GOVERNMENT OF PUERTO RICO
OFFICE OF THE INSPECTOR GENERAL OF PUERTO RICO

REGULATION ON SECURITY STANDARDS AND ACCESS TO THE FACILITIES OF THE INSPECTOR GENERAL OF PUERTO RICO

Regulation No. 8

2025

TABLE OF CONTENTS

Government of Puerto Rico
Office of the Inspector General of Puerto Rico
Regulations on Security Standards and Access to the Facilities of the Office of the Inspector General of Puerto Rico

CHAPTER I - GENERAL PROVISIONS

Article 1.1 - Title

This regulation shall be known as the "Regulation on Security Standards and Access to the Facilities of the Office of the Inspector General of Puerto Rico". It may also be cited as the "OIG Security Regulation".

Article 1.2 - Legal Basis

This Regulation is enacted under the powers granted to the Office of the Inspector General of Puerto Rico by Articles 7(o), (n), and 8(a) and (h) of Law 15-2017, as amended, known as the "Inspector General of Puerto Rico Act"; Law 46-2008, known as the "Public Buildings Security Act of the Commonwealth of Puerto Rico"; the Fourth Amendment of the Constitution of the United States of America; and Law 38-2017, as amended, known as the "Uniform Administrative Procedure Act of the Government of Puerto Rico". It is also enacted under the federal Occupational Safety and Health Act of 1970; and Law No. 16 of August 5, 1975, as amended, known as the "Occupational Safety and Health Act".

Article 1.3 - Applicability

This regulation applies to all officials, employees (regardless of status or category), contractors, tenants, and other individuals who visit the facilities of the Office of the Inspector General of Puerto Rico (hereinafter, "OIG" or "Office").

Article 1.4 - Prohibition of Discrimination

The Constitution and laws of the Government of Puerto Rico prohibit discrimination based on age, race, color, creed, religion, gender, sexual orientation, political affiliation, political beliefs, national origin, physical or mental health status or social condition, marital status, physical or mental disability, contagious diseases or acquired immunodeficiency syndrome, income level, or for being perceived as a victim of domestic violence, sexual assault, or stalking, or for filing a complaint or claim, or for being military, ex-military, serving or having served in the United States Armed Forces, or for holding veteran status in the performance of their respective services and obligations under this contract, or for any other discriminatory reason as established in the Constitution of the United States or that of Puerto Rico. The OIG reaffirms this public policy, and all terms used to refer to a person shall be understood to apply to all genders.

Article 1.5 – Purpose, Executive Summary and Cost-Benefit Analysis

This regulation is adopted to establish the security and access standards for the OIG facilities, including the handling of firearms, bladed weapons, objects or substances that could cause bodily harm or property damage, unauthorized animals, explosive materials, hooded individuals, temporary custody of objects, and rules related to the operation of electronic security and surveillance systems (e.g., security cameras and metal detectors). It also establishes controls for accessing recordings from security cameras and addresses the custody, disposal, storage, preservation, and use of such recordings.

The electronic security and surveillance system using cameras is intended to deter criminal acts and serve as a tool to identify individuals who commit crimes against property or persons at the OIG. Through the implementation of the security measures established herein, the OIG seeks to safeguard the safety of employees, officials, contractors, and the general public visiting its facilities, as well as to protect the property and assets of both the OIG and those who visit, while respecting their constitutional rights.

This regulation complies with OSHA requirements, which mandate that employers provide a safe and healthy work environment for all covered workers. Each employer must provide a workplace free of hazards that could cause physical harm to anyone working in or interacting with the facilities.

Nothing in this regulation shall be interpreted as an authorization to restrict the content of legitimate expressions and peaceful demonstrations protected by the Constitutions of the United States and Puerto Rico.

In accordance with the foregoing, the OIG certifies that the approval and implementation of this Regulation do not entail any additional fiscal impact for the OIG, administrative agencies or the general public. The adoption of this Regulation is necessary to provide a safe and healthy work environment and replaces the current regulations in compliance with the review requirement established in Section 2.19 of Law 38-2017, *supra*.

Article 1.6 - Interpretation of Words and Phrases

The words and phrases used in this Regulation shall be interpreted according to their context and common usage, except for those specifically defined later.

Article 1.7 - Relationship with Other Rules and Laws

The provisions of this regulation shall not be interpreted in isolation. They shall be interpreted in conjunction with applicable laws and regulations, including their subsequent amendments, that apply to the OIG. The interpretation process shall consider the nature of the OIG's investigative and auditing functions, confidentiality requirements under collaborative agreements with state and federal law enforcement agencies, and the ministerial duty to ensure the confidentiality of information under special laws governing human resources, social security, private financial data obtained during OIG interventions, among others.

CHAPTER II - DEFINITIONS

Article 2.1 - Definition of Terms

The following terms, words, and phrases used in the context of this regulation shall have the meanings specified below, unless the text provides otherwise or the interpretation is incompatible with the spirit and purpose of the provision. Words used in the present tense include the future; those used in the masculine gender include the feminine and neutral, except where such interpretation would be absurd; the singular includes the plural and vice versa.

1) **Law Enforcement Officer** - A member or officer of the Government of Puerto Rico, the United States of America, or any agency, bureau, department, subdivision, or branch of either government or any municipality in Puerto Rico

whose duties include protecting people and property, maintaining public order and safety, and making arrests. This includes, but is not limited to, members of the Puerto Rico Police, Municipal Police, correctional officers, investigators of the Bureau of Special Investigations, marshals of the Puerto Rico General Court of Justice and federal courts with jurisdiction in Puerto Rico, National Guard, inspectors and agents of the Department of Treasury's Internal Revenue, and rangers of the Department of Natural and Environmental Resources. It also includes agents of the Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Secret Service, Drug Enforcement Administration (DEA), Department of National Security (DNS).

2) **Video Storage** - A physical and/or digital location designated for storing security videos.

3) **Common Areas** - Places within the OIG's physical facilities where there is a lower expectation of privacy. This includes, but is not limited to, the following locations: parking lots, hallways, elevators, stairways, courtyards, entrances and exits, conference rooms, among others. Bathrooms and nursing rooms are expressly excluded from this definition.

4) **Weapon** - Any firearm, knife, or any other type of weapon, regardless of its name. It also includes any sharp, cutting, or blunt object that can be used as an instrument of aggression, capable of inflicting serious bodily harm, including death. It also includes any weapon, regardless of its name, capable of firing

ammunition or munitions by means of an explosion (it excludes work devices such as, but not limited to, nail guns used in construction, when used officially for work, art, or trade purposes). In addition, it includes any shotgun, rifle, or firearm designed to be fired from the shoulder; any weapon, by whatever name known, that is capable of propelling one or more projectiles by the release of gas or a mixture of compressed gases.

Any substance that may be considered dangerous, or that reasonably appears to be dangerous, and is understood to pose a risk to the health, physical integrity, or safety of visitors, contractors, or employees of the OIG. Any actual or perceived object is considered a "firearm" if a reasonable person could believe that the object is what it appears to be. If it does not appear to be a firearm but is in fact a firearm, the object will be considered as such.

5) **Notice** - Written notice posted in common areas designated by the OIG, warning of the existence of security measures and access control to its facilities, using, among other things, security cameras and metal detectors. It also includes any other related notices for general information.
6) **Incident Log** - A physical and/or digital form completed by the Security Officer or designated personnel to record extraordinary events or incidents captured by the electronic security system.
7) **Security Camera** - Technical camera equipment installed in the OIG areas permitted in this Regulation, which captures images that are recorded and can be reproduced in accordance with the provisions of this Regulation.

8) **Security Box** - space reserved for the control and locked storage of firearms surrendered by visitors to the OIG to the Security Officer or designated official.

9) **Suspicious Conduct** - action or omission that gives a prudent and reasonable person grounds or reason to infer that a crime is being or will be committed or that a rule will be violated.

10) **Contractor** - A natural or legal person, their representatives or employees who, through a collaboration agreement, covenant, contract, or legal transaction, whether remunerated or not, undertake to provide a professional or advisory service, which shall be governed by Title III of Law 2-2018, known as the Anti-Corruption Code for the New Puerto Rico, as well as the regulations applicable to government contracting and the standards of conduct of their respective profession, if applicable, as well as miscellaneous services or anything else requested by the OIG.

11) **Metal Detector** - Equipment, machinery, paddle, or instrument used as a security measure for detecting metal objects. It is divided into two types: arc metal detectors and handheld or paddle detectors.

12) **Electronic Devices** - refers to a device or mechanism that uses electronic components to perform a specific function. Without limitation, this definition includes mobile phones, recorders, laptops, tablets, microphones, cameras, and other similar devices.

13) **Employee or Official** - All public employees or officials working in OIG buildings, offices, and facilities.

14) **Constitutionally Protected Expressions** - Any peaceful expression or demonstration that is protected by the right to freedom of expression, in accordance with the Constitution of the Commonwealth of Puerto Rico and the Constitution of the United States of America, as well as the jurisprudential interpretations of this right issued by the Supreme Court of Puerto Rico and the Federal Supreme Court.

15) **Provisional Identification** – Temporary credential, for the purpose of identifying contractors of visitors to OIG facilities, as well as those employees who, at the time of accessing OIG facilities, do not have with them the official identification provided by the OIG.

16) **Inspector General** - A person appointed by the Governor, with the advice and consent of the Senate and the House of Representatives, who is in charge of directing the OIG and supervising its administration and management, as provided for in Article 8 of Law 15-2017, the regulations approved under it, and other applicable regulations.

17) **Firearm Carrying License** - Valid license to legally carry weapons, issued under Law 68-2019, as amended, known as the Puerto Rico Weapons Act of 2020 or similar state or federal legislation on the matter.

18) **X Ray Scanner** – A device with a scanning system capable of detecting the presence of any type of weapon or object that gives the impression of being a weapon, which may include narcotics, explosives, weapons, or substances containing chemical or biological threats, among others.

19) **Acceptable Forms of Identification** - Official physical or digital documents issued by government agencies or any other means of identification with a photo and signature issued by a legitimate public or government authority in Puerto Rico or the United States. In the case of foreign nationals who do not have state or federal identification, identification validly issued by a competent authority that issues identification to validate an individual's identity is required.

20) **Monitor** - Electronic equipment that allows real-time viewing of images captured and recorded by the security camera.

21) **Security Standards** - Security measures adopted by the OIG to ensure the safety of its visitors, contractors, and employees and to protect public property.

22) **Security Officer** - Person who holds such a position or who is designated by the Inspector General to perform surveillance functions for the purpose of protecting and ensuring the safety of OIG employees or officials, contractors, and visitors. In addition, this person is responsible for monitoring movable and immovable property that constitutes public property and the areas adjacent to such property. It also safeguards and operates the metal detector and maintains control over the entry of weapons and mobile phones of people visiting OIG facilities, when applicable. This person must be trained in the use and handling of firearms, in accordance with the laws of Puerto Rico, which shall be certified to the OIG.

23) **Belongings** - Items that the employee, contractor, or visitor bring with them when entering the OIG facilities.

24) **Weapons Log** - A digital and/or physical form to be completed by the Security Officer or person designated by the Inspector General for such purposes and signed by signed by the weapon carrier, where applicable.

25) **Electronic Devices Log** - Digital and/or physical form to be completed by the Security Officer or the person designated by the Inspector General for such purposes and signed and initiated by the weapon carrier, where applicable.

26) **Visitor Log** - Digital and/or physical form to be completed by the visitor or contractor, who may request assistance from personnel designated by the Inspector General for such purposes. This record may include all information necessary to identify the visitor or contractor, including a photo, the reason for the visit, time of entry and time of departure.

27) **Employee Log** - A digital and/or physical form to be completed by any OIG employee who does not have their identification card with them when accessing the facilities.

28) **Regulation** - Refers to the “Regulation on Security Standards and Access to the Facilities of the Office of the Inspector General of Puerto Rico”.

29) **Electronic Security and Surveillance System** - A mechanism that allows certain areas of the OIG's facilities to be monitored through images captured by installed cameras, in order to protect order and ensure the safety of operations, the lives and property of employees, and the public visiting the OIG.

30) **Hazardous Substance** - Substance containing chemical elements or any other toxic material that poses a risk to the health, physical integrity, and/or safety of visitors, contractors, or employees of the OIG.

31) **Access Card** - A card issued by the OIG granting access to designated areas.

32) **Identification Card** - card issued by the OIG containing the photo, name, and position of the employee or official or contractor status or any other authorized person by the OIG.

33) **Video** - digital recording or any other method or format that records the sequence of behavior of employees, contractors, citizens, visitors, or passersby who pass through the areas where security cameras have been installed. The recording will not include audio and will be kept, as a general rule, for a period of one hundred twenty (120) calendar days or for the time authorized by the Inspector General or his or her authorized delegate.

34) **Visitor** – Any person who is not an employee, official, or contractor who visits the OIG's facilities for an official and legitimate purpose, whether individually, collectively, or on behalf of others.

CHAPTER III – SECURITY STANDARDS AND ACCESS CONTROL

Article 3.1 – Powers of the Security Officer

The Security Officer shall perform, among others, the following duties:

a) Monitor the OIG facilities, including surrounding areas.

b) Protect property and ensure the safety of employees, officials, contractors, and visitors at OIG facilities. This also applies when they are on official OIG missions or activities.

c) Conduct regular patrols and inspections of OIG facilities.

d) Prevent and intervene in potential criminal acts or violations within OIG premises.

e) Assist in implementing this Regulation.

f) Report and document any incidents to their supervisor or the appropriate departments.

g) In the event of an incident, coordinate with emergency services and alert the Police or other relevant entities, as applicable, and implement access control measures.

h) Inspect visitor's belongings, attend them, and supervise until they are received by the appropriate personnel.

i) Operate metal detectors and X-ray scanners and manage the control of weapons brought by visitors to OIG facilities.

j) Maintain and safeguard the visitor log. This function may be delegated to other personnel.

k) Conduct civil arrests when warranted, while safeguarding the constitutional rights of the individual subject to the intervention.

l) Enforce security and Access rules and operate security systems, including cameras and detectors.

m) Stay informed about external security situations that may impact OIG operations or personnel.

n) Actively participate in reviewing and implementing emergencies, evacuation, or medical plans and guide staff on compliance.

o) Assist their supervisor in handling domestic violence cases and provide necessary support.

p) Regularly monitor OIG security cameras.

q) Provide support and security for internal processes across all OIG departments.

r) Advise and make recommendations to the Inspector General on security best practices and stay updated on trends, technologies, and mechanisms related to security.

Article 3.2 - Security Standards: In General

1) As part of the minimum-security standards at the OIG, the following are adopted:

a) Carrying weapons of any kind is prohibited, except for law enforcement officers on official duty, authorized employees or officials, and private security officers assigned to the OIG, who must carry them in a holster.

b) Entry of blunt or sharp objects or any item that could be used as a weapon is prohibited. Exceptions include items brought for exhibitions, crafts, awards, work tools, authorized events, walking aids, or medical

devices by any person with an apparent or not apparent disability or wound.

c) Animals are not permitted, except those that are properly trained to serve as guides or service animals for people with visual or hearing impairments or who have a disability that requires it, as well as those that are trained for security purposes, accompanied by a law enforcement officer. The Inspector General may grant other exceptions, based on a case-by-case assessment.

d) Explosive materials or hazardous substances are not permitted. Exceptions to this prohibition are those materials that, due to the nature of the service provided by the government agency, must be handled and stored. However, in these cases, the agency must take all necessary measures for the proper handling of such materials so that they do not endanger the health, physical integrity, or safety of employees, officials, contractors, and visitors.

e) Any person wearing hoods, masks, disguises, or who otherwise has their face covered or concealed are not permitted to enter the OIG facilities. Exceptions to the prohibition established in this subsection are those people wearing hoods, masks, costumes, or otherwise covering or concealing their faces for the purpose of an activity previously authorized by the OIG, such as trade shows or seasonal festivities. In addition, undercover agents or informants of law enforcement agencies

who are required to protect their identity are exempt from this provision. Any facial or body protection used to protect health, as a result of official recommendations in the event of a pandemic or other extraordinary event, is excluded. It is provided that any person wearing any item of clothing or attire motivated by a legitimate religious belief or practice may have access to the OIG's facilities. In the exceptions mentioned in this subsection, people who enter the Office wearing hoods, masks, disguises, or who otherwise have their faces covered or hidden must identify themselves, as established in these Regulations, prior to entering the facilities. For the purposes of this subsection, a practice of dress or personal grooming as a preference or fashion will not be authorized when it consists of having the face concealed or covered.

f) No public demonstrations shall be held on OIG premises, in its reception area, hallways, or common areas. They shall only be permitted in areas adjacent to the OIG that are considered traditional public forums, namely: sidewalks, plazas, parks, among others. The Security Officer or designated person shall ensure the safety of OIG employees, officials, contractors, and visitors. To this end, he or she may coordinate with the Puerto Rico Police on the logistics of such events.

g) All visitors and contractors, except for law enforcement officers performing official duties, shall be subject to a visual inspection and screening of their belongings using detection equipment prior to entering

the OIG facilities. Inspections may be conducted in any building, facility, or annex of the OIG premises.

h) The OIG shall post visible signs displaying these minimum-security standards at all public access entrances to facilitate public awareness. Additionally, a copy of this Regulation shall be made available upon request.

i) Any person identified as carrying any of the prohibited items, weapons, firearms, explosive or dangerous materials, hooded individuals, or animals, as well as anyone who fails to comply with the rules of this Regulation or any other rules of social coexistence, such as order and respect, will be denied entry to the OIG and may be ordered to leave the premises.

j) The Security Officer shall notify the relevant operational area or the employee concerned with the visit about the denial of entry.

Article 3.3 – Access rules for employees or public officials, contractors and visitors

1) Visitor Log

a) Visitors will have access to OIG offices and facilities through the main entrance area of each OIG facility and through areas designated as entrances when the parking lot is used as the main entrance. When Office facilities are located in a building with external security personnel, these personnel may request that contractors and visitors register. In addition,

they will only have access to the Office when the Security Officer or the person authorized by the Inspector General determines.

b) Any person entering the parking lot of the OIG facilities who is not an employee or official must visit the reception desk for identification by the Security Officer. Visitors who are authorized by an official with authority and can be verified by that official are exempt from this process.

c) Any visitor or contractor wishing to physically access the OIG's facilities must present acceptable identification, as defined in this Regulation, and complete the Visitor Log. The Office may implement mechanisms for the pre-registration of contractors or visitors.

d) When a visitor fails to provide acceptable identification, the OIG may deny them access to the facilities until they can prove their identity.

e) All people visiting OIG facilities, including contractors and those providing services or delivering goods, shall sign in and out in the Visitor Log located at the various entrances to OIG facilities. The Visitor Log shall include the person's full name and signature, as well as the reason for their visit and their contact information. Prior to registering, the person shall identify themselves to the Security Officer or to the person designated by the Inspector General for such purposes. In addition, if a temporary badge is issued, the visitor shall wear it for the duration of their stay at the OIG. When a visitor or contractor is meeting with an OIG employee or official, the

Security Officer or the person in charge of registration shall notify the latter of the visitor's or contractor's arrival and escort them to the meeting place.

f) No person in an apparent state of intoxication, whether due to the use of alcohol, drugs, or any other substance of any kind, shall be permitted to enter the OIG facilities. Any person experiencing effects as a result of medication duly prescribed by a physician or authorized person is exempt from this provision.

2) Rules relating to personnel and the registration of employees and officials

a) Employees and officials shall always wear their identification card visibly and carry their access card. Both cards are the exclusive property of the OIG. The obligation to use the cards extends to employees and officials who visit the Office outside their working hours or while on leave, unless they are visiting as visitors and not as employees.

b) The obligation to use the cards extends to employees and officials who visit the Office outside their working areas or while on leave, unless they are on the premises as a visitor and not as an employee.

c) When an employee or official ceases their duties at the OIG, they must return their identification and access cards to the Property Manager or designated person.

d) No employee or contractor may access any of the OIG's areas or offices without an access card or prior authorization from the Security Officer when they do not have an identification card.

e) When an employee or official does not carry their identification card, they shall notify the Security Officer or the designated person and sign the Employee Register. In such cases, they may be provided with temporary identification, which must be worn in a visible place during the working day.

f) When an employee or official loses their identification, they must notify the Human Resources Office so that the established internal procedure can be followed. When the lost identification card cannot be recovered, the employee or official must cover the cost of replacing it. The cost of the new card will be ten dollars ($10.00), payable by money order to the Office of the Inspector General of Puerto Rico.

g) The provision or transfer of the identification or access card to another employee or third party is prohibited.

h) Employees, officials and contractors are prohibited from accessing OIG facilities outside of working hours without proper coordination and authorization from an authorized official.

i) Any employee who remains on OIG premises outside of regular working hours must be authorized by their supervisor and must notify the Security Officer in advance.

j) No employee, official, or contractor of the OIG is authorized to provide access to any visitor without first notifying the Security Officer or the designated official.

k) All employees or officials must present their identification card to those responsible for ensuring the security of the premises where the OIG is located, if any of them are unable to recognize them.

3) Registry of law enforcement officers and exemption

a) Law enforcement officers shall register their entry into OIG facilities in accordance with this Regulation. They must present acceptable identification and state the reason for their visit. The Security Officer shall record the name of the law enforcement officer in the Weapons Registry; however, the bearer shall be exempt from storing the weapon in the safe only when the reason for their visit is an accredited official matter. Otherwise, they shall surrender the weapon in accordance with this Regulation.

4) Registration and deposit of weapons

a) Any visitor or contractor who comes to the OIG facilities and is carrying a weapon must inform the Security Officer or the person designated by the Inspector General. Employees and officials are prohibited from arriving at or entering the OIG facilities carrying a weapon, except for those designated to ensure security and who have the authorization of the Inspector General.

b) The Security Officer will request acceptable identification and a valid firearms license.

c) In addition, the person will be asked to deposit the weapon in an individual safety deposit box provided for this purpose, and you will be given the key or code for that box.

d) In addition to the Visitor Log, the bearer must sign the Weapons Log, in which they shall note their name, the time of delivery, the safe deposit box number, the weapons license number, and the serial number of the weapon.

e) Once the visit is over, the Security Officer will verify the identity of the weapon carrier, give them access to the safe where the weapon was deposited so that they can retrieve it, and request the key to the safe. The person will note in the Weapons Register the time at which they took possession of their weapon again and will sign the document once more.

f) Once the process is complete, the visitor or contractor shall record the time of departure in the Visitor Log. This record may be made at any of the OIG's facilities and annexes.

g) Any person who, while carrying a weapon, fails to comply with the process established in this Regulation for registering said weapon; fails to provide the required documents or has any of these documents expired, shall not have access to the facilities of the OIG, unless

authorized by the Inspector General or his or her authorized representative.

5) Electronic Devices Log

a) Any visitor, employee, or contractor may be asked to hand over their electronic devices to the Security Officer, who will keep them safe during their visit to the OIG. Upon leaving, the visitor will be given back the corresponding devices.

6) Use of parking areas

a) Only vehicles belonging to employees, officials, contractors, and authorized visitors will be permitted in the OIG parking lot.

b) Vehicles must be parked in such a way that they do not obstruct or hinder the flow of traffic or pedestrians.

c) The vehicle must be parked in reverse.

d) Vehicles may not be parked in traffic lanes or in parking spaces other than those assigned.

e) Do not walk on areas or ramps intended for vehicle traffic.

f) Vehicles must drive in accordance with speed limits and never against the direction of traffic.

g) When any activity is carried out, personnel stationed at vehicle entry checkpoints must have the list of authorized persons or vehicles available.

h) All vehicles in the OIG parking lot must comply with Act 22-2000, as

amended, known as the Puerto Rico Vehicle and Traffic Act.

i) The removal of any vehicle that fails to comply with this Regulation may be ordered at the expense of the owner of the removed vehicle.

CHAPTER IV – ELECTRNIC SECURITY AND SURVEILLANCE SYSTEM

Article 4.1 – Electronic Security and Surveillance System

1) An electronic security and surveillance system is established, using security cameras without audio, as a measure to protect employees, officials, contractors, and visitors, as well as public property.
2) Recordings generated by this system will not be used to evaluate employee productivity. However, the images may be accessed by authorized OIG personnel in the course of administrative or criminal investigations, in order to identify conduct that violates any law or regulation, persons who have committed any negligent act or engaged in behavior or activities aimed at committing a crime, even if it does not constitute a crime, against property, facilities, employees, officials, contractors, or visitors.
3) The installation and operation of the electronic security and surveillance system shall cover common or public areas, which shall be carried out at all times safeguarding protected constitutional rights, such as the right to privacy, human dignity, freedom of expression, freedom of association, and equal protection under the law. The common areas monitored by security cameras shall be duly identified and include, but are not limited to, the entrances and exits of all work areas, warehouses, and offices, all corridors

and exits to the outside, reception areas, and all accesses and outdoor premises.

4) The electronic security and surveillance system shall have the capacity to cover, monitor, and record on video the facilities occupied by the OIG, including, but not limited to, courtrooms and entrances to conference rooms, meetings, interviews, and interrogations. The security and surveillance system shall not be used within the spaces designated for interrogation processes, unless authorized for the purpose of preserving testimony or statements provided as part of an intervention or investigation, with the prior consent of the person being interrogated.

5) Security cameras shall not be installed in places where employees, officials, contractors, or visitors have an objective expectation of privacy, such as, but not limited to bathrooms, nursing rooms, offices, cubicles, conference rooms, or personal storage lockers. Hidden security cameras that cannot be detected or identified with the naked eye shall also not be installed. If there is a need to expand or improve security and surveillance, additional cameras may be installed, existing cameras may be replaced or relocated, among other measures, but always in accordance with the constitutional rights and in compliance with this Regulation. Exceptions may be made in cases of surveillance or administrative or criminal investigations that warrant the installation of cameras, following due process of law.

6) Images shall be recorded in video format. When there is information about possible illegal acts or when the situation or circumstances warrant it, the person authorized and designated as custodian of the electronic security and surveillance system may program it so that it can record one or more scenes continuously. When activity is observed that could give rise to the commission of a crime or the reporting of a person, a note shall be made of the observed conduct and the person designated by the Inspector General for this purpose shall be notified of the incident. The OIG may file a complaint with the Puerto Rico Police, or any other relevant entity, if necessary.

7) If deemed necessary, the real-time transmission of data captured by security cameras may be observed continuously by the Security Officer via a monitor, screen, or computer at the reception desk or any other designated location during their regular working hours.

8) Recordings shall not be edited, modified, or altered.

Article 4.2 - Frequency of operation of the electronic security system

1) The electronic security system will operate twenty-four (24) hours a day, seven (7) days a week, throughout the year, subject to any mechanical malfunction that may arise. In the latter case, the known reason for the malfunction or interruption, the duration, and the date and time when the electronic security system was restarted will be documented in the Incident Log. If the malfunction occurs during working hours, the Security Officer or

designated person shall complete this information once they become aware of the situation and are at the OIG facilities. When the malfunction occurs outside of working hours, the incident shall be recorded once the Security Officer or designated person returns to work.

Article 4.3 - Prohibited uses of the electronic security and surveillance system

1) The electronic security and surveillance system using security cameras may not be used for the following activities:
   a) Monitor the productivity, attendance, or efficiency of employees or officials in their areas of work.
   b) Monitoring using hidden security cameras.
   c) Installation of electronic security and surveillance systems specifically designed to discriminate against any person on the basis of age, race, color, creed, religion, gender, sexual orientation, political affiliation, political ideas, national origin, physical or mental health status or social condition, marital status, physical or mental disability, contagious diseases, or acquired immunodeficiency syndrome, income level, for being perceived as a victim of domestic violence, sexual assault, or stalking, for filing a complaint or claim, for being a member or former member of the military, serving or having served in the United States Armed Forces, for being a veteran in the performance of their duties and

obligations, or for any other discriminatory cause, as established in the constitutions of the United States of America and Puerto Rico.

2) Violation of the rules established herein shall be sufficient cause for the imposition of disciplinary measures, in accordance with established regulations.

Article 4.4 - Confidentiality of information obtained from security camera recordings

1) Information obtained from security camera recordings and any device or equipment used as part of the operation of the electronic security and surveillance system is confidential in nature. Consequently, employees, officials, or contractors who perform any function related to security cameras and/or the electronic security and surveillance system are required to handle such information with the strictest confidentiality.

2) Reproduction of security camera recordings shall not be permitted without authorization from the Inspector General or without an order from a competent court. This includes but is not limited to: taking photos or videos of data transmission with any type of electronic device; creating copies; downloading image content; sending image content via text, email, or any other existing method of data exchange, data sharing, or information exchange, among others.

Article 4.5 - Notice regarding the electronic security and surveillance system

1) Visible notices shall be posted in OIG facilities, which shall contain, at a minimum: a notification that the area is being monitored by image without audio, twenty-four (24) hours a day, seven (7) days a week; the purpose of the system; and the availability of a complaint mechanism under this Regulation.

Article 4.6 - Process for documenting in the Incident Log

1) The Security Officer or the person designated for this purpose shall maintain an Incident Log, in chronological order, describing each of the extraordinary events captured by the security cameras, as well as the actions taken in response. In addition, any action taken as a result of a breach of this Regulation and any situation or event affecting the safety of employees, officials, contractors, and visitors, as well as their property or that of the OIG, shall be recorded in this Log. If the incident occurs during working hours, the Security Officer or designated person shall complete this information once they become aware of the situation and are on the OIG premises. However, if the incident occurs outside working hours, it shall be recorded once the Security Officer or designated person returns to work.
2) The Incident Log shall *include, at a* minimum, the following information, as applicable:
   a) Number of the incidente;
   b) name and signature of the person registering the incident;
   c) date and time of the entry in the Incident Log;

d) date and time of the incident;

e) people involved;

f) summary of the incident

g) employee, official or agent of the law that received the notification of the incident;

h) when the Puerto Rico Police or any other law enforcement agency intervened, the complaint number, contact information for the officials who intervened, and a description of the actions taken by the officers shall be included; and

i) any other pertinent information.

3) When the person in charge of the monitors identifies incidents that require special observation and security or that could endanger the life, physical integrity, or safety of employees, officials, contractors, or visitors, they shall record this in the Incident Log. This log shall record the facts related to the event and shall refer to the day, month, year, and time of the recording.

Article 4.7 - Personnel in charge of the electronic security and surveillance system

1) The Security Officer, as well as any personnel authorized by the Inspector General, shall be responsible for the operation, management, and administration of the electronic security and surveillance system. Such personnel shall be trained in the technical use and handling of cameras and monitors and in the legal provisions applicable to the use of this technology.

Both the work of these personnel and the information generated by such work shall be highly confidential, and its use shall be limited to the provisions expressly set forth in this Regulation.

2) Only the Security Officer and personnel authorized by the Inspector General shall have access to security cameras, the recordings they generate, the locations where this equipment and recordings are located (physical or covered by technology), and cyber devices and portals, among others, where such recordings will be stored, safeguarded, or kept. The Information Technology Office personnel designated by the Inspector General shall safeguard the electronic equipment that records and stores the information captured by the security cameras.

3) When security camera operators observe behavior or activity that they believe may be suspicious, in the commission of a crime, or in the accusation of a person, they may zoom in on the activity for as long as it lasts. As soon as activity is observed that it may result in the commission of a crime or the accusation of a person, the operator shall notify their supervisor for immediate intervention. In addition, they shall proceed to document the incident as described in Article 4.6 of this Regulation.

Article 4.8 - Custody, storage, disposal, and preservation of recordings from the electronic security and surveillance system

1) The custody, preservation, and disposal of video recordings shall be the responsibility of the Security Officer or the person designated by the

Inspector General for such purposes. The recordings shall be stored and maintained on the server for a period not exceeding one hundred twenty (120) days. Once the period established herein has elapsed, except for the situations described below, said information shall be deleted.

2) Recordings of situations in which there is information or images that may be used for the investigation of acts directed toward or constituting the commission of a crime may be kept for a period longer than one hundred twenty (120) days. In such scenarios, the recordings shall be stored in a security file designated by the Inspector General for such purposes and shall remain stored until the Inspector General determines that they are no longer useful.

3) In order to maintain optimal system capacity, recordings that have reached the storage period established in this Regulation will be made available, except in cases where the recordings are needed as evidence in a criminal or administrative investigation or in response to an inspection request, in which case they will be retained for as long as necessary to fulfill the objectives of such investigations or requests. When the recording is part of an administrative file, the recordings shall be retained for the period of time that the agency is required to retain the file. Recordings that may be related to or give rise to claims against the OIG or third parties shall be retained for a period of one (1) year or for the statute of limitations period provided for in the current legislation to bring the corresponding action, whichever is

longer. The aforementioned recordings may only be disposed of with the authorization of the Inspector General or his or her authorized delegate.

4) With regard to security camera recordings that may be used in criminal, civil, or internal administrative proceedings, an official record shall be kept detailing the entire process from the acquisition of the digital recording to its final disposal. All recordings or their respective duplicates shall be kept under lock and key or in a safe to ensure their preservation and integrity. In addition, all recordings requested for internal administrative purposes shall be requested using the form provided for that purpose by the person designated by the Inspector General as responsible for the custody and disposal of digital recordings. Likewise, any recording requested for criminal or civil purposes shall be done through a court order or subpoena issued by the state or federal Department of Justice. Any authorized copy of a recording shall be provided by the OIG, upon payment of the corresponding fees established by the Inspector General.

Articl 4.9 - Security rules applicable to computers in the electronic security and surveillance system

1) The equipment, computers, and devices, among others, that make up the electronic security and surveillance system shall comply with the following security standards:

   a) They shall be kept in a place to which only authorized persons have access.

b) They shall have sufficient safeguards and security mechanisms in place to prevent unauthorized people from accessing the information contained in such recordings.

Article 4.10 - Procedure for requesting inspection or copies of recordings from the electronic security and surveillance system

1) The information obtained through the electronic security and surveillance system shall be subject to restrictions on its use. To this end, in accordance with this Regulation, its disclosure shall be controlled, and its retention and storage shall be limited.
2) The Inspector General may authorize the inspection and reproduction of recordings from the electronic security and surveillance system, upon duly substantiated request, by government law enforcement agencies.
3) Any person who requests an inspection or copy of a recording proves that they are an interested party with standing in a civil, criminal, or administrative action may examine or obtain a copy of a recording from the electronic security and surveillance system, subject to authorization by the Inspector General or an order from a competent court.
4) Any person interested in examining a recording or obtaining a copy thereof shall submit a request to the Inspector General, including a certified copy of the court order. The request shall be made in writing, duly substantiated, and shall refer to the action that is the subject of the request. In addition, it

shall detail the applicant's reasons for examining or obtaining a copy of the recording, indicating the time and date on which they wish to visit the OIG.

5) The inspection of the security and surveillance system shall be carried out at the OIG's facilities during working hours. The Security Officer or the person designated by the Inspector General for such purposes shall coordinate the date, time, and place of such process. During the inspection of the recording, the person authorized to examine it and their legal representative, as well as those who have been authorized by court order, may be present. Employees or officials authorized by the Inspector General or his or her authorized delegate shall also be present. When authorization to examine the recording is granted, only the part or parts of the recording that are relevant to the subject matter of the request shall be shown, unless a competent court order provides otherwise.

6) It is stipulated that, in the case of external administrative forums, the agency concerned shall obtain a court order to enable, at the request of a party, access to and inspection of the recording.

7) The inspection process shall be documented in the Incident Log by the designated OIG official, including the following information: names of people present, actions taken, duration, and comments or observations made by the parties or their legal representatives, as well as any other information relevant to the process.

8) The delivery of duplicate recordings to investigative authorities or authorized persons shall be recorded on official receipt issued for such purposes by the Security Officer or the person designated by the Inspector General. The receipt shall include, among other things, a description of the court order, the date and time of delivery, and an acknowledgment of receipt signed by the person to whom it is delivered.

Article 4.11 - Use of recordings in internal administrative proceedings of the OIG

1) During the course of an investigation or administrative proceedings against an employee or official, the following people may have access to this material: the Director of Human Resources, the Associate Inspector of the Legal Affairs Department, the attorneys in charge of the matter, and any other person designated by the Inspector General.
2) If, for reasons related to an internal investigation or administrative process conducted by the OIG, it is necessary to examine or obtain a copy of a video recording, said recording shall be stored separately during the course of the investigation, the administrative proceedings in this or another agency with jurisdiction, or the corresponding judicial proceedings. This material shall be kept in the custody of the Director of Information Technology or the person designated by the Inspector General.

Article 4.12 - Procedure for handling and processing complaints arising as a result of the application of this Regulation

1) Any employee, official, contractor, or visitor may file a complaint regarding the use and management of the electronic security and surveillance system or the application of this Regulation.
2) Complaints shall be submitted directly to the OIG Human Resources Office within a strict period of t (20) days of becoming aware of the incident that gave rise to the complaint. To this end, the petitioner shall submit a written document in physical or digital format, detailing the date and time of the incident, as well as a description of the events that gave rise to the complaint. Petitions or complaints may be submitted via email to the Human Resources Office, in person at that Office, or by certified mail.
3) The complaint will be evaluated by the Legal Affairs Department, which will make a recommendation to the Inspector General or his or her delegate regarding this matter.
4) The Inspector General or the delegated official shall issue a final determination regarding the complaint filed and shall notify the complainant in writing within thirty (30) business days of receipt, through the OIG Human Resources Office. If the complainant's email address is available, this shall be the preferred method of notification. Otherwise, notification will be made by certified mail or hand delivery. The OIG may use more than one method of notification simultaneously, if deemed appropriate. When this occurs, notifications are deemed to have been made on the date recorded in the records of the first notification sent.

CHAPTER V - ACCESS CONTROL THROUGH THE USE OF DEVICES TO DETECT DANGEROUS OBJECTS

Article 5.1 - Use of devices to detect dangerous objects when accessing OIG facilities

1) As part of the measures to ensure the safety of employees, officials, contractors, and visitors, metal detectors, as well as any other electronic device or apparatus deemed necessary, may be installed in their facilities to detect the presence of dangerous items or objects.
2) The number and location of these detection tools shall be determined from time to time by the Security Officer or personnel designated by the Inspector General.
3) When metal detectors are installed in OIG facilities, all visitors shall be subject to both physical inspection and inspection of their belongings. The physical inspection shall not be unreasonably invasive and shall adhere to established legal and judicial protocols. Pregnant people and people with pacemakers or metal prostheses shall be exempt from this regulatory provision but may be physically inspected.
4) The inspection includes all packages, bags, briefcases, electronic devices, or any similar equipment.
5) In cases where the fixed detector is not available or, if available, its alarm is activated, the person in charge of this equipment shall carry out an inspection using the handheld or paddle metal detector. If the person to be

inspected refuses to undergo this inspection or inspection using the metal detector or any other device provided for this purpose, without being exempted under this Regulation, the OIG will deny access to its facilities.

6) When the inspection using the metal detector or any other device detects the existence of any weapon, as defined in this Regulation, the established process for its deposit shall be carried out; otherwise, the carrier of these objects shall be denied access to the OIG.

CHAPTER VI – FINAL PROVISIONS

Article 6.1 – Severability Clause

If any word, clause, article, section, or part of these regulations is declared null and void or unconstitutional by a court with jurisdiction, such determination shall not affect, impair, or invalidate the remaining provisions and parts of these Regulations, but shall be limited to the specific word, clause, article, section, or part declared null and void or unconstitutional. The invalidity or unenforceability of any word, clause, article, section, or part shall not be construed to affect or impair in any way its application or validity in any other case.

Article 6.2 – Interpretation

This Regulation shall be governed by the laws of the Government of Puerto Rico and shall be interpreted in accordance with them. Likewise, in the interpretive function, the sensitive nature of the OIG's statutory mission shall be taken into consideration, as well as the rigor imposed by law or agreements with law

enforcement agencies to protect confidential information, among other provisions of the OIG regulations adopted in accordance with Act 15-2017.

Article 6.3 - Amendments

The provisions of this Regulation may be amended at any time, as required by the operations and needs of the OIG and in accordance with the relevant procedural formalities. In addition, the Inspector General, or the authorized delegate, may issue or adopt any guidelines, circulars, policies, procedures, or internal regulations that are necessary or convenient for the best interpretation or implementation of the provisions of this Regulation.

Article 6.4 - Repeal

This Regulation repeals Regulation No. 9228-2020, known as the Regulation on Security Standards and Access to the Facilities of the Office of the Inspector General of Puerto Rico; Administrative Order No. OIG-OA-2024-014, entitled Rules for Access, Use of Cards, and Visitor Registration at the Office of the Inspector General (OIG), as well as any other internal regulations or forms that contravene the provisions herein.

Article 6.5 - Validity

These Regulations shall take effect thirty (30) days after their filing with the Department of State, in accordance with the provisions of section 2.8 of Law 38-2017.

Article 6.6 - Approval

Approved on ____ of _____, 2025, in San Juan, Puerto Rico.

_____
Ivelisse Torres Rivera
Inspectora General