STATEMENT OF AUTHORITY
AND
CONFIDENTIALITY COMMITMENT FROM
THE UNITED STATES FOOD AND DRUG ADMINISTRATION
NOT TO PUBLICLY DISCLOSE NON-PUBLIC INFORMATION SHARED
BY
THE FISH QUARANTINE AND INSPECTION AGENCY OF THE MINISTRY OF MARINE AFFAIRS AND FISHERIES OF THE REPUBLIC OF INDONESIA

The Fish Quarantine and Inspection Agency (FQIA) of the Ministry of Marine Affairs and Fisheries (MMAF) of the Republic of Indonesia is authorized under the Law of the Republic of Indonesia Number 14 Year 2008 on Public Information Openness to disclose non-public information to the United States Food and Drug Administration (FDA) regarding FQIA-regulated products as part of cooperative law enforcement or cooperative regulatory activities.

FDA understands that some of the information it receives from FQIA may include non-public information exempt from public disclosure under the laws and regulations of the Republic of Indonesia which is confidential commercial information; trade secret information; personal privacy information; law enforcement information; designated national security information; or internal, pre-decisional information. FDA understands that this non-public information is shared in confidence and that FQIA considers it critical that FDA maintain the confidentiality of the information. Public disclosure of this information by FDA could seriously jeopardize any further scientific and regulatory interactions between FQIA and FDA. FQIA will advise FDA of the non-public status of the information at the time that the information is shared.

Therefore, FDA certifies that it:

1. has the authority to protect from public disclosure such non-public information provided to FDA in confidence by FQIA;

2. will not publicly disclose such FQIA-provided non-public information without the written authorization of the owner of the information, the written authorization from the individual who is the subject of the personal privacy information, or a written statement from FQIA that the information no longer has non-public status;

3. will inform FQIA promptly of any effort made by judicial or legislative mandate to obtain FQIA-provided non-public information from FDA. If such judicial or legislative mandate orders disclosure of FQIA-provided non-public information, FDA will take all appropriate legal measures in an effort to ensure that the information will be disclosed in a manner that protects the information from public disclosure;

4. will promptly inform FQIA of any changes to the United States of America's laws, or to any relevant policies or procedures, that would affect FDA's ability to honor the commitments in this document;

5. has established and will maintain compliance with current United States federal government National Institute of Standards and Technology (NIST) Risk Management and Cybersecurity Frameworks[1] which are Information Technology security guidelines and standards that focus on protecting information systems and shared sensitive information;

6. will safeguard information systems that contain FQIA-provided non-public information in compliance with current NIST guidelines and standards to ensure confidentiality and integrity. Confidentiality means preventing unauthorized access to and disclosure of non-public information, and integrity means guarding against improper information modification or destruction. Integrity includes ensuring information non-repudiation and authenticity based on the security terms found in this Statement of Authority and Confidentiality Commitment, including means for protecting non-public information;

7. will destroy FQIA-provided non-public information, whether in electronic form or hard copy form, once the information has been utilized and is no longer needed for official purposes in accordance with federal records retention requirements;

8. will restrict access to FQIA-provided non-public information to the employees, and officials of FDA who require access to such non-public information to perform their official duties in accordance with authorized uses of the non-public information unless otherwise authorized in writing by FQIA. FDA will advise all such employees and officials (1) of the non-public nature of the information; and (2) the obligation to keep such information non-public; and

9. in the event of a suspected or confirmed incident or breach[2], including a cybersecurity[3] incident, or any other type of breach, whether it is intentional or inadvertent, FDA will:

---

[1] The National Institute of Standards and Technology (NIST) Risk Management and Cybersecurity Frameworks provide a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle and provides guidance based on standards, guidelines, and practices for organizations to manage and reduce cybersecurity risk, respectively. These frameworks are primarily intended to manage and mitigate cybersecurity risk for critical infrastructure organizations based on standards, guidelines, and practices.

[2] An incident is defined as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the confidentiality of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." Incidents can be events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of confidentiality or integrity, unauthorized disclosure or destruction of information. For the purposes of this agreement, breach is defined as an actual compromise of security that results in the unauthorized disclosure of, loss, accidental or unlawful destruction, alteration, or access to protected data transmitted, stored, or otherwise processed. Breaches can be intentional or inadvertent.

[3] Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

(a) protect all FQIA-provided non-public information, including any non-public information created, stored, or transmitted to avoid a secondary information incident;

(b) report all suspected and confirmed incidents or breaches involving FQIA-provided non-public information in any medium or form, including paper, oral, or electronic, to FQIA as soon as possible and without unreasonable delay, no later than one (1) day of discovery or detection; and

(c) provide to FQIA impact and severity assessments of incidents or breaches, upon occurrence, including a description of the actions taken, including preventative security measures employed to address and remediate the incident.

FQIA and FDA do not intend for this text to create rights and obligations under international or other laws.

Signed on behalf of FDA:

_____/s/_____ ____July 10, 2023_____

Mark Abdoo Date
Associate Commissioner
Office of Global Policy and Strategy

The United States Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
United States of America