Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

OPPORTUNITIES EXIST FOR THE NATIONAL INSTITUTES OF HEALTH TO STRENGTHEN CONTROLS IN PLACE TO PERMIT AND MONITOR ACCESS TO ITS 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

February 2019
A-18-18-09350

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: February 2019
Report No. A-18-18-09350

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

Why OIG Did This Review

As part of the Department of Health and Human Services (HHS), the National Institutes of Health (NIH) is the largest public funder of biomedical research agency in the world, investing more than $30 billion in taxpayer dollars to achieve its mission. NIH's mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability. OIG has identified risks related to the sharing of sensitive data.

Our objective was to assess whether NIH had adequate controls in place when permitting and monitoring foreign principal investigators' (PIs) access to NIH genomic data.

How OIG Did This Review

We reviewed NIH's internal controls for monitoring and permitting access to foreign PIs. To accomplish our objective, we used appropriate procedures from applicable Federal regulations and guidance. We reviewed NIH policies, procedures, and supporting documentation, and we interviewed NIH staff.

Opportunities Exist for the National Institutes of Health To Strengthen Controls in Place To Permit and Monitor Access to Its Sensitive Data

What OIG Found

NIH did not consider the risk presented by foreign PIs when permitting access to United States genomic data. NIH expects foreign PIs to safeguard NIH data and use sound security practices in accordance with signed user agreements entered into with the respective NIH Institute or Center. However, NIH has not assessed the risks to national security when permitting data access to foreign PIs. We also found that NIH does not verify that foreign PIs have completed security training, even though NIH's Security Best Practices for Controlled-Access Data emphasize security training as a key control.

What OIG Recommends and NIH Comments

We recommend that NIH work with an organization with national security expertise and knowledge of international risk areas to assess the impact of the potential misuse of genomic data provided to foreign PIs. NIH could strengthen its controls by developing a security framework, conducting a risk assessment, and implementing additional appropriate security controls designed specifically for foreign PIs that have access to genomic data that includes United States citizens. We also recommend that NIH develop and implement mechanisms to ensure that the Genomic Data Sharing Policy keeps current with emerging threats to national security. Lastly, we recommend that NIH make security training and security plans a requirement and develop additional internal controls to verify that foreign PIs and entities have fulfilled those requirements.

NIH did not concur with our recommendations to develop a security framework, conduct a risk assessment, and implement additional controls for sensitive data. NIH concurred with our recommendations to ensure security policies keep current with emerging threats and to make training and security plans a requirement; however, NIH did not agree to the addition of controls to ensure training and security plan requirements have been fulfilled.

We maintain that our findings and recommendations are valid. We recognize that NIH reported that it is already taking certain actions, that may address recommendations. We provided NIH with other potential actions to address our findings.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181809350.asp.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

As part of the Department of Health and Human Services (HHS), the National Institutes of Health (NIH) is the largest public funder of biomedical research agency in the world, investing more than $30 billion in taxpayer dollars to achieve its mission. NIH's mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability. The Office of Inspector General (OIG) has identified risks related to the sharing of genomic data between NIH and foreign principal investigators (PIs),[1] researchers, and foreign entities (collectively, foreign PIs). In addition, there has been congressional interest in NIH's role when permitting foreign PIs access to the genomic data of United States citizens.

OBJECTIVE

Our objective was to assess whether NIH had adequate controls in place when permitting and monitoring foreign PIs' access to NIH genomic data.

BACKGROUND

NIH Genomic Data

NIH's research includes genomic studies, which may advance the understanding of factors that influence health and disease. Sharing genomic data with the research community and combining it with large and information-rich datasets provides opportunities to accelerate that research. NIH developed the Genomic Data Sharing (GDS) Policy, which according to NIH, sets forth expectations that, if followed by researchers, are intended to ensure the broad and responsible sharing of genomic research data. The policy applies to all domestic and foreign NIH-funded research that generates large-scale human subjects' and nonhuman subjects' genomic data.[2] Generally, nonhuman subjects' data is made publicly available through widely used data repositories. However, because of the sensitive nature of human subjects' data, NIH has put in place requirements to limit access to human genomic data (controlled-access data).

[1] NIH does not have a formal definition of a "foreign PI." We discussed with NIH the definition of foreign PIs for purposes of this review, and NIH agreed that a foreign PI can be defined as an applicant from an entity outside the United States. Foreign entities are described by NIH as any non-United States organization, institution, company, etc.

[2] According to NIH's Genomic Data Sharing Policy, "Large-scale non-human genomic data, including data from microbes, microbiomes, and model organisms, as well as relevant associated data (e.g., phenotype and exposure data), are to be shared in a timely manner."

In addition, NIH expects PIs who submit controlled-access data requests to meet NIH's GDS Policy to protect the confidentiality of the data and privacy of the human subjects. According to NIH, prior to submitting data to the NIH repositories, PIs should de-identify human subjects' genomic data according to the standards set forth in the HHS Regulations for the Protection of Human Subjects and the Health Insurance Portability and Accountability Act. As of October 2017, NIH requires a Certificate of Confidentiality to help protect the privacy of individuals who are the subjects of research.

Access to Genomic Data

NIH primarily relies on the appropriate Data Access Committee[3] (committee) to review and approve PI data access requests. Approval depends on (1) correct completion of the request and (2) the committee's confirmation that the data use is consistent with participant consent forms and any other data use limitations. According to NIH, the same set of criteria is used to evaluate data access requests from domestic PIs and foreign PIs.

Risks of Genomic Data Sharing

According to the Federal Bureau of Investigation (FBI), foreign PIs could present increased risks to the United States. The FBI, Weapons of Mass Destruction Directorate (WMDD),[4] has identified risks for entities that share research data (specifically genomic data) and flagged China as a country that presents national security risks to the United States. In testimony before the U.S.-China Economic and Security Review Commission[5] on March 16, 2017, WMDD Supervisory FBI Special Agent Edward H. You stated:

> . . . there is a theoretical risk that the U.S. may become marginalized in the global pharmaceutical market and cede the lead in innovation in the burgeoning and dynamic biological-cyber realm. This could have significant implications on the U.S. at the level of the individual, the

[3] Data Access Committee members (DACs) consist of NIH Federal employees with appropriate expertise (e.g., scientific, bioethics, human subjects research). The Director of the appropriate NIH Institutions or Centers appoints members.

[4] In July 2006, "the FBI created the Weapons of Mass Destruction (WMD) Directorate to build a cohesive and coordinated approach to incidents involving chemical, biological, radiological, or nuclear material, with an overriding focus on prevention. The WMD Directorate proactively seeks out and relies on intelligence to drive preparedness, countermeasures, and investigations designed to keep WMD threats from becoming reality." https://www.fbi.gov/investigate/wmd (Accessed on 6/12/2018).

[5] *Safeguarding the Bioeconomy: U.S. Opportunities and Challenges, Testimony for the U.S.- China Economic and Security Review Commission* (March 16, 2017). The U.S.-China Economic and Security Review Commission (Commission) is mandated to make policy recommendations to Congress based on its hearings and other research and assess the implications of China's developments in biotechnology for the United States.

> economy, for biodefense, and overall national security. [The] WMDD is working to develop countermeasures, in partnership with scientific industry and academia, to prevent adversaries from acquiring and exploiting material and technology that may pose a national security concern. [These] biological threat issues have historically focused upon the potential acquisition, development, and use of materials such as viruses, bacteria, and toxins.

According to Agent You, the risks to national security include, but are not limited, to the weaponization of biological specimens and the bioeconomic imbalance of Chinese companies acquiring United States genomic companies.[6] Moreover, Agent You pointed out that Chinese regulations prevent foreign companies from taking genomic data out of China, resulting in lack of reciprocity.

We have not performed audit work to verify the FBI's conclusions; however, as of the time of our audit, NIH had not considered the national security risks presented by foreign PIs, foreign entities, and nation-states when determining whether to permit access to research data.

FEDERAL REQUIREMENTS

To assess whether NIH controls were adequate to permit and monitor access to NIH data by foreign PIs in accordance with Federal requirements, we used the Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

HOW WE CONDUCTED THIS REVIEW

We reviewed NIH's internal controls for monitoring and permitting access to foreign PIs. To accomplish our objective, we used appropriate procedures from applicable Federal regulations and guidance. We reviewed NIH policies, procedures, and supporting documentation, and we interviewed NIH staff.

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

[6] Some risks posed by foreign PIs may be part of broader national security risks posed by nation-state efforts that generally affect the scientific and research industries in those countries. For example, at the end of 2008, China initiated "the Recruitment Program of Global Experts" (known as "the Thousand Talents Plan"), under which it would bring leading Chinese scientists, academics and entrepreneurs living abroad back to China over the next 5 to 10 years. By the end of May 2014, more than 4,180 overseas high-level individuals were involved in the "1000 Talent Plan."

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 preliminary findings before issuing our draft report.

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

FINDINGS

NIH did not consider the risk presented by foreign PIs when permitting access to United States genomic data. NIH should reassess its current security posture regarding genomic data sharing and fully analyze national security implications before permitting and while monitoring foreign PIs' and entities' data access.

NIH DID NOT CONSIDER NATIONAL SECURITY RISKS WHEN PERMITTING AND MONITORING FOREIGN PRINCIPAL INVESTIGATORS' ACCESS TO UNITED STATES CITIZENS' GENOMIC DATA

We found that NIH:

- had not assessed the risks to national security when permitting access to foreign PIs,
- did not ensure that DAC members and the GDS Policy keep current with emerging threats to national security, and
- did not verify that foreign PIs had completed information security training or verify whether foreign PIs had a security plan.

We determined that NIH permitted access to genomic data to for-profit entities, including companies from China, such as WuXi Nextcode Genomics and Shenzhen BGI Technology Company (even though the FBI has identified those companies as having ties to the Chinese Government). NIH officials did not consider risks related to the United States' national security by foreign PIs connected to state-sponsored activities, the presence of United States and international sanctions, or whether the PI is in a foreign country that is on a United States Government watch list. Although NIH is not specifically required to assess national security risks, allowing companies from China that the FBI has identified as having ties to the Chinese Government highlights the effect of not considering the risks to the United States when permitting access to genomic data.

NIH expects foreign PIs to safeguard NIH data and use sound security practices in accordance with signed user agreements entered into with the respective NIH Institute or Center. PIs requesting access to controlled-access data must submit a Data User Certification Agreement

that references the GDS policy, Genomic Data User Code of Conduct, Certificates of Confidentiality, and Security Best Practices for Controlled-Access Data. We asked NIH whether the signed NIH user agreements are legally binding in foreign or international courts of law. NIH officials responded that to the best of their knowledge, those user agreements have not been used in foreign courts of law against a PI that has misused, abused, or released NIH controlled-access data. Accordingly, it is unclear whether these documents could be effectively enforced should an issue end up in a foreign court.

We reviewed the qualifications of 10 judgmentally selected committee members and spoke with NIH officials about the members' experience with international law and national security. We determined that most of the members have a scientific research background but no formal training in international law pertaining to genomic data sharing. In addition, the committee members did not have a professional background in national security. All 10 committee members had completed a federally mandated counterintelligence training course,[7] but NIH has not considered incorporating any of the counterintelligence training information into the existing internal control framework. As noted in the training course, NIH acknowledged that "[t]hreats that affect NIH are typically driven by economic, social or political agenda, and/or criminal motivation and foreign intelligence entities who want information that will give their organization, company, or country an economic, or competitive advantage over the U.S." We recognize that national security/international law experience may not be typical of individuals who work for NIH, given its mission and function; nevertheless, NIH is exposed to risks of exploiting genomic data from foreign PIs and nations.

NIH has continued to allow access to anyone who meets research requirements and has agreed to comply with the data access request, user agreement, GDS Policy, and Code of Conduct. From a research perspective, NIH has adequate procedures in place for determining whether to permit foreign PIs access to NIH genomic data. For example, NIH has denied applicants based on inconsistencies between the data access request and the expected research use of the requested data (e.g., the foreign PI requests datasets for radiology, but his/her research use statement in the request does not apply to radiology). NIH has also denied PIs' access requests based on limitations, such as limited sharing, placed on the use of the genomic data by other entities. We judgmentally selected a nonstatistical sample of 20 foreign PIs, reviewed their data access requests, and found that all 20 were approved according to NIH policy. However, from a national security perspective, NIH did not consider any restrictions on which foreign PIs were permitted access to research data based on national security risks such as weaponizing viruses for biological warfare.

NIH GDS policy states that it is essential that PIs and their staff who have access to data or maintain it complete appropriate information security training. We found that NIH does not verify that foreign PIs have completed security training, even though NIH's Security Best

[7] NIH Information Security and Information Management Training (https://irtsectraining.nih.gov/publicUser.aspx).

Practices for Controlled-Access Data emphasizes security training as a key control. NIH informed us that it verifies that its own PI staff have completed information security training. In addition, the NIH Security Best Practices for Controlled-Access Data strongly recommend that foreign entities applying for access to NIH data have a security plan in place. NIH informed us that it does not verify whether foreign entities have a security plan. Therefore, NIH does not know whether a security plan exists. Security plans are designed to protect data from high-risk vulnerabilities, which could be specific to the country where the PI resides. Without a risk assessment or documented security plan, it is difficult to identify which risk factors the foreign entities considered and addressed prior to being permitted access to NIH data.

RECOMMENDATIONS

We recommend that NIH work with an organization with national security expertise and knowledge of international risk areas to assess the impact of the potential misuse of genomic data provided to foreign PIs. NIH should determine which resource with national security expertise can best address its needs and assist NIH in developing a comprehensive risk framework. Then, NIH should conduct a risk assessment, develop a security framework, and implement appropriate security controls designed specifically for foreign PIs that have access to genomic data that includes United States citizens.

We also recommend that NIH develop and implement mechanisms to ensure that the GDS Policy keeps current with emerging threats to national security. For example, NIH should involve other Federal committees that specialize in national security and international law to advise the NIH Director on policy changes that ensure the implementation of proactive security controls. Lastly, we recommend that NIH (1) make security training and security plans a requirement that PIs and entities must fulfill before being permitted access to genomic data and (2) develop additional internal controls to verify that foreign PIs and entities have fulfilled those requirements.

NIH COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We would like to thank NIH for its comments on our draft report. We recognize the sensitivities raised by NIH concerning foreign influence in the domestic scientific research community. Our report is not intended to stymie or discourage the advancement of science and the bioeconomy.

NIH provided general comments that questioned the evidence to support the risks identified in our report, including Agent You's testimony cited by OIG regarding the "theoretical risk" of negative economic implications for the United States and the weaponization of biological specimens using genomic data.

We included Agent You's quote as context for the emerging national security risks related to sharing genomic data with foreign entities. Furthermore, NIH has made statements that recognize the actual risks related to foreign governments' actions that target U.S.-conducted

research. These statements align with our findings and the risks identified in our report. The NIH Advisory Committee to the Director (ACD), recently issued a report "ACD Working Group for Foreign Influences on Research Integrity" (December 2018), which identified issues that align with the theoretical risk we presented. Specifically, the report noted:

- "Unfortunately, some foreign governments have initiated systematic programs to unduly influence and capitalize on U.S.-conducted research, including that funded by NIH."
- "These efforts by foreign governments to obtain a competitive advantage in critical areas of research and innovation at the cost of the U.S. research enterprises, the federal government, and the American taxpayer are few, but serious."

In addition, NIH released "Statement on Protecting the Integrity of U.S. Biomedical Research" (August 23, 2018), which identified concerns of influence from foreign entities and foreign governments in NIH research. In the Statement, NIH said it would work to improve accurate reporting of all sources of research support, mitigate the risk to intellectual property security, and explore additional steps to protect the integrity of peer review.

NIH's general comments also stated that its existing controls for all PIs and related entities were sufficient to protect genomic data and ensure genomic data is able to be shared responsibly. NIH cited to their existing controls as a basis for non-concurrence with our first, second, third, and sixth recommendation.

We believe further response by NIH is merited that addresses the risks posed by foreign PIs. However, if NIH has determined that additional controls are not necessary based on our findings, consistent with OMB A-123, NIH should document its acceptance of the risks we presented, in the form of a signed document (by a senior level official). This document should note that NIH conducted a risk assessment of existing controls related to foreign PIs' access to genomic data, that NIH determined existing controls are adequate to protect its sensitive data, and NIH will take no additional actions. This risk acceptance described is one approach that NIH could take to address our findings.

Should NIH choose to conduct a thorough documented risk assessment, it should address recommendations one, two, three and six (NIH concurred with recommendations four and five). Risk mitigation steps that NIH takes in response to the ACD Working Group's recommendations may also address OIG's recommendations.

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

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed NIH's internal controls, policies, and procedures related to access and monitoring practices of genomic data; reviewed NIH supporting documentation; and interviewed NIH staff. We conducted our audit work from June 2017 to September 2018.

METHODOLOGY

To accomplish our objectives, we:

- reviewed applicable Federal regulations and FBI guidance;
- reviewed NIH policies and procedures;
- interviewed NIH data access committee members to discuss internal policies and procedures when permitting access;
- assessed NIH policies and procedures for applicable audit areas;
- analyzed supporting documentation, such as reasons for denying applicants;
- judgmentally selected 20 data access requests of foreign PIs to determine whether their access was approved;
- judgmentally selected 10 NIH employees to determine whether they completed security training; and,
- 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 discussed with NIH information about our preliminary findings in advance of issuing our draft report.

APPENDIX B: FEDERAL CRITERIA

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, emphasizes the importance of having appropriate risk management processes to identify challenges and bring them to the attention of agency leadership so that agency leadership may develop solutions. The Circular states, ". . . agency managers, Inspectors General (IG) and other auditors should establish a new set of parameters encouraging the free flow of information about agency risk points and corrective measure adoption. An open and transparent culture results in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient government."

APPENDIX C: NIH COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES — Public Health Service

National Institutes of Health
Bethesda, Maryland 20892

DATE: December 6, 2018

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

FROM: Director, NIH

SUBJECT: NIH Comments to the Draft Report, *The National Institutes of Health Does Not Have Adequate Controls in Place To Grant and Monitor Foreign Principal Investigators' and Entities Access to Its Genomic Data* (A-18-18-09350)

Attached are the National Institutes of Health's comments on the draft Office of Inspector General (OIG) report, *The National Institutes of Health Does Not Have Adequate Controls in Place To Grant and Monitor Foreign Principal Investigators' and Entities Access to Its Genomic Data* (A-18-18-09350).

NIH appreciates the review conducted by 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

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 DOES NOT HAVE ADEQUATE CONTROLS IN PLACE TO GRANT AND MONITOR FOREIGN PRINCIPAL INVESTIGATORS' AND ENTITIES ACCESS TO ITS GENOMIC DATA" (A-18-18-09350)

NIH appreciates the opportunity to respond to the OIG's draft report entitled *NIH Does Not Have Adequate Controls in Place to Grant and Monitor Access to Foreign Principal Investigators' and Entities' Access to Its Genomic Data (A-18-18-09350).* NIH is sensitive to many of the concerns raised in the draft report regarding foreign influence; in fact, NIH has recently established a Working Group to the Advisory Committee of the Director to address how to mitigate the risk to intellectual property security and protect the integrity of peer review in the face of foreign influence.

NIH must emphasize, however, that the concerns raised by the OIG specific to the security of controlled-access human genomic data are not supported by evidence, and respectfully submits the following general comments in addition to responses to the OIG's recommendations to the agency.

- Principal documentation cited is a single Congressional testimony speculating a **"theoretical risk"** of negative economic implications for the U.S. by the open sharing of genomic information. This argument seems a bit specious, since it is not limited to human genomic data maintained in controlled-access. Moreover, many stakeholders, including Congress, have routinely made the argument that sharing such data is critical to the advancement of both science and the bioeconomy. In fact, if policies were set up to counter every possible theoretical risk, the entire scientific enterprise would arguably come to a halt under the weight of government red tape. It is also important to note that the OIG admits in this report that this singular testimony has not been independently verified, suggesting more evidence needs to be collected to support such an austere recommendation.
- The report points to concerns regarding the weaponization of biological specimens, and we would like to note that numerous policies and international agreements are in place to address global issues around these areas of research. Moreover, we note that again, these issues are not limited to (or even typically focused on) **human genomic data** given the improbability of weaponizing this information.
- Importantly, as NIH has described throughout the OIG engagement, the NIH GDS Policy sets forth expectations and responsibilities to ensure the timely, broad, and responsible sharing of genomic data, in a manner consistent with the consent of the study participants for human genomic data. NIH controls verify that investigators and entities using such broad and timely data sharing is consistent with the NIH mission, advances science and health, and enables NIH to maximize its return on investment. Since 2007, dbGaP has served as the NIH central database for providing controlled-access to human genomic data. Recognizing the importance of transparency in how these data are being used, NIH provides information and statistics accessible by the public on the data submitted to dbGaP, as well as a list of all approved users for each dataset, their institutional affiliations, and their proposed research use of those data. Thus far this system has been successful in protecting against the risks and emerging threats identified by NIH for the sharing of human genomic data.

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 DOES NOT HAVE ADEQUATE CONTROLS IN PLACE TO GRANT AND MONITOR FOREIGN PRINCIPAL INVESTIGATORS' AND ENTITIES ACCESS TO ITS GENOMIC DATA" (A-18-18-09350)

OIG Recommendation 1:
NIH conduct a risk assessment specifically for foreign PIs that have access to genomic data that includes United States citizens.

NIH Response:
NIH does not concur with OIG's finding and corresponding recommendation regarding conducting a risk assessment specifically for foreign PIs as it pertains to access to genomic data. As mentioned above, NIH is sensitive to issues around foreign influence and continues to seek ways to improve the protection of human research data, including genomic data.

That being said, the current process, including institutional sign-off and agreement to follow certain norms and standards is the standard NIH process to establish controls for many mechanisms such as for the submission of funding applications, contracts, and other types of agreements. In doing so, the institution maintains the responsibility to follow those norms and standards. NIH does not independently administer policies directly to different types of investigators, as this would be inefficient and burdensome, difficult to monitor and enforce compliance, and would lead to inconsistencies in policy implementation and practice. For example, NIH's current policies and controls for human genomic data are designed such that the institutions submitting data to the database of Genotypes and Phenotypes (dbGaP) are responsible for assuring that the data submission meets the expectations of the NIH Genomic Data Sharing (GDS) Policy. This assurance includes a delineation of the appropriate uses of the data (based on the consent of the study participants), a review of the proposal for data submission by an Institutional Review Board (IRB) and/or Privacy Board (or equivalent body) to confirm that the deidentification plans are appropriate and to confirm that the data are appropriate for broad sharing through controlled-access. Investigators requesting access to these data must have an account in the NIH electronic Research Administration (eRA) Commons system, which gives the investigators and their institution, whether foreign or domestic, the same level of credentialing and oversight as that which is needed for submitting a funding application.

OIG Recommendation 2:
NIH develop a security framework.

NIH Response:
NIH supports the OIG's assessment of the importance of a robust security framework. However, NIH feels that this framework is indeed in place, as described throughout the OIG engagement of this topic. When requesting access to human genomic data in dbGaP and prior to NIH approval of a request by a NIH Data Access Committee (DAC), all institutions, whether foreign or domestic, must sign-off and agree to the same participant protection principles and data security practices described in the NIH Genomic Data Sharing (GDS) Policy, thus assuring their responsible stewardship and appropriate use of human genomic data. The attestation to

implement the participant protection principles and security requirements provides NIH's expectations for the management and protection of NIH controlled access data transferred to and maintained by institutions whether in their own institutional data storage systems or in cloud computing systems. The sign-off includes institutional agreement to the Genomic Data User Code of Conduct, terms and conditions for data use in the Data Use Certification Agreement, and management and oversight of the data according to the expectations delineated in the NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy "NIH Security Best Practices". Additionally, a DAC will only approve a request if the proposed research use is consistent with the appropriate uses of the data, as delineated by the institution which submitted the data. Such policies and guidelines have been established to control the access or transfer of human genomic data, irrespective of whether the PI is foreign or domestic.

Furthermore, the NIH Security Best Practices document outlines expectations and best practices for key provisions such as security guidelines, controls for servers, controls for copies of data and their destruction, as well as guidance for cloud computing. It also references the Center for Internet Security, the National Institute for Standards and Technology, and the United States Government Configuration Baseline for benchmarks and best practices for security configurations, standards, and baselines, which are widely accepted by Federal agencies. Thus, based on the processes and guidelines which have been established for data submission, access, and management and security, NIH has mechanisms and controls in place which have successfully addressed the risks associated with the sharing human genomic data through controlled-access repositories.

OIG Recommendation 3:
NIH implement appropriate security controls designed specifically for foreign PIs that have access to genomic data that includes United States citizens.

NIH Response:
NIH does not concur with OIG's finding and corresponding recommendation regarding the needs for security controls designed specifically for foreign PIs that have access to genomic data for reasons described in responses to recommendations 1 and 2.

OIG Recommendation 4:
NIH develop and implement mechanisms to ensure that the GDS Policy keeps current with emerging threats to national security.

NIH Response:
NIH concurs with OIG's finding and corresponding recommendation regarding the need to ensure all NIH policies, including the GDS Policy, keep pace with emerging threats to national

security. For instance, in 2013, NIH issued a policy focused on the oversight of life sciences "Dual Use Research of Concern (DURC) (https://grants.nih.gov/grants/guide/notice-files/NOT-OD-13-107.html). To stay abreast of these issues, NIH leadership participates in numerous White House coordinating councils to monitor the landscape and assure that the agency's practices for all data sharing, including human genome sequence sharing, remain up to date with current technologies, consistent with federal security standards, and appropriate to meet any risks related to participant protection or emerging threats to national security.

OIG Recommendation 5:
NIH make security training and security plans a requirement that PIs and entities must fulfill before being permitted access to genomic data.

NIH Response:
NIH concurs that security training and security plans are always beneficial to ensure the conduct of research. NIH will make its current security training more broadly available to non-NIH employees, and examine the feasibility of incorporating it as a requirement in the GDS policy. Of note, however, NIH would like to point out that concerns about the use of human genomic data for bioweapons or other breaches of security are most likely based on concerns about nefarious intent and not due to inappropriate training protocols. Thus, implementation of this measure is not likely to achieve the intended mitigation strategies outlined in the OIG's report.

OIG Recommendation 6:
NIH develop additional internal controls to verify that foreign PIs and entities have fulfilled those requirements (security training and security plans), as stated in Recommendation 5.

NIH Response:
NIH does not concur with OIG's finding and corresponding recommendation regarding additional internal controls specific to foreign PIs for reasons as defined in responses 1 and 2.