U.S. FOOD & DRUG ADMINISTRATION

FDA Management Response: PDUFA VII Cloud Assessment Summary

December 31, 2023

Prologue

Our FDA Office of Digital Transformation (ODT) welcomes the opportunity to share our perspectives regarding the Eagle Hill Independent Cloud Assessment Report to meet the provision of the Prescription Drug User Fee Act (PDUFA) VII agreement that specifies the U.S. Food and Drug Administration's (FDA) commitment to "leverage cloud technology to progress regulatory digital transformation" by assessing "challenges or barriers in FDA's adoption of cloud-based technologies in applicant-regulator interactions."

Contained within this report, you will find documented highlights of several key challenges across areas such as cloud computing, legacy infrastructure, security requirements, and data location issues. However, it important to note the importance of federal IT policy, mandates and safeguards enforced by executive orders and other security requirements. The controls derived from such directives are critical for securing our data and sustaining cyber and IT security compliance. While the report captures the necessity for modernization along with associated challenges and barriers, it not all inclusive of the significant progress FDA has made in leveraging cloud technologies and key modernization projects already underway at FDA in areas such as software-defined networking, and containerization. Enterprise-wide, FDA has had a 38% increase in cloud adoption since 2021, moving from 71 to 115 systems and applications hosted in federally authorized cloud environments.

Further, cybersecurity is among the top priorities of the U.S. Food and Drug Administration (FDA), and we take our responsibility to protect industry and public health information seriously, especially in today's environment of increased cybersecurity threats. The FDA Office of Digital Transformation (ODT) recognizes the risks associated with operating a global information technology enterprise in support of our public health mission and works continuously to collaborate and partner with all our FDA Centers and Offices. Presently, operating, collaborating, and sharing data within commercial versus government authorized cloud environments[1] is wholly separate and distinct given FDA data, as well as industry data and information[2], must be protected from unauthorized disclosure, access, or misuse—whether accidental or intentional—to maintain confidentiality, integrity, and availability in accordance with the Federal Risk and Authorization Management Program (FedRAMP)[3]. The information system security and privacy controls that provide this protection must meet minimum federal requirements with additional risk-based and business-driven control implementation achieved through a defense-in-depth security structure.

Cyber Threat Landscape. FDA remains a prime target for cyber-crime and economic espionage due to trillions of dollars of industry trade secret, company confidential, and other commercial and intellectual property within our IT systems. Nation state intelligence services and transnational criminal organizations are continuously developing advanced technical capabilities to thwart FDA's defenses, whether through cyber means or by taking advantage of trusted insiders. Americans spend 20 cents of

[1] See draft OMB FedRAMP Guidance: *Modernizing the Federal Risk Authorization Management Program (FedRAMP)* https://www.fedramp.gov/2023-10-27-omb-fedramp-memo/. The Office of Management and Budget (OMB) extended the comment period for the Modernizing the Federal Risk and Authorization Management Program (FedRAMP) memo to December 22, 2023. As a result, this memorandum (if/when codified) will update vision, scope, and governance structure for the FedRAMP program that is responsive to developments in Federal cybersecurity and substantial changes to the commercial cloud marketplace.

[2] FDA must adhere to federal standards to identify and categorize data, to include Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information, and Information Systems*, and National Institute of Standards and Technology (NIST) Special Publication 800-60 Rev. 1 (Volume 1, Volume 2), *Guide for Mapping Types of Information and Information Systems to Security Categories*.

[3] The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services. The governing bodies of FedRAMP include the Office of Management and Budget (OMB), US General Services Administration (GSA), US Department of Homeland Security (DHS), US Department of Defense (DoD), National Institutes of Standards & Technology (NIST), and the Federal Chief Information Officers (CIO) Council. Cloud Service Providers (CSPs) who want to offer their Cloud Service Offerings (CSOs) to the US government must demonstrate FedRAMP compliance. FedRAMP uses the NIST Special Publication 800 series and requires cloud service providers to complete an independent security assessment conducted by a third-party assessment organization (3PAO) to ensure that authorizations are compliant with the Federal Information Security Management Act (FISMA).

every dollar on products regulated by the FDA, which has a global mission as it regulates products manufactured in over 136,400 facilities located in more than 150 countries.

The FDA Global IT Enterprise consists of 398 systems/applications (115 systems in the cloud) along with 20 petabytes of data stored and transiting this evolving cyber landscape, while risks to our critical assets, industry trade secrets, and sensitive data remain moderately high. In this environment, the FDA must remain constantly aware of legal, reputational, business, operational, technical, and compliance risks, as well as the impact of a cyber breach, potential loss of IT operations and the congressional and industry scrutiny that would accompany such events. Although the FDA has not experienced a significant cyber-attack or loss of sensitive data in the recent past, the Agency must remain vigilant given the emerging increase in sophisticated malware attacks and advanced persistent threats (APTs). FDA experiences over 9 billion attempts monthly against our IT infrastructure, which represents a 457% increase in cyber threat activity against the FDA as compared to pre-pandemic attempts. This activity includes significant increases in phishing, social engineering, doxing, cyber exploitation attempts, and other nefarious activities by cybercriminals and nation state actors that target individuals, private industry, and government healthcare organizations.

In addition to complying with federal policies, guidance, and requirements, e.g., Federal Risk and Authorization Management Program, (FedRAMP), and Trusted Internet Connection (TIC)[4] and standards to protect FDA systems and data, we have prioritized cybersecurity innovation and modernization to advance the mission and business of the FDA. Non-compliance with security authorizations and federal policies, guidance, and requirements would leave FDA's information systems exposed and vulnerable to increased likelihood of data breaches, phishing, ransomware, and reputational damage; would increase potential financial fraud, information theft or misuse, privilege abuse, unauthorized disclosure by trusted insiders; and would impact the FDA's ability to protect against cyber threats that could expose personnel, critical IT systems, infrastructure, and sensitive information. Increased scrutiny and legal liability from Congress, industry, the Government Accountability Office, and HHS Office of Inspector General would negatively impact our reputation as a global leader and custodian of industry information. Industry partners and public entities would lose confidence in FDA's ability to protect their sensitive data in the event of a cyber breach or data theft.

Specifically, ODT developed the Cybersecurity Modernization Action Plan (CMAP) to strengthen our ability to protect sensitive information, modernize cybersecurity capabilities, and improve situational awareness to decrease overall security risks to the Agency. The CMAP is guiding our collaborative work to enhance the enterprise resulting in specific improvements, including the following: Improved Customer Experience, Increased Performance, Enhanced Visibility and Situational Awareness, Enhanced Threat Protections, and Reduced Latency and Speed to the Cloud. Strengthening FDA's network/cloud environments, identity capabilities, and data protections are critical as the Agency continues to modernize and deploy new digital services and facilitate more seamless data sharing across its global regulatory environment, while at the same time balancing our FDA business and operational needs. Additionally, ODT has developed a Zero Trust Cybersecurity Network Defense Implementation Plan that will serve as our roadmap to effectively transition to a Zero Trust model using an incremental approach to prioritize, initiate, execute, mature, and monitor progress across a multi-year phased approach. We are strengthening FDA's network environment, identity capabilities, and data protections while we continue to modernize and deploy new digital services and facilitate greater ecosystem interactions and data sharing across our global regulatory environment.

[4] The purpose of the Trusted Internet Connections (TIC) initiative is to enhance network security across the Federal Government. Initially, this was done through the consolidation of external connections and the deployment of common tools at these access points. As outlined in OMB Memorandum (M) 19-26: this modernized version of the initiative expands upon the original to drive security standards and leverage advances in technology as agencies adopt mobile and cloud environments. The goal of TIC 3.0 is to secure federal data, networks, and boundaries while providing visibility into agency traffic, including cloud communications. OMB Memorandum 19-26 also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats. In early iterations, the TIC initiative's main goal was to consolidate TIC access points and develop a federal perimeter security baseline to secure the federal network landscape. The TIC 3.0 program expands on the existing foundation by adding new concepts that allow for increased flexibility to federal agencies in their quest for hardening network security or acquiring new technologies.

We are implementing software defined networking, cloud to cloud, secure access service edge, and other technologies that will enhance our FDA IT network and enterprise.

As the nation's regulatory organization for public health, we recognize that CDER and CBER play a critical role in advancing medical innovation based on sound science, data, and patient-centered approaches. Our global public health mission requires using complex and real-time data to identify meaningful patterns, gain new insights, and inform regulatory decision-making. We are working diligently to enable our mission by modernizing our technology, data, and cybersecurity/compliance processes. Specifically, the FDA IT Strategy 2024-2027 outlines the next step in our technological advancement, aligning with our commitment to enhance public health. The strategy focuses on key goals**:** Enhancing Collaboration; Strengthening Infrastructure; Modernizing Services; Sharing Data; Adopting AI and Innovations; and Cultivating Talent and Leadership.

Strengthen IT Infrastructure. FDA will continue to modernize and secure the foundational IT infrastructure for all IT services and solutions. We will proactively provide the ability to adapt to changes in workload demand, detect issues before they impact stakeholders, and quickly resolve technology issues to avoid disruptions to day-to-day operations. Objectives:

- Provide Flexible Infrastructure Offerings: Offer a marketplace with usage-based models for users to identify and implement the infrastructure solutions based on business requirements with an appropriate chargeback model.
- Accelerate Cloud Adoption: Empower users with cloud offerings to meet their mission needs, e.g., scalability and agility. Provide best practice guidance on cloud models, e.g., hybrid and transition strategies based on the unique needs across Centers and Offices.
- Ensure Service Availability: Provide stable access to IT services through proactive, continuous monitoring of IT infrastructure service performance (e.g., Service Level Agreements, Operating Level Agreements) and feedback from FDA users to identify potential problems and implement targeted improvements.

Implement Zero Trust[5] Approach: Establish a comprehensive zero trust and risk-based approach to obtain the optimal maturity level by upgrading, modernizing, and enhancing FDA's security and cyber defenses. In summary, while this report highlights the challenges and barriers FDA encounters in leveraging cloud technology to advance regulatory digital transformation, the progress, strategic intent, modernization efforts, along with the hard work and dedication of our FDA staff cannot be over-stated. We take seriously our commitment to meet the objectives our Prescription Drug User Fee Act (PDUFA) VII agreement and collaboration with industry partners, and we have made substantive advancements toward that end and will continue improvement in our applicant-regulatory interactions.

[5] OMB Memorandum (M) 22-09 *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, this memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. In the current threat environment, the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data. As President Biden stated in EO 14028, "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life." A transition to a "zero trust" approach to security provides a defensible architecture for this new environment. As described in the Department of Defense Zero Trust Reference Architecture,3 "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction."