U.S. FOOD & DRUG ADMINISTRATION

DEC 10 2018

The Honorable Michael C. Burgess, M.D.
Chairman
Subcommittee on Health
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Burgess:

Thank you for providing the Food and Drug Administration (FDA or the Agency) with the opportunity to testify at the June 6, 2018, hearing before the Subcommittee on Health, Committee on Energy and Commerce, entitled "Examining the Reauthorization of the Pandemic and All-Hazards Preparedness Act." This letter is a response for the record to questions posed by the committee.

If you have further questions, please let us know.

Sincerely,

John Martin
Principal Associate Commissioner
for Legislative Affairs

U.S. Food & Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
www.fda.gov

Your questions have been restated in bold below, followed by FDA's responses.

The Honorable Gus M. Bilirakis

1. **Resiliency is vital to preparedness and ultimately response and recovery. The stockpile of drugs, vaccines, and other medical products and supplies, known as the Strategic National Stockpile is critical to our ability to respond and recover from catastrophic events. Reliable storage and delivery of these lifesaving medicines is also important in terms of patient safety and cost.**

   a. **In what way is your agency working with industry to extend shelf life and improve resiliency of the Strategic National Stockpile?**

FDA recognizes the challenges that public health authorities such as CDC face when managing stockpiles of MCMs and is engaged, when appropriate, in various expiration dating activities.

.

One of the most significant ways FDA helps the SNS manage its assets is through the Shelf Life Extension Program (SLEP). Through SLEP, the federal, fee-for-service program managed by the Department of Defense, select products undergo periodic stability testing conducted by FDA, and if appropriate, the products' shelf life can be extended. Through expiration dating extensions, SLEP helps to defer the replacement costs of certain products in the SNS.

FDA has continues developed novel approaches in this space. For example, in 2013, FDA obtained explicit authority in section 564A(b) of the Federal Food, Drug, and Cosmetic Act to extend the expiration dating of eligible FDA-approved MCMs stockpiled for use in CBRN emergencies. In April 2017, FDA announced the availability of a draft guidance for government public health and emergency response stakeholders entitled "Extending Expiration Dates of Doxycycline Tablets and Capsules in Strategic Stockpiles." This document provides guidance to government stakeholders on testing to extend the shelf life of stockpiled doxycycline tablets and capsules for public health emergency preparedness and response purposes for an anthrax emergency under Section 564A(b) of the Federal Food Drug and Cosmetic Act (FD&C Act). Based on this guidance, in August 2018, FDA extended the expiration date of certain lots of doxycycline tablets. And, most recently in October 2018 for the first time under the 564A(b) authority, FDA extended the expiration date of certain lots of ciprofloxacin held in the SNS. The Center for Devices and Radiological Health (CDRH) works with industry and Agency partners to extend the shelf life of stockpiled medical devices.
FDA also has worked with manufacturers of vaccines seeking an extension of the dating period. Reviewers in the Center for Biologics Evaluation and Research (CBER) evaluate information regarding the potency, purity and identity of the product using real time stability data to determine if an extension of the expiration date can be granted.

The manufacturer of approved medical products may extend the products' expiration dates based on acceptable data in accordance with protocols approved in their marketing applications. FDA

encourages medical product manufacturers to submit data in support of longer shelf lives for medical countermeasures (MCMs) stored in the Strategic National Stockpile (SNS); however, the Agency does not have the authority to require drug, biologics, or device manufacturers or sponsors to pursue longer shelf lives for these products.

Through contracts utilized by agencies with procurement authorities, manufacturers can be incentivized to pursue longer shelf lives for their MCMs.

For more information about FDA's expiration dating extension activities, please see FDA's website at:
https://www.fda.gov/EmergencyPreparedness/Counterterrorism/MedicalCountermeasures/MCMLegalRegulatoryandPolicyFramework/ucm411446.htm.

The Honorable Markwayne Mullin

1. **Do you all believe that current law puts some constraints on how BARDA is able to partner new companies and new technologies?**
   a. **Follow up: Can you explain to me the limits of BARDA's authority to work with companies developing non-therapeutic technologies to counter antibiotic and antimicrobial resistance?**
   b. **Follow up: Do you believe giving BARDA the flexibility to work with companies more broadly would be beneficial to BARDA as they work to achieve their mission to counter anti-biotic and antimicrobial resistance?**

Defer to ASPR/BARDA

The Honorable Frank Pallone, Jr.

1. **The FDA previously expressed concerns about the medical countermeasure (MCM) priority review voucher (PRV) that was created as part of the 21st Century Cures Act in 2016. Now that the PRV has been in effect for two years, can the FDA comment on the challenges of this program?**

In an effort to provide uniform guidance on the MCM priority review voucher (PRV) program, on January 19, 2018, FDA announced the availability of a new draft guidance, titled "Material Threat Medical Countermeasure Priority Review Vouchers." In the question and answer format in this guidance, FDA provides details about the Agency's interpretation and implementation of the MCM PRV program. As of July 1, 2018, FDA received two comments from industry on the draft guidance and is considering those comments prior to issuing a final guidance document.

Additionally, on July 13, 2018, FDA approved the first product to be awarded a Material Threat Medical Countermeasure priority review voucher. It is the first drug approved with an indication for treatment of smallpox.

The first material threat MCM PRV was awarded on July 13, 2018. This was the 20th voucher to have been awarded, and to date, 7 have been redeemed for priority reviews.

With only one voucher issued for a product that was far along in its development before the program was established, it remains too soon to say that it has impacted FDA resources or to assess whether the program is incentivizing MCM development.

There is some evidence that the value of priority review vouchers has been impacted by the increasing number of vouchers that have been awarded. For example, see BIOPHARMDIVE article at *http://journals.sagepub.com/doi/10.1177/0098858818789430).*

2. Should the PRV program be made permanent during the reauthorization of PAHPA? Please explain why or why not.

Congress established the material threat MCM PRV program in December 2016 with the intent of incentivizing the development of MCMs. We appreciate and share Congress' interest in finding innovative incentives to spur the development of MCMs. However, it is premature to conclude how expanding the PRV incentive programs to include material threat MCMs has impacted MCM development. When expanding the PRV programs to include material threat PRVs, Congress recognized the that there are resource implications for the FDA in implementing PRV programs, including impacting FDA's ability to meet its commitments to process applications for priority products (including MCMs). Congress also recognized the importance of assessing these programs, imposing a sunset on the material threat MCM PRV program, and requiring a study of the effectiveness to and overall impact of the three FDA PRV programs: the neglected tropical disease PRV program, the rare pediatric disease PRV program and the material threat MCM PRV program. More specifically, the Cures Act required that the GAO study and report back to Congress by 2020 on the effectiveness of the voucher program for MCMs and other priority areas, including the question "whether, and to what extent, the voucher impacted the sponsor's decision to develop the drug." Pub. L. 114-255, Section 3014(c)(1)(B) of the FD&C Act. FDA believes it would be prudent to wait until the GAO study is completed in January 2020 to inform the future of this program.

3. How can drug development tools and the qualification process impact national security?

Developers can submit very sensitive information to FDA, particularly in the process of qualifying an animal model through the Animal Model Qualification Program (AMQP). The AMQP will qualify animal models that are to be used for efficacy testing of medical countermeasures that are being developed under the Animal Rule. Some examples of the potential impact on national security are as follows:

- If a developer submitted the genetic code of a deadly virus in its qualification materials, we would not want to release that information. Some of these viruses, like the one that causes smallpox, could potentially be created from scratch in the lab, so long as the genetic code is known.

- Similarly, we may need to see the details of how anthrax spores were manufactured for an anthrax animal model. This same information could be a roadmap to weaponize the bacteria that causes anthrax.

4. If the agency is given authority to limit disclosures that may have national security implications, how will the FDA work with sponsors and other stakeholders to ensure consistent implementation of this authority?

FDA would work closely with the submitter (including other government agencies, such as NIH, BARDA, and DoD) to determine if there is any information in the submission that, for the purposes of protecting national security, should not be released. FDA would communicate transparency expectations to sponsors up front as they make their submissions, FDA could highlight sensitive subject matter areas as sponsors proceeded from step to step, and would utilize Agency disclosure personnel as needed.

5. HHS has proposed language that would allow for public postings of drug development tool qualification submissions to be modified if there is information that would compromise national security, when and how would the FDA exercise this authority?

In some cases, sponsors would likely identify national security concerns themselves, near the start of the qualification process. In other cases, FDA personnel who work on medical countermeasures might be the ones to identify concerns, particularly if the sponsor was unfamiliar with the public posting process around drug development tools. In either case, FDA would carefully consider relevant facts, including information provided by sponsors, in determining whether any information should be redacted before posting.

6. What actions has FDA taken to address the cybersecurity threats to medical devices?

FDA has been a leader in addressing the need for strengthening medical device cybersecurity. Part of our public health mission is to help ensure that patients have timely access to safe and effective medical devices, and that devices be protected from cybersecurity vulnerabilities that, if exploited, could potentially harm patients.

At the premarket stage, FDA's approach recognizes that, to avert potential risk, cybersecurity needs to be included in product design and development, including capabilities that enable device patching and updating in a timely way. Appropriate threat modeling and premarket testing needs to be conducted to assess the adequacy of security for the device's use environment. In 2014, FDA issued a guidance document, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," to describe the factors in the design and development of medical devices that manufacturers should consider to help to ensure device cybersecurity, maintain device functionality, and reduce potential risk to patients. Once a device is on the market, risk-management planning is essential to manage any risks that might emerge and to reduce the likelihood of future risks. In 2016, FDA issued a guidance document, "Postmarket Management of Cybersecurity in Medical Devices," to emphasize that manufacturers should take a proactive, risk-based approach to cybersecurity throughout a device's life cycle, including a combination of monitoring, maintenance, identification of potential issues, and action to address

cybersecurity vulnerabilities and exploits.

FDA recognizes that a key to the adoption of proactive postmarket cybersecurity is the sharing of cyber risk information and intelligence within the medical device community. FDA routinely collaborates with the Department of Homeland Security (DHS), the central point for cyber threat information sharing into the government, on potential cybersecurity vulnerabilities and exploits that could impact medical devices or the healthcare sector. In addition, FDA has been taking steps towards creation of a collaborative, multi-stakeholder environment that fosters communication about cybersecurity vulnerabilities that may affect the safety, effectiveness, and security of medical devices, or the integrity and security of the surrounding healthcare IT infrastructure. FDA also continues to work with external partners to advance the state of cybersecurity in the medical device ecosystem through several initiatives, including supporting the establishment of additional medical device vulnerability Information Sharing Analysis Organizations (ISAOs).

Because cybersecurity is rapidly evolving, we recognize the importance of adapting our thinking to meet the emerging threats and vulnerabilities of medical device concerns that challenge the healthcare ecosystem. We therefore are continually looking for ways to improve our cybersecurity activities.

7. **What actions does FDA plan to take in the future to help industry prepare and respond to cybersecurity threats?**

We are planning several actions to help industry and the broader device community better prepare and respond to cybersecurity threats. We plan to update our premarket guidance on medical device cybersecurity to better protect against moderate risks (such as ransomware campaigns that could disrupt clinical operations and delay patient care) and major risks (such as exploiting a vulnerability that enables a remote, multi-patient, catastrophic attack). Our Medical Device Safety Action Plan, which we published in April 2018, outlines these and other actions we plan to take to help combat cybersecurity threats.

8. **Under the proposed bill, H.R. _, .the Pandemic and All-Hazards Preparedness Reauthorization Act of 2018, FDA's emergency use authorities (EUA) and the definitions of "eligible product" and "qualified pandemic or epidemic product" would be modified. How would extending FDA's EUA be beneficial? What challenges may result from this expanded authority?**

The proposal to incorporate cyberthreats into the PAHPA context, including the EUA authorities, raises many novel questions and considerations. FDA is committed to addressing cyberthreats and is considering the implications of this proposal. As discussed in response to questions 6 and 7, FDA is committed to improving our capabilities to prepare for and respond to cybersecurity threats, including working with Congress on these important issues.

9. **Please provide an example of how the FDA may issue an EUA related to a cybersecurity threat or how a medical product could be developed with cybersecurity threats in**

mind?

In situations where cyber exploits disable all units of a device (regardless of manufacturer), public health would be at risk if there are no alternative products available. In such cases, FDA could envision authorizing (via EUA) the use of uncleared or unapproved devices. While extending FDA's EUA authority to cover cyber threats could provide FDA with the flexible tools we have successfully used to protect public health in response to other threat types (i.e., CBRN threats), more thought may be needed to consider how the existing authorities could be applied to this type of threat.

Medical products can be developed with cybersecurity threats in mind by building cybersecurity considerations into the design of the device. Building capability into a device for it to be updated and patched is one way to address cybersecurity. Another is ensuring devices are accompanied by a Software Bill of Materials (SBOM) that details the software components of a device so users know if their device may be subject to a cybersecurity threat or exploit. FDA is exploring ways to address these considerations. Our recently-published Medical Device Safety Action Plan contains more information about these efforts.

10. Please comment on FDA's implementation efforts of H.R. 4374, To amend the Federal Food, Drug, and Cosmetic Act to authorize additional emergency uses for medical products to reduce deaths and severity of injuries caused by agents of war, and for other purposes and any resources the Department of Defense has expended in the implementation of this legislation.

FDA takes very seriously our role in ensuring the well-being of the warfighter. We continue to be responsive and work collaboratively to address DoD's priorities. We meet regularly with DoD's MCM enterprise experts—in collaborative informal subject matter expert (SME)-to-SME meetings, as well as in more formal leadership-level meetings. After passage of H.R. 4374, FDA and DoD jointly announced a pilot program to better understand the military's medical needs; give the highest level of attention to and expedite the review of priority DoD medical products, treating those products as if they had breakthrough therapy designation. DOD and FDA signed an MOU on November 2, 2018, setting the foundation for these collaborations.

More specifically, DoD's highest priority has been to provide efficient access to a freeze-dried plasma product (FDP) to control hemorrhage from battlefield trauma. In July 2018, FDA issued an Emergency Use Authorization (EUA) for an FDP manufactured in France for the treatment of U.S. military personnel for the treatment of hemorrhage or coagulopathy during an emergency involving agents of military combat (e.g., firearms, projectiles, and explosive devices) when plasma is not available for use or when the use of plasma is not practical. The FDA issued this EUA in response to a request from DoD and after receiving the required determination by DoD and a declaration by the Secretary of the Department of Health and Human Services. This action was the result of the close collaboration between the FDA and the DoD to prioritize the efficient development of safe and effective medical products intended to help save the lives of American military personnel.

In addition, In August 2018, FDA approved the antimalarial drug, tafenoquine, which was a high priority for DoD.

FDA is providing its highest level of attention to help expedite the development and review of DoD priority products. FDA is also providing ongoing technical advice to DoD to aid in the rapid development and manufacture of medical products for the military. We have also successfully collaborated on:

- the conduct of minimal risk research;
- development of products in the chemical defense portfolio, including approval of a new auto-injector for MCMs for nerve agent exposure for warfighter and civilian uses and continued efforts to make available auto-injector products through shelf life extensions; and
- development of diagnostic devices, including marketing authorization of the BioFire Defense FilmArray NGDS Warrior Panel that includes detection of several biothreat agents and in vitro diagnostic (IVD) approvals.