Pilgrim House, Old Ford Road
Aberdeen, AB11 5RL
Geoff.Ogle@fss.scot

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

24th July 2025

Dear Mr. Abdoo,

Food Standards Scotland (FSS), a non-ministerial office in the Scottish Administration and the public food safety authority, established by the Food (Scotland) Act 2015, which carries out functions in Scotland to protect the public from risks to health which may arise in connection with food, appreciates that the United States Food and Drug Administration (FDA) is a public health agency that protects the safety of the food supply and consumers. FSS considers cooperation on matters of mutual interest as important and is pleased to facilitate the sharing by FDA of non-public information regarding FDA-regulated products as part of cooperative law enforcement or cooperative regulatory activities.

FSS understands that some of the information it receives from FDA may include non-public information (i.e. data or knowledge not meant for general public dissemination, which encompasses various categories of confidential and sensitive data, including proprietary, confidential, and information protected by law). FSS understands that the FDA may share non-public information which is exempt from public disclosure by the laws and regulations of the United States, and includes confidential commercial information; trade secret information; personal privacy information; law enforcement information; designated national security information; or internal, pre-decisional information with FSS, only insofar as sharing of such information is permitted. FDA considers it critical that FSS maintain the confidentiality of the information. Unauthorised or public disclosure of this information by FSS could seriously jeopardise any further scientific and regulatory interactions between FDA and FSS. FDA will advise FSS of the non-public status of the information at the time that the information is shared.

Therefore, FSS certifies that it:

1. has the authority to protect from public disclosure such non-public information provided to it (including its officials and representatives) by FDA. Should any request for the disclosure of such information be made to FSS under the Freedom of Information (Scotland) Act 2002 or the Environmental Information (Scotland) Regulations 2004, FSS will endeavour to withhold

such information as information through the application of relevant statutory exemptions from disclosure.

2. subject to paragraph 3 below, will not publicly disclose such FDA-provided non-public information without the written authorisation of the owner of the information, the written authorisation from the individual who is the subject of the personal privacy information, or a written statement from FDA that the information no longer has non-public status;

3. will inform FDA promptly of any effort made by judicial or legislative mandate to obtain FDA-provided non-public information from FSS. If such judicial or legislative mandate orders disclosure of FDA-provided non-public information, FSS will take all appropriate legal measures, so far as may be possible within the terms of the order, to disclose information in such a way as to limit its circulation or use and to protect the information from public disclosure.

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

5. has established and will maintain compliance with standards consistent with current United States federal government National Institute of Standards and Technology (NIST) Risk Management and Cybersecurity Frameworks[1] and/or International Organization for Standardization and International Electrotechnical Commission (ISO/IEC)[2] Information Technology security guidelines and standards that focus on protecting information systems and shared sensitive information;

6. will safeguard information systems that contain FDA-provided non-public information consistent with current NIST and/or ISO/IEC 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 FDA-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;

8. will restrict access to FDA-provided non-public information to the employees, and officials of FSS 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

[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] The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) is an international standard that assists organizations in managing the security of their information assets. It provides a management framework for implementing an information security management system to ensure the confidentiality of all corporate data. Foreign counterparts are strongly encouraged to meet the ISO 27001 standard requirements, or the most recent standard, and to be certified by an accredited certification body.

in writing by FDA. FSS 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. will, in the event of a suspected or confirmed incident or breach[3], including a cybersecurity[4] incident, or any other type of breach, whether it is intentional or inadvertent:

(a) protect all FDA-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 FDA-provided non-public information in any medium or form, including paper, oral, or electronic, to FDA as soon as possible and without unreasonable delay, no later than one (1) day of discovery or detection; and

(c) provide to FDA 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.

Final matters

If information shared by FDA is not identified as non-public or confidential at the time it is communicated, FSS will confirm with FDA that the information is not confidential or non-public before wider disclosure or publication at the discretion of FSS.

Any dispute about the interpretation or application of this letter will be resolved by consultations between FSS and the FDA, and will not be referred to any national or international tribunal or third party for settlement.

The contents of this letter are voluntary which creates no legal commitments or obligations on the part of FSS.

Yours sincerely

-/s/- 7/24/25
Date

Geoff Ogle
Chief Executive
Food Standards Scotland

[3] 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.

[4] 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.