Hon. Joe Biden, through the Executive Order issued on May 12, 2021, and with any subsequent orders related to cybersecurity.

Section 4.- Definitions.

For the purposes of this Act, except as otherwise provided, the following terms shall have the meanings stated hereunder:

(a) "Unauthorized Access"- when a person, group, code, program, application, or any other entity or information process obtains logical, digital, or physical access, without authorization or consent, to a critical infrastructure network, system, data, application, data room, or other information technology resource of the Government, or when access to information or resources that are not necessary to perform a task or duty, in accordance with the Principle of Least Privilege, is obtained or there is an attempt to obtain such access.

(b) "Sensitive Assets"- means information, equipment, or media, which if lost, misused, or without authorization is accessed or modified, could adversely affect Government interests and/or the privacy of citizens.

(c) "Agency"- means the set of functions and includes offices and positions all of which constitute the entire jurisdiction of an appointing authority regardless of it being designated as a department, public corporation, office, administration, commission, board, or otherwise.

(d) "Cybersecurity and Infrastructure Security Agency (CISA)"- the agency within the U.S. Department of Homeland Security that is responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states and jurisdictions, and improving the government's cybersecurity protections against private and nation-state hackers as provided in the Cybersecurity and Infrastructure Security Agency Act of 2018.

(e) "Zero Trust Architecture"- means the assumption that no connection, user, or asset can be implicitly trusted without verification.

(f) “Authorization”- means the process of granting a user access privileges to information or information systems according to the Principle of Least Privilege.

(g) “Cyber Attack”- The term “cyber attack” means the use of unauthorized or malicious code on an information system, or the use of another digital mechanism, such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system.

(h) “Cybersecurity”- shall mean prevention of damage to, protection of, and restoration of computers and electronic communications systems and/or services, including the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

(i) “Confidentiality”- means preserving the restrictions on information access and disclosure, including means for protecting personal privacy and confidential information.

(j) “Credentials”- means the unique attributes provided to each authorized user to access information system resources and applications.

(k) “Data”- means any sequence of one or more symbols to which meaning is assigned through interpretation.

(l) “Minimum Cybersecurity Standards and Principles”- means a framework that provides strategic objectives and priorities for network security and Information Resources.

(m) “Incident Handling”- means all the administrative, physical, and technical procedures implemented to investigate and mitigate reported incidents or suspected incidents. It includes notifying the parties or individuals affected by the

Incidents of any violations or breaches, as applicable, pursuant to federal and local regulations.

(n) "Government"- means the Commonwealth of Puerto Rico.

(o) "Incident" or "Cybersecurity Incident"- means an occurrence that (i) actually or imminently jeopardizes, without authority, the integrity, confidentiality, or availability of information, or an information system, process, or Information Resource; or (ii) is a misuse of an Information Resource or constitutes a violation or imminent threat of violation of law, security policies, security procedures, acceptable use policies, or standard cybersecurity practices.

(p) "Critical Infrastructure"- refers to the services, systems, resources, and essential assets, whether physical or virtual, the incapacity or destruction of which would have a debilitating impact on Puerto Rico's cybersecurity, health, economy, or any combination thereof.

(q) "Institute" or "Institute of Statistics"- refers to the Puerto Rico Institute of Statistics, created by virtue of Act No. 209-2003, as amended, known as the "Puerto Rico Institute of Statistics Act."

(r) "Office"- refers to the Cyber Incident Review Office created under this Act.

(s) "Ransom Payment"- The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a Ransomware attack, excluding legitimate payments for incident response services.

(t) "Chief Information Security Officer"- means the Chief Information Security Officer of the Government.

(u) "Principle of Least Privilege"- Each entity (process, user, or program, depending on the subject) shall only have access to the information and resources necessary for it to perform its legitimate function.

(v) "(PRITS)"- means the Puerto Rico Innovation and Technology Service Office of the Executive Branch in charge of implementing, developing, and coordinating the public policy of the Government on innovation, information, and technology, as provided in Act No. 75-2019.

(w) "Program" or "Software"- refers to the computer programs and associated data that may be dynamically written or modified during execution.

(x) "Managed Service Provider"- means an entity, whether a natural or juridical person, public or private, that delivers services, such as network, application, software, infrastructure, or security measures, via ongoing and regular support and active administration on the premises of an Agency, in the data center of the Agency (such as hosting), or in a third-party data center.

(y) "Ransomware"- The term "Ransomware"

i. means a Cyber Attack that includes the threat of use of unauthorized or malicious code on an Information Resource, or the threat of use of another digital mechanism such as a denial-of-service attack, to interrupt or disrupt the operations of an Information Resource or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an Information Resource to extort a demand for a Ransom Payment; and

ii. does not include any such event where the demand for payment is made by a Federal Government entity, for good-faith security research, for incident response services, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.

(z) "Information Resources"- means information and related resources, such as personnel, equipment, programs, and Information Technology, among others.

(aa) "Risk"- means any reasonably identifiable circumstance or event with the potential to adversely impact network security and Information Resources.

(bb) "Information Security"- means the combination of controls, safeguards, and other measures implemented by an organization to protect the information contained in any format. This implies the protection of information technology assets, regardless of whether such assets are interconnected.

(cc) "Information Technology (IT)"- The term "Information Technology (IT)"

i. For an Agency, it means any interconnected system or resource, or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, destruction, transmission, or reception of data or information, if the equipment is used by the agency directly or by a contractor under a contract with the agency that requires the use (i) of that equipment; or (ii) of that equipment to a significant extent for the performance of a service or the furnishing of a product;

ii. includes computers, ancillary equipment, (including the imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by a computer's central processing unit, software, firmware, and similar procedures, and services (including support services) and related resources.

Any word importing the singular shall also include the plural, except when the context indicates otherwise. Likewise, any terms importing the feminine gender shall include the masculine gender, and vice versa.

The definitions herein provided shall be evaluated in accordance with the definitions promulgated by the National Institute of Standards and Technology (NIST).

Section 5.- Implementation of Public Policy.

The Puerto Rico Innovation and Technology Service (PRITS) shall be responsible, pursuant to the public policy established herein, for ensuring the secure management of Information Resources and implementing information technology security standards and procedures at the government level. Moreover, it shall advise Agencies, update and develop the Government's cybersecurity strategies and plans, and ensure Agencies' compliance therewith.

Every Agency, in conjunction with PRITS, shall develop, document, and implement a Cybersecurity program in accordance with this Act. The program shall include, at a minimum, all of the Agency's information assets, including third-party information technology services, a Cybersecurity risk assessment to be conducted by the Agency at least once annually, an education plan to educate its personnel, contractors, and customers (citizens), which shall include specialized courses on the best Cybersecurity practices to develop system and information technology administrators, and penetration testing to assess internal and external vulnerabilities and validate the effectiveness of the security controls implemented by the Agency.

PRITS shall review and evaluate the Cybersecurity programs of each Agency to validate that they are consistent with the standards and principles adopted by PRITS, and that they comply with the provisions of this Act and any other applicable law.

PRITS shall identify critical Government information technology systems and services and develop and implement plans to validate the effectiveness of their security controls.

PRITS shall ensure that every Agency publishes its Privacy Policy on its website and makes it available to citizens.

PRITS, in conjunction with any other Agency it deems pertinent, shall develop and publish a Cybersecurity Emergency Protocol.

The Institute and PRITS shall be required to disclose and make publicly available on their websites the statistics on the Incidents reported by the Agencies while ensuring that Confidential information regarding the Government's Information Resources is protected.

The Institute and PRITS shall also coordinate with the private sector to publish the Incident notifications they receive, provided that the disclosure thereof has been willingly authorized.

Section 6.- Chief Information Security Officer of the Government.

The office of Chief Information Security Officer of the Government is hereby created within PRITS. However, this office shall enjoy a certain level of autonomy to enable it to perform its duties independently with the resources provided by PRITS. Upon the creation of this position, the Office of Management and Budget shall authorize and create the position of Chief Information Security Officer of the Government as well as notify the Government of Puerto Rico Human Resources Administration and Transformation Office to ensure compliance with all the applicable laws and regulations.

The Chief Information Security Officer shall be appointed by the Chief Innovation and Information Officer of the Government. The person appointed as CISO must be of recognized professional capacity.

The Chief Information Security Officer shall be responsible for implementing the appropriate security measures to prevent any unauthorized access to, and the disclosure, use, damage, degradation, and destruction of its digital information, systems, and critical infrastructure. CISO shall also be

responsible for mitigating Risks and reducing the impact and cost of Cyber Attacks by establishing the framework for the minimum information technology (IT) security requirements, defining roles and responsibilities, and establishing the information security standards.

The Chief Information Security Officer shall work, in conjunction with the Institute and the personnel designated by each Agency, to carry out such duties and formulate and implement strategies to protect the Government's public information.

Section 7.- Minimum Cybersecurity Standards and Principles.

Every Agency and Managed Service Provider shall comply with and ensure that every natural or juridical person with whom they do business or enter into contract comply with the following Minimum Cybersecurity Standards and Principles:

(1) To establish control mechanisms to stop internet traffic classified as inappropriate and a security policy to, at a minimum, block pornographic websites, malware, phishing attacks, and other identified threats unless access thereto is required to perform their duty;

(2) To implement layered security controls to further protect the confidentiality, integrity, and availability of information;

(3) To establish policies on the appropriate use of equipment and information systems, strengthen such policy with administrative and technical controls, and implement administrative and technical control mechanisms to access internal and external information networks;

(4) To implement administrative controls that require the use of encryption, based on the best recommendations of the National Institute of Standards and Technology (NIST) to strengthen the confidentiality and integrity of data in transit or at rest. To establish technical mechanisms to strengthen the established policies;

(5) To establish that remote connections to the Government network may only be carried out through a virtual private network (VPN) or any other type of virtual private network contracted by the government for official use only when work-related tasks so require. An agreement shall be entered into for the use of a VPN or any other type of virtual private network contracted or used by the government, which agreement shall include an authorization from the data administrator, as well as a reference to the minimum information protection and management responsibilities and duties.

(6) Any program developed or application used by an Agency, or under a contract with a Managed Service Provider to render online services to citizens or facilitate the internal operations of an Agency shall comply with the Minimum Cybersecurity Standards and Principles prior to its implementation.

(7) Any agency that accepts credit card payments through its website shall comply with the payment card industry's best data security practices and standards (PCI-DSS or better). If the agency lacks its own system, it shall require its payment service provider to furnish third-party compliance reports to determine whether it complies with such standards prior to contracting it.

(8) Agencies shall establish a data classification mechanism based on sensitivity for the government and citizens to ensure the best cybersecurity practices. Multi-factor authentication (MFA) shall be implemented for all users once the data has been classified.

(9) Any contracts entered into with Managed Service Providers shall include measures to safeguard Sensitive Assets. All managed providers shall comply with the Federal Information Security Management Act and keep not less than three (3) years of information. If the information is required for law enforcement purposes, Managed Service Providers should have the capacity to furnish the information digitally within two (2) days after it has been requested.

(10) Managed information technology and communications Service Providers shall share information with and notify PRITS and the contracting Agency, within forty-eight (48) hours, of any cybersecurity incident or potential cybersecurity incident they discover that may place data, software, Firmware, or the confidential services of the Government or any natural or juridical person at Risk.

(11) For any Cybersecurity service contract, the external service provider shall submit monthly cybersecurity status reports to PRISTS regarding its information systems and any Sensitive Assets managed on behalf of the Agency. The reports shall include the following information:

a. The threats detected, the threat actors, and any vulnerabilities.

b. The immediate response and remediation actions.

c. The total number of cybersecurity incidents reported to PRITS through the Cybersecurity Incident Report platform.

d. The Cybersecurity risk assessment performed.

(12) Managed Contracted Service Providers that render Cybersecurity services or whose services require that the sensitive information of citizens be stored in their systems shall hold all valid security certifications required by PRITS at the time the contract is executed. Furthermore, they shall comply with the best cybersecurity certification practices as well as with this Act and all the applicable laws, regulations, and standards.

(13) The Agencies shall install automatic security controls for the detection of unwanted programs (for example, viruses, adware, spyware, malware, Ransomware) and the prevention of intrusion events or activities that can affect information security.

(14) Government Information Technology (IT) systems shall be strictly used for government matters or for the purposes authorized by the Government. Access

to the Government's IT systems shall be granted based on roles and shall only include the information necessary for the person to do their job or duty in accordance with the Principle of Least Privilege.

(15) Information processing facilities and assets (for example, servers, network closets, telephone connections, and printing areas for sensitive or confidential data) shall be located in secure and unmarked areas protected by an appropriate security perimeter and controls to prevent unauthorized access and any damage. As part of a contingency protocol, such areas shall also have a generator to prevent failure in the event of power outages.

(16) Confidential information (for example, IPP, IPS) shall not be left exposed or unprotected under any circumstances. It shall be encrypted in all of its states (i.e., in transit and at rest).

(17) To establish and maintain a Cybersecurity Education Program for its personnel and the citizenry, including the personnel of entities providing services to the Government.

(18) To establish data backup and recovery plans that shall be integrated into the Agency's contingency plan to ensure business continuity. Such plans shall take into account the systems maintained locally and the systems maintained by vendors and third-party cloud service providers.

(19) Any other Cybersecurity standards and principles deemed necessary by PRITS.

Agencies shall consult with PRITS prior to entering into any contract or amending, renewing, or extending a contract with a Managed Service Provider on the minimum Cybersecurity requirements that said provider must meet to comply with the Cybersecurity Standards and Principles.

Any contract entered into with a Managed Service Provider without first consulting with PRITS shall be delivered to PRITS for evaluation and may be

cancelled should PRITS find that it fails to comply with, or cannot be amended to comply with, the Cybersecurity Standards and Principles.

Section 8.- Cyber Incident Review Office

The Cyber Incident Review Office is hereby created within PRITS. It shall be directed by the Chief Information Security Officer.

The Office shall be responsible for:

1. Conducting incident management every time an Incident or Information Security Incident occurs;

2. Defining the processes to comply with the 24/7 Cybersecurity monitoring;

3. Monitoring, identifying, responding, and managing risks and events involving security irregularities, infractions or that compromise information assets, including loss, misuse, and unauthorized access or disclosure.

4. Conducting quarterly assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information and information systems that support the operations and assets of the Agencies;

5. Establishing controls to prevent Cyber Attacks launched from its internal networks to other external information systems;

6. Addressing the adequacy and effectiveness of cybersecurity practices and procedures in the management plans and reports;

7. Supporting Agencies in the investigation, mitigation, and resolution of security incidents, including collaborating with local and federal agencies with jurisdiction over the incident;

8. Reporting to PRITS any cybersecurity incident, intrusion, or threat using the tools provided for such purposes;

9. Developing and promulgating metrics on the attacks suffered and confirmed;

10. Establishing a Ransomware Protocol;

11. Establishing a contingency Protocol;

12. Establishing training requirements for those persons who use an electronic information system;

13. Establishing minimum requirements for system management and use;

14. Establishing penalties for the misuse of information systems;

15. Establishing a program that assigns responsibilities to system users and consequences for failure to meet responsibilities.

Every Agency shall meet the requirements and requests of the Office and shall accept and implement any recommendation or directive notified by the Office.

Every Agency shall be required to report any suspected Security Incident to the Office in order for it, in conjunction with the Agency, to conduct incident management, take measures to isolate the Incident, take action to mitigate the impact of the Incident, participate in the coordination with local and federal agencies with jurisdiction over the Incident, as well as resolve and document the Incident, and identify the lessons learned.

The Office shall prepare a quarterly report to be filed with the House of Representative and the Senate of Puerto Rico, stating the results of its efforts and investigations, which shall be published in the websites of PRITS and the Institute. PRITS shall adopt policies and standards regarding the content and format of these reports.

Section 9.-Duty to Inform and Educate About the Public Policy on Cybersecurity.

PRITS shall establish and maintain a virtual education program to inform and educate the people about Cybersecurity. This program shall include education about technical aspects for the appropriate and secure use of electronic tools that

provide access to public information. The educational material shall contain tools to identify and manage any potential cyberattack, as well as where and when to report said attack. The information and asynchronous virtual education to be provided shall be made available on PRITS website.

In addition, PRITS, in conjunction with the Government Ethics Office shall establish and maintain a continuing education program on the provisions of this Act and the Public Policy on Cybersecurity for Agency Information Officers and employees. As part of said program, Government Information Officers and employees shall be required to complete a continuing education course on Cybersecurity every year. In addition, PRITS may schedule training and preparation exercises, such as the so-called Tabletop Exercises, among others.

Section 10.- Penalties.

If any Agency fails to comply with the provisions of this Act, PRITS may impose on the Agency, upon notice and an opportunity to be heard, a fine of not less than fifty (50) dollars nor more than one hundred (100) dollars per day per Incident, for each day of noncompliance with the Cybersecurity Standards and Principles set forth in Section 6 [sic] of this Act.

If obstruction, negligence, bad faith, recklessness, or willful refusal is shown in the management or reporting of a Cyberattack, PRITS may impose on the Agency, upon notice and an opportunity to be heard, a fine of not less than one thousand (1,000) dollars nor more than five thousand (5,000) dollars for each violation.

If a public employee is found to have engaged in this conduct, PRITS, in conjunction with the Human Resources Administration and Transformation Office (HRATO) and the appropriate appointing authority shall order, upon notice and an opportunity to be heard, that the determination be included in the public employee’s file. If said action results in the public employee’s termination, such

employee shall not be hired by an Agency or government contractor either as an employee, a contractor or a subcontractor, for a period of five (5) years.

If a Managed Service Provider is found to have engaged in this conduct, monetary penalties shall be assessed against said provider up to the contract amount, plus any other established by the contract or for other damages caused including the penalties established in the applicable local and federal laws. In addition, neither the Managed Service Provider nor any other agency substantially composed of the same people may be contracted by an Agency or Government contractor, or as subcontractor for a period of five (5) years.

Any noncompliance with this Act shall entail a reeducation and training program to be coordinated by PRITS in conjunction with the Government Ethics Office.

Section 11.- Budget Appropriation.

The expenses entailed by the application of the provisions of this Act shall be subject to the availability of funds, as certified by the Office of Management and Budget and the Puerto Rico Fiscal Agency and Financial Advisory Authority to the Agencies concerned. Likewise, the funds necessary for its implementation shall be allocated in the corresponding budgets for each fiscal year.

Section 12.-Repealing Clause

Any provision of law or regulation that is inconsistent with the provisions of this Act is hereby repealed to the extent of such inconsistency.

Section 13.-Supremacy Clause.

If any statute, regulation, administrative order, or circular letter in effect is inconsistent with the provisions of this Act, the provisions of this Act and the corresponding amendment or repeal of any inconsistency with this mandate shall prevail, unless it is preempted by or substantially conflicts with a federal law, in which case the provisions of the federal law shall prevail.

Section 14.-Rulemaking.

PRITS is hereby authorized to adopt the necessary regulations or to amend the regulations in effect to enforce the provisions of this Act. The process to adopt these regulations shall be exempt from the provisions of Act No. 38-2017, as amended.

In addition, PRITS shall ensure that the adopted regulations are not more restrictive than those established by the Federal government.

Section 15.- Transition Clause.

The Government shall complete all processes necessary to comply with this Act within six (6) months.

Section 16.- Severability.

If any part of this Act were held to be unconstitutional or invalid by a competent court, the holding to such effect shall not affect, impair, or invalidate the remainder of this Act. The effect of such holding shall be limited solely to the clause, paragraph, article, section, or specific part of the Act held to be unconstitutional or invalid.

Section 17.- Effectiveness.

This Act shall take effect upon its approval.