Office of the Commissioner of Insurance

Compliance Checklist for Rule No. 108, "Cybersecurity Standards for the Insurance Industry"

Learn more about Rule 108 and resources for technology implementation in the insurance industry at https://ciberseguridad.ocs.pr.gov.

Annual Certification of Compliance

No later than June 30 of each year, all Licensees shall submit an annual certification of compliance with the OCS Cybersecurity Portal. This document is a written statement in which the Licensee certifies being in compliance with the requirements set forth in Section 8:

- ☐ **Implementation of a Cybersecurity Program** – This consists of developing, implementing, maintaining, and documenting a comprehensive program to protect the Licensee's data and information systems.
  - ☐ Administrative cybersecurity controls (policies, standards, processes, and plans directed at (a) protecting the confidentiality, integrity, and availability of data; (b) preventing any unauthorized access or use; and (c) defining appropriate retention and destruction periods for nonpublic information.
  - ☐ Technical cybersecurity controls (e.g., firewalls, antivirus, settings, etc.) that will be used to implement the controls set forth in policies, standards, and procedures.
  - ☐ Physical security controls (access controls, security cameras, etc.)

- ☐ **Risk Assessment** – There are several frameworks, methodologies, and tools that may be used to assess your cybersecurity risk, for example, CISA CPGs, CIS Critical Security Controls, and other tools aligned with NIST CSF
  - ☐ Designate individuals to be responsible and accountable for the Cybersecurity Program
  - ☐ Identify internal and external threats.
    - ☐ Assess the likelihood and potential damage of each threat.
  - ☐ Reassess the sufficiency of the Cybersecurity Program and the effectiveness of the implemented controls at least once a year and make the necessary adjustments.

- ☐ **Risk Management** – This consists of the implementation of cybersecurity controls based on your Risk Assessment:
  - ☐ Include measures to mitigate identified risks in your Cybersecurity Program (service contractors must be included):
    - ☐ Implement a formal training program on cyberattack modalities for staff and keep track of each employee's performance.
    - ☐ Assign and train staff on their cybersecurity responsibilities
    - ☐ Establish access controls, including multi-factor authentication, to the extent possible and/or that is appropriate to prevent unauthorized access
    - ☐ Oversee service providers with access to your data through requirements for service agreements and cybersecurity controls.
    - ☐ Identify enterprise information assets and manage them securely
    - ☐ Restrict physical access to areas where Nonpublic Information is located
    - ☐ Implement encryption or other controls to protect data while being transmitted and information stored on portable devices
    - ☐ Adopt secure software development practices and test the security of applications developed in-house and by external resources
    - ☐ Include backup, safeguard, and log management processes (audit logs)
    - ☐ Regularly test and monitor systems and procedures to detect attacks and suspicious activity, including backups, safeguards, and log management (audit logs)
    - ☐ Prevent destruction, loss, or damage due to environmental hazards, natural disasters, or technological failures through a business continuity plan, disaster recovery plan, and cybersecurity incident response plan
    - ☐ Implement and maintain procedures for the secure disposal of data
  - ☐ Stay informed regarding new threats or vulnerabilities for a prompt response with the necessary mitigations

- ☐ Include cybersecurity in your business risk management process and on corporate governance reports.
- ☐ Perform regular vulnerability scans on your information systems

To learn more about the effective implementation of cybersecurity controls, refer to the **Implementation Guide for Cybersecurity Controls for the Insurance Industry**, available on the OCS Cybersecurity webpage: https://ciberseguridad.ocs.pr.gov.

Vulnerability Scanning Results

Licensees must file a self-assessment of their cybersecurity vulnerabilities on a biannual basis. The OCS only requires necessary information to determine whether the Licensee has duly mitigated its external vulnerabilities. To analyze these actions, the OCS uses the following metrics:

- **Number of assets scanned**
  Services and devices that allow or could allow access to a network through an interface, specialized software, IP addresses, or any other means. Some examples include computers, servers, multifunctional devices, etc.
- **Number of services scanned**
  Of all assets scanned, those portals, applications, and executed protocols that provide Internet communication capabilities
- **Number of devices scanned**
  Of all the assets scanned, those devices that have at least one open port or service
- **Number of vulnerable devices**
  Of the devices scanned, those devices where a vulnerability has been detected
- **Number of vulnerabilities**
  Weaknesses in the information system, security process, internal controls, or implementation that a cyber adversary or threat could exploit. The following are analyzed based on severity:
  - **Number of critical vulnerabilities**
  - **Number of high-risk vulnerabilities**
  - **Number of medium-risk vulnerabilities**
  - **Number of low-risk vulnerabilities**
- **Maximum age of active vulnerability**
  Refers to the maximum age, in days, that each vulnerability has remained active.
- **Open services (potentially risky)**
  Of all the services scanned, those particular services that could increase the risk to information systems because of their exposure:
  - **RDP**
  - **SMB**
  - **NetBIOS**
  - **RPC**
  - **SQL**
  - **Telnet**
  - **LDAP**
  - **Kerberos**
  - **FTP**
  - **IRC**

To facilitate the delivery of this requirement, Licensees are advised to enroll in the *Cyber Hygiene Services* that the Cybersecurity and Infrastructure Security Agency (CISA) offers **free of charge** to all types of organizations. The information requested in your vulnerability report appears on page 6 of the *Cyber Hygiene Assessment*, titled "*Cyber Hygiene Report Card*". You may request this service by emailing ngai.oliveras@cisa.dhs.gov. For more information, visit https://ciberseguridad.ocs.pr.gov.

Cybersecurity Incident Notification

If it is necessary to notify the Commissioner of a cybersecurity incident, Licensees may do so through the portal https://ciberseguridad.ocs.pr.gov. In the Licensee section, you will find a notification form with all the information required in Rule No. 108, which must be filed electronically within 72 hours after the time it has been determined that a cybersecurity incident has occurred.

The Licensee must send as much information as possible using the electronic form. The use of an electronic form reduces the security risk by providing a method other than the Licensee's email, which could be compromised. If notification through this form is not feasible, and to send any update or additional information about the incident, Licensees may send an email to ciberseguridad@ocs.pr.gov.