Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE NATIONAL INSTITUTES OF HEALTH COULD IMPROVE ITS MONITORING TO ENSURE THAT AN AWARDEE OF THE *ALL OF US* RESEARCH PROGRAM HAD ADEQUATE CYBERSECURITY CONTROLS TO PROTECT PARTICIPANTS' SENSITIVE DATA

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

June 2019
A-18-17-09304

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: June 2019
Report No. A-18-17-09304

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

The National Institutes of Health Could Improve Its Monitoring To Ensure That an Awardee of the *All of Us* Research Program Had Adequate Cybersecurity Controls To Protect Participants' Sensitive Data

Why OIG Did This Review

The *All of Us* Research Program (*All of Us*) is a major component of the Precision Medicine Initiative. *All of Us* is responsible for building a national research cohort of more than 1 million participants who will provide their personal health information to the National Institutes of Health (NIH) so researchers, providers, and patients can work together. Ensuring that participant data are securely maintained is paramount to retaining the participants' trust and participation in *All of Us*.

Our objective was to determine whether NIH ensured that two awardees that provide support for *All of Us* had adequate controls to protect participants' sensitive data.

How OIG Did This Review

We reviewed information system general controls at two of the seven components of the *All of Us* program: the Participant Technology Systems Center (PTSC), awarded to Vibrent Health, and the Data and Research Center, awarded to Vanderbilt University Medical Center. These controls included security plans, access controls, information protection and system maintenance, audit logging, data and physical security, incident response, and disaster recovery. To accomplish our objective, we used appropriate procedures from applicable Federal requirements and guidance.

What OIG Found

The PTSC did not have adequate controls to protect *All of Us* participants' sensitive data. NIH did not adequately monitor the PTSC to ensure that the PTSC had implemented adequate cybersecurity controls to protect the participants' sensitive data. Based on the results of our penetration testing at the PTSC, we identified vulnerabilities that could expose personally identifiable information, including personal health information of the *All of Us* participants, and allow access to their data. These vulnerabilities could have allowed an attacker with limited technical knowledge to exploit and compromise the PTSC's systems, as most of the vulnerabilities did not require significant technical knowledge to exploit. In addition, the PTSC failed to enable encryption in the S3 buckets used for cloud storage. The PTSC did not have policies and procedures to address remediating source code vulnerabilities and timely disabling of network access. Finally, the PTSC did not adequately scan its network.

During the audit, NIH and the PTSC addressed and remediated all of the vulnerabilities we identified.

We did not identify any general control vulnerabilities at the Data and Research Center.

What OIG Recommends and NIH Comments

We recommend that NIH revise its *All of Us* Cooperative Agreements and cooperative agreements with security and privacy requirements to include a detailed description of how NIH will monitor cybersecurity and ensure that future awardees adequately implement security controls to protect sensitive data.

In written comments on our draft report, NIH requested that we revise our recommendation to limit the scope of applicability to "appropriately focus on those cooperative agreement awards with security and privacy requirements," which we have done. NIH stated that, based on our recommendation, it is reviewing *All of Us* Research Program awards. Specifically, NIH stated that it will make necessary updates to security and privacy terms and conditions.

TABLE OF CONTENTS

APPENDICES

INTRODUCTION

WHY WE DID THIS REVIEW

Data management, use, and security are essential to the effective and efficient operations of the National Institutes of Health's (NIH) programs. As it works to implement the Precision Medicine Initiative (PMI), NIH can expect to accumulate an increasing volume of sensitive data, such as personal health information. Specifically, the *All of Us* Research Program (*All of Us*), a major component of the PMI, is building a national research cohort of more than 1 million participants who will provide their personal health information to NIH so that researchers, providers, and patients can work together. Ensuring that participant data are securely maintained is paramount to retaining the participants' trust and participation in *All of Us*.

OBJECTIVE

Our objective was to determine whether NIH ensured that two awardees that provide support for *All of Us* had adequate controls to protect participants' sensitive data.

BACKGROUND

Precision Medicine Initiative

In his January 2015 State of the Union address, President Obama announced the PMI as a bold research effort to revolutionize how we improve health and treat disease. The ultimate goal of the PMI is to transform disease prevention and medical treatment so that they can be tailored to each patient by taking into account individual variability in genes, environment, and lifestyle.

The PMI launched in fiscal year 2016, when $200 million was allocated to NIH: $130 million to build the *All of Us* Research Program and $70 million for NIH's National Cancer Institute to lead efforts in cancer genomics. As of April 2, 2019, more than 209,000 individuals had registered for *All of Us*, and of those, more than 126,000 had completed all steps in the protocol to contribute their data.[1]

Privacy and Security of Data in the Precision Medicine Initiative

In March 2015, to ensure that privacy was built into the PMI, the White House convened an interagency working group to develop the *Precision Medicine Initiative: Privacy and Trust Principles* (Principles). The Principles provided broad guidance for future PMI activities in the areas of governance; transparency; participant empowerment; respect for participant preferences; data sharing, access, and use; and data quality and integrity. The interagency

[1] There are four levels of participation: Interested, Registered, Consented, and Participant. A Participant is an individual who has completed all steps in the initial protocol to contribute their data.

working group was co-led by the White House Office of Science and Technology Policy, the Department of Health and Human Services (HHS) Office for Civil Rights, and NIH.

The interagency working group took steps to build security practices into the PMI to ensure the confidentiality and integrity of all PMI data and created the *Precision Medicine Initiative: Data Security Policy Principles and Framework* (Security Framework). The Security Framework recognizes that there is no "one size fits all" approach to managing data security and provides a system for protecting participants' data and resources of organizations conducting and participating in precision medicine activities. In addition, the Security Framework states that PMI organizations will comply with all applicable laws and regulations governing privacy, security, and the protection of PMI data at every stage of data collection, storage, analysis, maintenance, use exchange, and dissemination. The Security Framework was developed through a collaborative interagency process with input from the above-mentioned interagency working group and several other Federal departments and agencies, including the National Institute of Standards and Technology (NIST), the National Security Council, and the Department of Defense.

All of Us **Research Program**

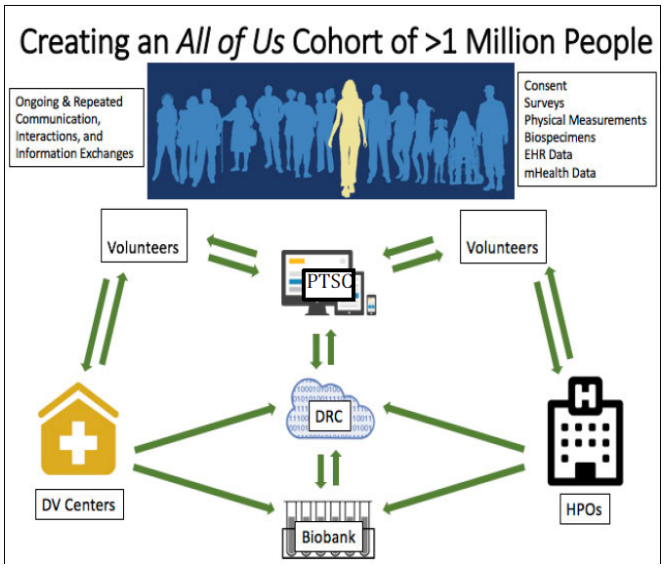
By combining health-related information from 1 million or more diverse participants, *All of Us* will have the scale and inclusive scope to enable research on a wide range of diseases, both common and rare. "A cohort of this size will have the statistical power to detect associations between genetic and environmental exposure and a wide variety of health outcomes."[2] Through cooperative agreements,[3] NIH established four components of *All of Us*: the Biobank, the Data and Research Center (DRC), the Participant Technology Systems Center (PTSC), and the Participant Center.[4] We reviewed cooperative agreements involving two of the components—the DRC and the PTSC. Figure 1 shows the information flow among the seven components.

[2] *All of Us Research Program, Operation Protocol,* p. 5.

[3] NIH uses multiple types of research instruments to support an awardee carrying out a project's activities: grants, cooperative agreements, contracts, and other transaction authority. For more information on *All of Us* awards, please see https://allofus.nih.gov/funding/awardees. For specific components of *All of Us*, NIH used cooperative agreements. NIH frequently uses cooperative agreements for high-priority research that requires a level of involvement from NIH staff that is higher than a typical research grant. This involvement is usually needed for oversight, coordination, or facilitation, but NIH is not meant to play a dominant role or assume direction or primary responsibility for awardee activities.

[4] *All of Us* also awarded cooperative agreements to four Healthcare Provider Organizations in July 2016. In November 2017, under a limited competition, these awardees competed for and received Other Transaction Authority Awards (https://allofus.nih.gov/sites/default/files/hpo_2018_ot_final.pdf). Upon receipt of the award, the Cooperative Agreements were terminated.

Figure 1: *All of Us* Research Program Protocol Figure for Participant Flow



Participant Technology Systems Center

Vibrent Health (Vibrent), located in Fairfax, Virginia, was selected to develop and manage the PTSC. The PTSC develops mobile applications and websites for participants to enroll in *All of Us*, provide data, and receive updates. The PTSC also supports ongoing testing and upgrades to improve the user experience, implements innovative participant tools, and ensures the security of these participant-facing systems.

Data and Research Center

Vanderbilt University Medical Center (Vanderbilt), located in Nashville, Tennessee, was selected to develop and manage the DRC. The DRC acquires, organizes, and provides secure access to what will be one of the world's largest and most diverse datasets for precision medicine research. The DRC will also provide support for a platform through which individuals may access and analyze *All of Us* data. These individuals may be researchers at community colleges to top healthcare research institutions and industries and may include citizen scientists. Individuals approved for use of *All of Us* scientific resources are issued data passports, meaning the user, rather than the proposal, is approved by the program. Research aims are not approved. Rather, once a user is granted access, the user may access any number of workspaces without advance review, so long as the projects housed in those workspaces are described in the public-facing workspace profile. Workspaces and project descriptions may be reviewed as part of periodic NIH audit procedures.

How Participants Enroll and Submit Data in the *All of Us* Research Program

All eligible individuals living in the United States may join *All of Us*.[5] Participants are asked to contribute information about their medical history and lifestyle. Participants will have access to their study results, along with summarized data from across the components of *All of Us*.

Participants can enroll and submit their data (1) at a participating HPO[6] or (2) as a direct participant. HPOs assist interested parties with using the research program website or mobile application. Both HPO assisted participants and direct participants rely on a smartphone application or the *All of Us* website,[7] which the PTSC developed to enroll participants. All participants must complete an informed consent process prior to submitting their personal data, which include questionnaires and surveys, electronic health records (EHR), physical measurements and biospecimens, and passive mobile and digital health data.[8] After HPO-assisted participants give consent, they can share their EHR data directly with the DRC. Through a pilot program, direct participants can share their EHR data via Sync for Science (S4S) technology[9] or similar technology from other vendors at S4S-enabled participant sites. Figure 2 on the following page provides an overview of the flow of information when a participant enrolls in *All of Us*.

[5] At this time, eligibility is contingent on age of consent in the relevant locality, capacity to provide consent, ability to make a unique mark to signify consent, and ability to participate in the program in either English or Spanish. Furthermore, *All of Us* cannot enroll individuals who are incarcerated and cannot allow for the continued participation of participants who become incarcerated, though these individuals may enroll or reactivate their participant status once they are no longer incarcerated. These criteria are subject to change as the program develops the appropriate policies and infrastructure to support more inclusive enrollment and participation.

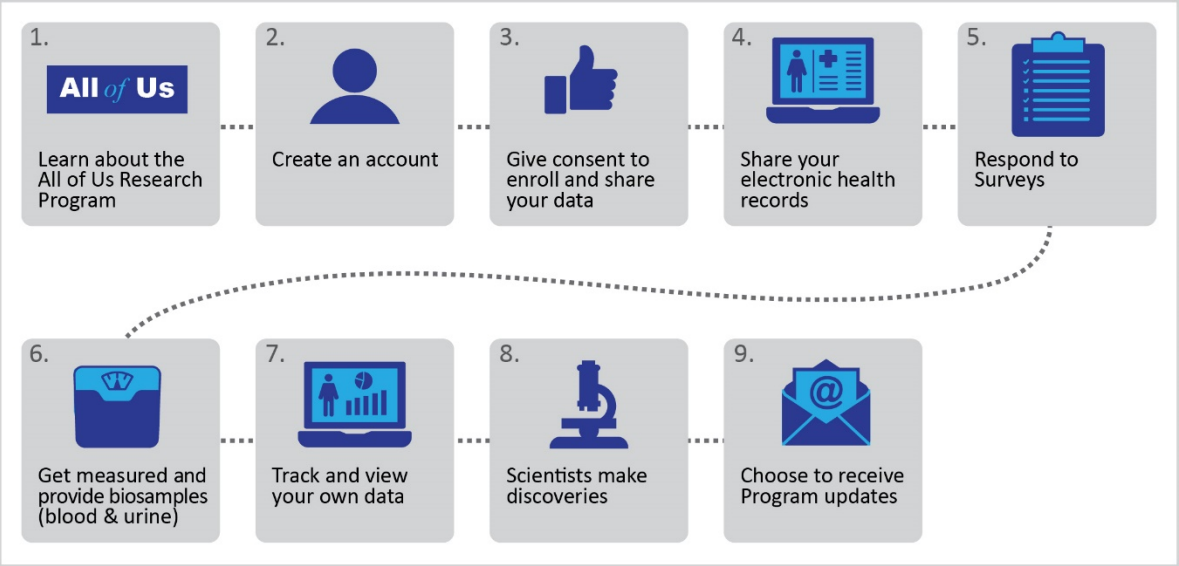
[6] The HPO network includes regional medical centers, community health centers, and medical centers operated by the U.S. Department of Veterans Affairs.

[7] The website is compatible with major browsers, and the smartphone application is available free of charge for the Apple operating system within the Apple App Store and for the Android operating system on the Google Play marketplace. Before downloading, individuals may review a high-level description of *All of Us* posted on the Apple App Store and Google Play marketplace. After downloading, individuals can review educational content about *All of Us* within the mobile application. Available at https://www.joinallofus.org/en.

[8] Additional data may eventually be collected from a subset of participants to be determined, through health, wellness, and fitness devices (e.g. Fitbit), other sensors, or mobile applications.

[9] S4S is a national collaboration among electronic health record vendors, NIH, the Office of the National Coordinator for Health IT, and Harvard Medical School's Department of Biomedical Informatics. (http://syncfor.science/)

Figure 2: Overview of *All of Us* Participant Journey



NIH Cooperative Agreement

The Notice of Award Cooperative Agreement (Cooperative Agreement) between NIH and the PTSC dated May 27, 2017, included a special award condition that the PTSC comply with both the Principles and the Security Framework, plus any additional security policies established during the project period. In addition, the Cooperative Agreement states that the principal investigator (PI) from the awardee has primary responsibility for "adhering to physical, technical, and policy safeguards for data that will ensure state-of-the-art security for all *All of Us* Research Program data and systems." The Cooperative Agreement between NIH and Vanderbilt includes the same special award condition and similar language about PI responsibilities.

Federal Requirements and Guidance

All of Us awardees, such as the PTSC and the DRC, are required to follow the Principles and the Security Framework. The Security Framework is based on the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1. In addition, we used for guidance NIST Special Publication (SP) 800-30, Revision 1, *Guide for Conducting Risk Assessments*; NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST SP 800-115, section 3.4, *Technical Guide to Information Security Testing and Assessment;* NIST SP 800-95, *Guide to Secure Web Services;* NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers;* NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management;* and NIST SP 800-163, *Vetting the Security of Mobile Applications*.

HOW WE CONDUCTED THIS REVIEW

We reviewed the information system general controls related to the PTSC and DRC at Vibrent and Vanderbilt respectively. We began our fieldwork at Vibrent in Fairfax, Virginia, in August 2017 and at Vanderbilt in Nashville, Tennessee, in February 2018. Our fieldwork concluded in February 2019. We reviewed general controls including security plans, access controls, information protections and system maintenance, audit logging, data and physical security, incident response, and disaster recovery. To accomplish our objective, we used appropriate procedures from applicable Federal requirements and guidance. At both Vibrent and Vanderbilt, we reviewed policies and procedures, interviewed staff, and reviewed supporting documentation. We also conducted penetration tests[10] on Vibrent's internal and external networks and on the mobile applications used to enroll participants in *All of Us*. We shared with NIH and Vibrent information about our preliminary findings before issuing this draft report. We chose not to perform penetration testing of the DRC because doing so could affect the integrity or availability of the DRC (*All of Us*) database.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology. Appendix B contains specific Federal requirements and guidance.

FINDINGS

The PTSC did not have adequate controls to protect *All of Us* Research Program participants' sensitive data. Through our penetration testing at Vibrent,[11] we identified vulnerabilities that could have exposed the *All of Us* participants' PII, including their personal health information, and allowed unauthorized users to alter the participants' data. These vulnerabilities could have allowed an attacker with limited technical knowledge to exploit and compromise the PTSC's systems, as most of the vulnerabilities did not require significant technical knowledge to exploit. These vulnerabilities were not discovered before our penetration testing because NIH did not adequately monitor the PTSC to ensure that it had implemented adequate cybersecurity controls to protect the participants' sensitive data.

[10] These tests were performed by contracted security assessors using methods and tools commonly used by attackers to circumvent the security features of an application, system, or network. Such methods included network reconnaissance, vulnerability scanning, and attempts to obtain administrator credentials and to access sensitive data, such as *All of Us* participants' personally identifiable information (PII). PTSC provided the security assessors access behind firewalls and layered defenses based on "greybox" testing protocols.

[11] We have provided detailed results of our penetration tests to officials at NIH and Vibrent.

In addition, we identified several other issues at the PTSC that could affect the security of sensitive participant data. The PTSC failed to enable encryption in the S3 buckets.[12] In addition, the PTSC did not have policies and procedures to address remediating source code vulnerabilities and timely disabling of network access. Finally, the PTSC did not adequately scan its network.

We did not identify information system general control vulnerabilities at the DRC; we attribute this to Vanderbilt's routine assessments and monitoring of DRC security controls.

During the audit, NIH provided documentation to us supporting that all vulnerabilities we identified at the PTSC had been addressed, remediated, and closed according to NIH policy. We reviewed and verified the supporting documentation NIH provided and agreed that the PTSC had remediated the vulnerabilities we identified. Accordingly, we did not include recommendations to address those vulnerabilities in our report.

THE PARTICIPANT TECHNOLOGY SYSTEMS CENTER'S CONTROLS TO PREVENT CYBER-ATTACKS COULD BE IMPROVED

We determined, based on our penetration tests performed at the PTSC, that the PTSC had some controls that were effective at preventing or detecting cyber-attacks. For example, the web application firewall deployed by the PTSC helped to delay and prevent basic automated attacks on its system, and the network was adequately segmented to limit unauthorized movement within parts of the network. However, we identified 13 vulnerabilities, of which 2 were classified as "High," 10 as "Medium," and 1 as "Low."[13] Many of the vulnerabilities were a result of server misconfigurations and design oversights when building the web application. Because of the nature of the vulnerabilities identified, an attacker with limited technical knowledge could exploit and compromise the PTSC's systems, as most of the vulnerabilities did not require significant technical knowledge to exploit. Overall, the tests resulted in access to critical and moderate systems and the potential to access sensitive data or negatively affect systems (e.g. SQL injection[14] or man-in-the-middle attacks[15]). Without effective controls, the

[12] The PTSC utilized Amazon Web Services (AWS) S3 buckets as cloud storage, where data can be uploaded and stored securely in virtual storage locations.

[13] Vulnerability classifications: High – access to critical system(s) or sensitive data such as PII or protected health information; Medium – access to critical/moderate system(s) and the potential to access sensitive data or affect systems negatively; Low – access to system(s) but no access to data.

[14] SQL injection is a computer attack in which malicious code is embedded in a poorly designed application and then passed to the backend database.

[15] A man-in-the-middle attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party.

PTSC's systems could expose *All of Us* participants' PII and allow access to alter or delete participants' data.

THE PARTICIPANT TECHNOLOGY SYSTEMS CENTER'S PRIVATE CLOUD STORAGE WAS NOT ENCRYPTED

We found that none of the PTSC's 22 private S3 buckets[16] in the AWS cloud were encrypted. PTSC officials were not aware that encryption was turned off on the buckets until we requested that they show us that the buckets were encrypted. PTSC officials immediately called an AWS representative; however, the representative could not explain how this had occurred. Soon after the phone call, a PTSC official enabled encryption on the buckets. The S3 buckets contained sensitive information such as configuration settings, web application logs, Virtual Private Network logs, and Virtual Private Cloud logs and could provide an attacker with enough information to attack the rest of the system. By not encrypting sensitive data in its S3 buckets, the PTSC could have allowed unauthorized users access to its sensitive data.

THE PARTICIPANT TECHNOLOGY SYSTEMS CENTER LACKED POLICIES AND PROCEDURES FOR REMEDIATING SOURCE CODE VULNERABILITIES AND REMOVING USER ACCOUNTS

We determined that the PTSC had not developed and implemented formal written policies and procedures for (1) remediating source code vulnerabilities that the PTSC had identified and (2) removing (disabling) user accounts of terminated or transferred employees within a specific time period. PTSC officials stated that their focus was on functionality to meet operating deadlines related to launching the *All of Us* program and not on completing some policies and procedures. Without having formal policies and procedures for remediating coding errors, the PTSC could not ensure that any coding vulnerabilities it discovered were adequately and consistently remediated to protect participants' PII. Without policies and procedures requiring the user accounts of all terminated or transferred employees to be disabled in a specified time period, unauthorized users may be able to use those accounts to log into a system, access sensitive data, and make undetected changes or deletions for malicious purposes or personal gain.

THE PARTICIPANT TECHNOLOGY SYSTEMS CENTER DID NOT ADEQUATELY SCAN ITS NETWORK

The PTSC conducted its vulnerability scans using general compliance checks and not Federal compliance checks that look for specific Federal Information Security Modernization Act (FISMA) requirements. PTSC officials informed us that NIH did not initially provide the PTSC with specific requirements for conducting its network vulnerability scans. However, while we were onsite, PTSC officials informed us that NIH had instructed the PTSC to start scanning using Federal compliance checks. Without using Federal compliance checks for its network scanning,

[16] An Amazon S3 bucket is a public cloud storage resource available in AWS's Simple Storage Service (S3). Amazon S3 buckets, which are similar to file folders, store objects, which consist of data and its descriptive metadata. (https://searchaws.techtarget.com/definition/AWS-bucket)

the PTSC could not ensure that it was scanning for vulnerabilities to meet Federal requirements such as FISMA.

NIH DID NOT ADEQUATELY MONITOR THE PARTICIPANT TECHNOLOGY SYSTEMS CENTER TO ENSURE SECURITY CONTROLS WERE IMPLEMENTED

We determined that NIH did not adequately monitor the PTSC to ensure that it had implemented adequate security controls to protect participants' sensitive data. According to NIH officials, NIH performed biweekly penetration testing of the PTSC's systems; however, these tests were less robust than our test and typically used only vulnerability scanning software tools. The tests we performed included attack techniques that attempted to bypass security controls to gain access to protected systems or sensitive data. By using these techniques, we were able to analyze information systems and applications and attempt to manipulate software applications, which is not possible using only vulnerability scanning software. In addition, our penetration tests accumulated data from multiple exploits of vulnerabilities to gain access to the PTSC's information systems.

NIH's monitoring was not sufficient to ensure that the PTSC implemented adequate security controls to protect participants' sensitive data because the Cooperative Agreement did not specify how NIH would monitor the PTSC's cybersecurity. The Cooperative Agreement with the PTSC stated that the PTSC must comply with both the Trust Principles and the Security Framework, but it did not describe how NIH staff should monitor the PTSC's compliance with those documents to ensure that adequate cybersecurity controls were implemented. Without providing a detailed description of how it will monitor an awardee's cybersecurity in the Cooperative Agreement, NIH staff may not be able to ensure that awardees have implemented adequate security controls to protect sensitive information. We believe that inadequate monitoring by NIH contributed to the vulnerabilities that we found at the PTSC.

RECOMMENDATION

We recommend that NIH revise its *All of Us* Cooperative Agreements and cooperative agreements with security and privacy requirements to include a detailed description of how NIH will monitor cybersecurity and ensure that future awardees adequately implement security controls to protect sensitive data.

NIH COMMENTS

In written comments on our draft report, NIH requested that we revise our recommendation to limit the scope of applicability to "appropriately focus on those cooperative agreement awards with security and privacy requirements," which we have done. NIH stated that, based on our recommendation, it is reviewing *All of Us* Research Program awards. Specifically, NIH stated that it will make necessary updates to security and privacy terms and conditions.

NIH also provided technical comments, which we addressed as appropriate. NIH's comments, excluding the technical comments, are included as Appendix C.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed the information system general controls related to the PTSC and DRC at Vibrent and Vanderbilt respectively. These general controls included security plans, access controls, information protection and system maintenance, audit logging, data and physical security, incident response, and disaster recovery. We conducted our review after an Authority to Operate (ATO) had been issued and signed by NIH and both awardees. The ATO signified that the awardee's information systems were operating and ready for production. We chose not to perform penetration testing of the DRC because there was a risk that such testing could affect the integrity or availability of the *All of Us* database. We performed our fieldwork over 2 weeks at Vibrent in Fairfax, Virginia, in August 2017 and over 1 week at Vanderbilt in Nashville, Tennessee, in February 2018. Our fieldwork concluded in February 2019.

We contracted with Defense Point Security to provide subject-matter experts to conduct penetration testing at Vibrent on behalf of OIG.[17] The assessment consisted of two stages. The first stage was penetration testing and vulnerability assessment of information technology supporting Vibrent's *All of Us* infrastructure and systems both externally and internally. The second stage was mobile application penetration testing to assess the security of Vibrent's *All of Us* mobile applications on both iOS and Android platforms.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal requirements and guidance, NIST guidance, and NIH policies and procedures;
- reviewed NIH awardee documentation;
- assessed NIH policies and procedures for applicable audit areas;
- analyzed supporting documentation such as vulnerability assessment reports;
- selected vulnerabilities from the vulnerability assessment reports to determine whether those vulnerabilities were addressed, remediated, or both;
- judgmentally selected terminated employee user accounts to verify that they were adequately disabled according to NIST guidance; and

[17] Penetration testing is a security assessment where a tester attempts to use attack techniques to bypass security controls to gain access to protected systems or sensitive data.

- discussed our findings with NIH officials.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We shared with NIH information about our vulnerability scan findings immediately following the scans and informed NIH about other preliminary findings in advance of issuing our draft report.

APPENDIX B: FEDERAL REQUIREMENTS AND GUIDANCE

THE WHITE HOUSE

The *Precision Medicine Initiative: Data Security Policy Principles and Framework* (May 25, 2016) states:

> PMI organizations should develop a comprehensive risk-based security plan that outlines roles and responsibilities related to security, consistent with the principles and framework outlined here. The security plan should identify the governance body for the organization's security program. The governance body will ensure that those who use or manage PMI data adhere to the security plan.[18] The security plan should be reviewed by the governance body and updated periodically to incorporate evolving standards and best practices. The plan should describe its approach for:
>
> - Complying with applicable laws and requirements, and other organization-specific security policies and standards;
> - Designating and maintaining an appropriately resourced and technically experienced information security team;
> - Identifying, assessing, and responding to vulnerabilities and threats;
> - Conducting continuous monitoring;
> - Responding to security incidents and breaches;
> - Ensuring the physical security of areas where PMI data is located, as well as that appropriate administrative and technical controls are in place to safeguard the data; and
> - Ensuring participants, researchers, vendors, contractors, and technical staff are aware of their security responsibilities.
>
> PMI organizations should have an independent review of their security plans and of the effectiveness of controls on a periodic basis. The reviewer, at a minimum, should perform: a review of the organization's adherence to its security plan; regular vulnerability assessments (e.g., network scans, penetration testing, and assessments to protect against social engineering attacks); and evaluation and

[18] Please also see governance principles outlined in the White House Precision Medicine Privacy and Trust Principles: https://obamawhitehouse.archives.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf

adjustment of the security program in light of vulnerability assessments and evolving circumstances.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GUIDANCE

NIST SP 800-53, Revision 4 (R4), *Security and Privacy Controls for Federal Information Systems and Organizations*, section SA-11, recommends the developer of the information system, system component, or information system service to implement a verifiable flaw remediation process and correct flaws identified.

NIST SP 800-53 R4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section PS-4, recommends the organization disable information system access upon termination of individual employment.

According to NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment,* section 3.4, "System configuration review is the process of identifying weaknesses in security configuration controls, such as systems not being hardened or configured according to [Federal] security policies, identify unnecessary services and applications, improper user account and password settings, and improper logging and backup settings. Examples of security configuration files that may be reviewed are Windows security policy settings and Unix security configuration files such as those in /etc."

NIST SP 800-53 R4, *Security and Privacy for Federal Information Systems and Organizations*, section SC-28(1), states: "The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [Assignment: organization-defined information system components]."

NIST SP 800-95, *Guide to Secure Web Services*, section 3.1, states that authentication is required to limit access to resources, to identify participants in transactions, and to create seamless personalization of information based on identity. A means of sharing the fact that authentication has been performed successfully is necessary to support single sign-on, allowing users to authenticate with one system and use other services and applications within a Service Oriented Architecture.

NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, section 7, states that without user authentication, organizations will not be able to restrict access to specific information to authorized users. Information that resides on a public server will then be accessible by anyone with access to the server.

NIST SP 800-53, R4, *Security and Privacy Controls for Federal Information Systems and Organizations*, section IA-5, states that the organization manages information system authenticators by protecting authenticator content from unauthorized disclosure and modification and requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.

NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, section 6.1, authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used, possibly in conjunction with other authenticators, to authenticate for that account. Authenticators SHALL be bound to subscriber accounts by either issuance by the Credential Service Provider (CSP) as part of enrollment; or associating a subscriber-provided authenticator that is acceptable to the CSP. These guidelines refer to the binding rather than the issuance of an authenticator as to accommodate both options.

According to NIST SP 800-163, V*etting the Security of Mobile Applications*, section 3.1.3, apps may possess the ability to invoke lower-level command line programs, which may allow access to low-level structures, such as the root directory, or may allow access to sensitive commands. These programs potentially allow a malicious app access to various system resources and information (e.g., finding out the running processes on a device). Although the mobile operating system typically offers protection against directly accessing resources beyond what is available to the user account that the app is running under, this opens up the potential for privilege elevation attacks.

APPENDIX C: NIH COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES Public Health Service

National Institutes of Health
Bethesda, Maryland 20892

DATE: April 17, 2019

TO: Gloria L. Jarmon
Deputy Inspector General for Audit Services, HHS

FROM: Director, National Institutes of Health

SUBJECT: NIH Comments to the Draft Report, *"The National Institutes of Health Could Improve Its Monitoring To Ensure that an Awardee of the All of Us Research Program had Adequate Cybersecurity Controls to Protect Volunteers' Sensitive Data"* (A-18-17-09304)

Attached are the National Institutes of Health's comments on the draft Office of Inspector General (OIG) report, *"The National Institutes of Health Could Improve Its Monitoring To Ensure that an Awardee of the All of Us Research Program had Adequate Cybersecurity Controls to Protect Volunteers' Sensitive Data"* (A-18-17-09304).

The NIH appreciates the review conducted by the OIG and the opportunity to provide clarifications on this draft report. If you have questions or concerns, please contact Meredith Stein in the Office of Management Assessment at 301-402-8482.

/s/ Francis S. Collins, M.D., Ph.D.

Francis S. Collins, M.D., Ph.D.

Attachments
NIH General Comments
NIH Technical Comments

GENERAL COMMENTS OF THE NATIONAL INSTITUTES OF HEALTH (NIH) ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) OFFICE OF INSPECTOR GENERAL (OIG) DRAFT REPORT ENTITLED: "THE NATIONAL INSTITUTES OF HEALTH COULD IMPROVE ITS MONITORING TO ENSURE THAT AN AWARDEE OF THE *ALL OF US* RESEARCH PROGRAM HAD ADEQUATE CYBERSCURITY CONTROLS TO PROTECT VOLUNTEERS' SENSITIVE DATA" (A-18-17-09304)

We appreciate the opportunity to provide these general comments to the OIG draft report, "*The National Institutes of Health Could Improve Its Monitoring To Ensure that an Awardee of the All of Us Research Program had Adequate Cybersecurity Controls to Protect Volunteers' Sensitive Data.*" The security of our participant data is of paramount importance to the *All of Us* Research Program. As such, we require our awardees to abide by Precision Medicine Initiative Trust Principles and Privacy Framework, and we employ many layers of testing and oversight.

It is important to note that the OIG's audit of the *All of Us* Participant Technology Systems Center (PTSC) took place in August 2017, and the penetration texting of the PTSC in October 2017, prior to the opening of the program to broad enrollment. It was during this time that the program was engaged in a robust beta testing phase, the purpose of which was to uncover any potential vulnerabilities. OIG discovered these vulnerabilities within the PTSC firewall under a greybox testing framework. The OIG audit was useful—along with other testing and oversight methods—in identifying specific concerns. The PTSC, with oversight from *All of Us*, remedied these findings, and confirmed with OIG that they were adequately addressed.

As an additional layer of assurance, in April 2018, before the national launch, the program engaged with HackerOne for "real world" security vulnerability testing. HackerOne provides a crowdsourced approach leveraging members of the ethical hacking security community, known as 'Finders,' to conduct penetration testing external to our firewall. These 'Finders' are provided numerous incentives not typically provided by third-party security testers such as immediate compensation (via the bounty), notoriety within the security community, and supplying trusted and accurate vulnerability information to organizations before bad actors do. By engaging with HackerOne, *All of Us*, NIH, and its grant partners benefited from new insight into unknown and exploitable vulnerabilities from a "real-world" perspective without opening firewall holes. The HackerOne engagement tested APIs (Application Protocol Interfaces), Web, Application servers, Web firewall, Access Control Systems (ACS). HackerOne identified 34 security flaws that were all corrected since the testing, with many corrected before the national launch. We plan to continue using HackerOne in 2019. Under a "real-world" situation, like the one *All of Us* engaged in with HackerOne, the additional firewall layer provides additional security to the data.

We are committed, as evidenced in our Core Values (https://allofus.nih.gov/about/about-all-us-research-program), to protecting the data provided. As part of this commitment, we have built and continually enhance a robust security and privacy program. Our *All of Us* Security Program not only partners with the NIH Information Security Program, we also extend operations to work closely with our grant partners to develop an active and evolving security program.

Our systems that process, transmit, and store participant data adhere to the PMI Data Security Policies and Principles Framework (PMI DSP), a framework that is flexible for grant partners to apply a risk-based approach when implementing security controls. The NIH is committed to safeguarding highly sensitive personally identifiable information on behalf of our participants

and has advised our grant partner to apply a FISMA Moderate security baseline from NIST SP 800-53, Revision 4. In addition to security controls selected that provide minimum assurance safeguards, the NIH increased visibility and testing frequency on internal and external facing systems. We apply a layered defense with employing web application firewalls and technologies to cyber-attacks.

By granting a FISMA Authorization to Operate (ATO) for both the Data and Research Center (DRC) and PTSC on May 2017, the NIH emphasized its commitment to safeguarding highly sensitive information on behalf of participants contributing data and formalized its operational security procedures. The NIH provides oversight of the systems and is an active partner in protecting data from misuse, theft, and total loss. In order to receive an ATO, each grant partner must follow a rigorous security review following the six-step process of the Risk Management Framework (RMF). The RMF provided structure and a repeatable process that supplemented the systems development lifecycle (SDLC). Now that the grant partner systems have received ATOs, they are continuously assessing risk within their respective Continuous Monitoring Programs.

OIG Recommendation:
We recommend that NIH revise its cooperative agreements to include a detailed description of how NIH will monitor cybersecurity in the Cooperative Agreement and ensure that future awardees adequately implement security controls to protect sensitive data.

NIH Response:
Based on the scope of the OIG's audit and its findings that focus on a single cooperative agreement award, the recommendation appears broad. As written, the recommendation will affect all NIH cooperative agreement awards regardless of whether those awards involve research participants or sensitive data. As evidenced through the actions taken by NIH to remediate all of the vulnerabilities identified during the audit, we respectfully request that the recommendation be revised to appropriately focus on those cooperative agreement awards with security and privacy requirements.

All of Us is proactively engaged with the PTSC and DRC to continually monitor and improve our security apparatus. Based on the OIG recommendation, we are reviewing our security and privacy terms and conditions in the applicable *All of Us* Research Program awards and, if warranted, will make any necessary updates to ensure we continue to have a multi-faceted, robust security program to protect participant information. NIH will provide an update in our six-month Management Decision response to the OIG.