Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

NATIONAL INSTITUTES OF HEALTH GRANT PROGRAM CYBERSECURITY REQUIREMENTS NEED IMPROVEMENTS

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

Amy J. Frontz
Deputy Inspector General
for Audit Services

September 2022
A-18-20-06300

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 audits 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.

National Institutes of Health Grant Program Cybersecurity Requirements Need Improvement (A-18-20-06300)

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

September 16, 2022

Ms. Tamara Lilly
Assistant Inspector General for Audit Services
Office of Audit Services
330 Independence Avenue, SW
Washington, DC 20201

Dear Ms. Lilly:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the U.S. Department of Health and Human Services (HHS) – National Institutes of Health's (NIH's) compliance with cybersecurity controls and requirements over its grant program.

We appreciate the assistance we received from the HHS Office of Inspector General and the NIH Office of Extramural Research. We will be pleased to discuss any questions you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Ms. Tamara Lilly
Assistant Inspector General for Audit Services

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the National Institutes of Health's (NIH) cybersecurity controls and requirements over its grant program. The objective of this audit was to determine whether NIH has adequate requirements in place to ensure grant awards have risk-based cybersecurity provisions to protect sensitive and confidential data and NIH's intellectual property.

For this audit, we reviewed NIH's policies and procedures to determine if NIH includes cybersecurity provisions as part of the pre-award risk assessment process and to determine the extent of current cybersecurity requirements. We also reviewed a sample of 75 grants to determine if risk-based cybersecurity provisions were included for the grants. In addition, we completed a review of 3 grantees to determine if post-award monitoring of grantee cybersecurity compliance by NIH was taking place. Audit fieldwork was performed remotely from September 2020 to November 2021 due to COVID-19 health and travel restrictions.

Our audit was performed in accordance with *Generally Accepted Government Auditing Standards*, also known as the Yellow Book, issued by the Government Accountability Office. Those standards require that we plan and perform the audit to obtain sufficient, appropriate audit 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 concluded that NIH did not have adequate controls in place to ensure grants have appropriate cybersecurity provisions. We found that NIH had (1) an inadequate pre-award risk assessment process because it does not consider cybersecurity and has no special term and condition addressing cybersecurity risk in the Notice of Award, (2) inadequate policies because the *NIH Grants Policy Statement* does not include specific, risk-based provisions on cybersecurity, and (3) inadequate post-award monitoring to ensure grantees maintain effective cybersecurity. We made 5 recommendations for NIH to improve its assessment and oversight of cybersecurity compliance within the grant program.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. We concluded our fieldwork and assessment on May 16, 2022. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to May 16, 2022.

The purpose of this audit report is to report on our assessment of NIH's requirements to ensure grants have appropriate cybersecurity protections in place and is not suitable for any other purpose. Additional details on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP

Arlington, Virginia
September 16, 2022

Report in Brief
Date: September 2022
Report No. A-18-20-06300

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

National Institutes of Health Grant Program Cybersecurity Requirements Need Improvement

Why We Did This Review

The Department of Health and Human Services (HHS), Office of Inspector General (OIG) has identified protecting data from misuse or unlawful disclosure as a key component within HHS's top management challenges. Among the issues of interest within data protection were matters pertaining to HHS work with grantees to ensure medical research programs funded and overseen by the Department are adequately secured.

National Institutes of Health (NIH) invests more than $30 billion annually in medical research for the American people. More than 80 percent of NIH's funding is awarded through almost 50,000 competitive grants to various research institutions in all 50 states and around the world. Thus, the data safeguards and security controls protecting federally funded research efforts are of significant importance to both HHS and the Federal government.

The objective of this audit was to determine whether NIH has adequate requirements in place to ensure grant awards have risk-based cybersecurity provisions to protect sensitive and confidential data and NIH's intellectual property. OIG engaged CliftonLarsonAllen LLP (CLA) to conduct this audit.

How We Did This Review

To accomplish our objective, CLA interviewed NIH officials, reviewed NIH's policies and procedures; tested cybersecurity provision adequacy, monitoring and enforcement; and reviewed post-award monitoring and implementation of cybersecurity controls for a sample of grantees.

What We Found

CLA found that NIH did not have: (1) an adequate pre-award risk assessment process because it does not consider cybersecurity and does not include a special term and condition addressing cybersecurity risk in the Notice of Award, (2) adequate policies because the *NIH Grants Policy Statement (NIHGPS)* does not include specific, risk-based provisions on cybersecurity, and (3) adequate post-award monitoring to ensure grantees maintain effective cybersecurity to protect sensitive and confidential data and NIH's intellectual property.

These weaknesses existed because: (1) the NIHGPS and funding opportunity announcements do not specifically identify and address how cybersecurity risk will be evaluated as a requirement of the pre-award process, (2) current NIHGPS cybersecurity provisions are generic and do not establish clear and measurable standards for implementing safeguards proportionate to the assessed level of cybersecurity risk during the pre-award process, and (3) cybersecurity is not part of the scope of current post-award process for grants described in the NIHGPS.

What We Recommend and NIH Comments

CLA recommends that NIH:

(1) Assess its grant award programs to determine which grants should require additional cybersecurity protections due to research potentially including sensitive and confidential data or NIH intellectual property or both.

(2) Based on results of NIH's risk assessment of grant awards, include in the funding opportunity announcements or grant terms and conditions or both the cybersecurity controls that should be implemented.

(3) Strengthen the NIHGPS to establish clear and measurable standards for cybersecurity protections.

(4) Strengthen its pre-award process to identify and address how cybersecurity risk will be assessed.

(5) Strengthen its post-award process to confirm that cybersecurity protections have been implemented to adequately safeguard sensitive and confidential data.

In written comments on our draft report, NIH did not indicate concurrence or nonconcurrence with our recommendations. NIH considers the five recommendations closed and implemented. Based on our review of NIH's comments, we determined that the actions described do not sufficiently address the identified cybersecurity risks. As such, we maintain that our findings and recommendations are accurate and valid. We encourage NIH to implement our recommendations to enhance cybersecurity controls over its grant program. NIH also provided technical comments, which we addressed as appropriate.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Department of Health and Human Services (HHS), Office of Inspector General (OIG) has identified protecting data from misuse or unlawful disclosure as a key component within HHS's top management challenges. Among the issues of interest within data protection were matters pertaining to HHS work with grantees to ensure medical research programs funded and overseen by the Department are adequately secured.[1]

The National Institutes of Health (NIH), in its capacity as a grant making organization, is the primary Federal agency for conducting and supporting medical research to enhance health, lengthen life, and reduce illness and disability. NIH is the largest public funder of biomedical research in the world, investing more than $30 billion in taxpayer dollars annually to achieve its mission.[2] More than 80 percent of NIH's funding is awarded through almost 50,000 competitive grants to more than 300,000 researchers at more than 2,500 universities, medical schools, and other research institutions in all 50 states and around the world.[3]

NIH grant awards cross the spectrum of scientific research. Some awards include genomic research involving human subjects while others focus on the research and development of medical products, like vaccines, that may be NIH's intellectual property. In the November 2020 Grants and Contracts Funding News article,[4] the National Institute of Allergy and Infectious Diseases (NIAID) stated: "At NIH, we handle many kinds of sensitive private information – from patient health records to intellectual property. We protect sensitive information by correctly identifying and storing it using proper protocols. We also expect grantees to follow best practices for cybersecurity and understand the consequences of failing to secure private information."

In his October 2020 Open Mike blog post,[5] Dr. Michael Lauer, NIH's Deputy Director for Extramural Research, stated: "Cybersecurity risks in biomedical research are continually evolving, threatening the integrity of our science and the public's trust in our findings. [Therefore,] as healthcare and research institutions continue to face mounting threats from cyberattacks, it's important that we [i.e., the extramural research community] all not only know

---

[1] *2020 Top Management and Performance Challenges Facing HHS*, https://oig.hhs.gov/reports-and-publications/top-challenges/2020/2020-tmc.pdf.

[2] About NIH, *Impact of NIH Research*, https://www.nih.gov/about-nih/what-we-do/impact-nih-research.

[3] About NIH, *Budget*, https://www.nih.gov/about-nih/what-we-do/budget.

[4] Grants and Contracts Funding News, *Here Are Some Resources to Explore for Cybersecurity Awareness Month*, https://www.niaid.nih.gov/grants-contracts/cybersecurity-awareness-month-2020.

[5] NIH Extramural Nexus, *More Thoughts on Cyber Safety and NIH-Funded Research*, https://nexus.od.nih.gov/all/2020/10/01/more-thoughts-on-cyber-safety-and-nih-funded-research/.

how to protect sensitive information, but also make a personal commitment to keeping data safe. When institutions like yours accept NIH awards, you also accept responsibility for protecting sensitive and confidential data as part of proper stewardship of federally funded research [Section 2.3.12 of *NIH Grants Policy Statement* (GPS)]."

OBJECTIVE

The objective of this audit was to determine whether NIH has adequate requirements in place to ensure grant awards have risk-based cybersecurity provisions to protect sensitive and confidential data and NIH's intellectual property.

BACKGROUND

Federal Internal Control and Risk Assessment Requirements

NIH is responsible for implementing and maintaining a system of effective internal controls over its grant program in line with guidance from the Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* which states:

> Each Federal employee is responsible for safeguarding Federal assets and the efficient delivery of services to the public. Federal leaders and managers are responsible for establishing goals and objectives around operating environments, ensuring compliance with relevant laws and regulations, and managing both expected and unexpected or unanticipated events. They are responsible for implementing management practices that identify, assess, respond, and report on risks. Risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats, and to identify previously unknown opportunities to improve the efficiency and effectiveness of government operations.

Awarding agencies must also "have in place a framework for evaluating the risks posed by applicants before they receive Federal awards," and the awarding agency may apply "special conditions that correspond to the degree of risk assessed" to the award. (*Code of Federal Regulations (CFR)*, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for HHS Awards*, 45 CFR § 75.205(b)). Federal grantees must establish and maintain effective internal controls to provide reasonable assurance that the grantee is managing the award in compliance with Federal laws and policies, as well as the terms and conditions of the award. (45 CFR § 75.303).

The National Institutes of Health as a Grant-Making Organization

NIH must comply with the uniform administrative requirements laid out in Federal regulations at 45 CFR Part 75 and with the Department's Grants Policy Administration Manual (GPAM),

which establishes policies for HHS agencies awarding grant funds. Before making a grant award, NIH must comply with Federal regulations at 45 CFR § 75.205, which states that Federal awarding agencies are required to review the risks posed by applicants. Even if NIH determines that a grant award will be made, it may impose on the grantee special conditions that correspond to the degree of risk associated with making the grant award. Upon award, grantees must comply with all terms and conditions in the Notice of Award. As part of post grant award administration, NIH monitoring activities include, but are not limited to, corresponding with the recipient, reviewing audit reports, reviewing progress reports, and conducting site visits during the award period.[6]

Also, as set forth in NIHGPS § 8.3, "Management Systems and Procedures," grantees are required to establish and maintain effective internal controls (e.g., policies and procedures) that provide reasonable assurance that the award is managed in compliance with Federal statutes, regulations, and the terms and conditions of award. NIH cannot support research unless it has assurance that the grantee will use its funds appropriately, maintain adequate documentation of transactions and safeguard assets. Compliance with the NIHGPS is a term and condition for all NIH grant awards.

The NIHGPS includes general statements about grantee responsibilities to protect and ensure the security of data.[7] NIHGPS § 2.3.12 Protecting Sensitive Data and Information Used in Research requires grantees to consider "their vital responsibility to protect sensitive and confidential data as part of proper stewardship of federally funded research and to take all reasonable and appropriate actions to prevent the inadvertent disclosure, release or loss of sensitive personal information." NIHGPS § 2.3.12 also includes a requirement for grantees to not store personally identifiable, sensitive, and confidential information about NIH-supported research or research participants on portable electronic devices. NIHGPS § 2.3.12 additionally includes requirements to limit access to personally identifiable information through proper access controls such as password protection and to transmit research data only when the security of the recipient's systems is known and satisfactory to the transmitter.

Cybersecurity controls required by the Federal Information Security Modernization Act (FISMA) apply to a grant system when the recipient's system collects, stores, processes, transmits, or uses information on behalf of HHS or any of its component organizations. Grantees are responsible for the security of their original data and intellectual property, subject to all applicable laws protecting security, privacy, and research. NIHGPS § 4.1.9 FISMA requires that

---

[6] The GPAM addresses reduction of applicant risk at part F, chapter 4, and monitoring and reporting at part H, chapter 2.

[7] NIHGPS, https://grants.nih.gov/grants/policy/nihgps/nihgps.pdf
Section 2.3.11 Availability and Confidentiality of Information, clarifies that certain types of information may be considered proprietary or private information that cannot be released. Examples provided in subsection 2.3.11.2.3 Access to Research Data, include, among others, trade secrets; commercial information; intellectual property; personnel and medical files, the disclosure of which would constitute an unwarranted invasion of personal privacy; or information that could be used to identify a particular person in a research study.

"All information systems, electronic or hard copy which contain Federal data need to be protected from unauthorized access. This also applies to information associated with NIH grants and contracts."

Grant award requirements may vary depending on the type of data involved in the research. For example, NIH established the Genomic Data Sharing (GDS) Policy that applies to all NIH-funded research that generates large-scale human or nonhuman genomic data as well as the use of these data for subsequent research.[8] This policy provides additional controls for the sharing of genomic research, such as data sharing plans. Through this policy, NIH also issued a best practices document related to controlled access for genomic data. The best practices document establishes 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.

HOW WE CONDUCTED THIS AUDIT

To determine whether NIH has policies, procedures, and requirements in place to help ensure that grant awards have risk-based cybersecurity provisions to protect sensitive and confidential data and NIH's intellectual property, we reviewed the GPAM, the NIHGPS, the GDS Policy and other NIH related procedures to identify (1) any requirement(s) for pre-grant award consideration of cybersecurity risks, (2) any cybersecurity requirements with which grantees must comply during the grant period, and (3) any NIH oversight responsibilities to monitor grantees compliance with cybersecurity requirements during the grant period. We additionally obtained an understanding of the NIH pre- and post-grant award processes and how the Office of Extramural Research ensures the integrity of and compliance with applicable laws, regulations, and policies that govern NIH extramural research funding.

We obtained a list of all 62,899 extramural grant awards, totaling $32 billion, that were made in Fiscal Year (FY) 2020. To determine if cybersecurity provisions were included for the grants, we selected a judgmental sample of 75 grant awards totaling $1.4 billion, intended to cover a mix of the types of extramural research awards (table, below).

Type of Recipients and Awards Considered When Selecting Grants for Review

Type of Recipient	Type of Award
New grantee	Research projects
Existing grantee	Cooperative agreements
University or private organization	Fellowship programs

We also reviewed specific applicant and grant characteristics that could indicate increased cybersecurity risk. Therefore, we included in our sample grant awards with one or more of the following increased risk characteristics:

- the applicant was a foreign organization or had a foreign component,

[8] Genomic Data Sharing Policy (genome.gov).

- the applicant proposed use of cloud computing to help carry out proposed research,
- the grant involved genomic data sharing,
- the grant involved collection of personally identifiable or personal health information of human subjects, or
- the grant had one of the highest or lowest dollar amounts funded in FY 2020.

We reviewed the documentation for the selected awards to determine whether NIH's process to assess the applicants' management systems included consideration of cybersecurity risk (i.e., the steps NIH takes to ensure grantees can protect sensitive and confidential data and NIH's intellectual property throughout the grant life cycle).

Additionally, we judgmentally selected a sample of three grantees from the 75 sampled grants for testing to determine whether NIH's post-grant award monitoring included confirming (or ensuring) that the grantees had implemented fundamental cybersecurity controls. We also determined whether grantees had implemented cybersecurity controls from the following areas to protect sensitive and confidential data and NIH's intellectual property: Access Control, Contingency Planning, Physical and Environmental Protection and System and Communications Protection. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* was used as a frame of reference for the cybersecurity controls required to secure Federal Government systems. It should be noted that the controls specified in the publication are also required to be implemented by any organization for its IT systems if the system processes, stores, or transmits information on behalf of the Federal government.

Audit fieldwork was performed remotely from September 2020 to November 2021 due to COVID-19 health and travel restrictions. Preliminary findings were communicated to NIH in advance of issuing the draft report. This performance audit was conducted in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*, also known as the Yellow Book, which is issued by the Government Accountability Office (GAO). Those standards require that we plan and perform the audit to obtain sufficient, appropriate audit 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 also describes the details of our audit scope and methodology in brief. **Appendix B** contains other relevant, specific Federal requirements and guidance. **Appendix C** includes NIH's management comments.

FINDINGS

CLA found that NIH did not have (1) an adequate pre-award risk assessment process because it does not consider cybersecurity and does not include a special term and condition addressing cybersecurity risk in the Notice of Award, (2) adequate policies because the NIHGPS does not include specific, risk-based provisions for considering (or requiring) cybersecurity, and (3) adequate post-award monitoring to ensure grantees maintain effective cybersecurity.

These weaknesses existed because: (1) the NIHGPS and funding opportunity announcements do not specifically identify and address how cybersecurity risk will be evaluated as a requirement of the pre-award process, (2) current NIHGPS cybersecurity provisions are generic and do not establish clear and measurable standards for safeguards proportionate to the potential assessed level of cybersecurity risk if conducted during the pre-award process, and (3) cybersecurity is not part of the scope of current post-award process for monitoring grants described in the NIHGPS.

NIH'S PRE-AWARD REVIEW OF GRANT APPLICANTS' CYBERSECURITY RISK AND CONTROLS

Federal Requirements

Prior to making a Federal award, the HHS awarding agency is required to review grant applicant information available through any OMB-designated repositories of governmentwide eligibility qualification or financial integrity information as appropriate (45 CFR § 75.205(a)). In addition, for competitive awards, the awarding agency must have in place a framework for evaluating the risks posed by applicants before they receive Federal awards (45 CFR § 75.205(b)). When evaluating risks posed by grant applicants, the HHS awarding agency may use a risk-based approach considering factors such as the grant applicant's financial stability, quality of management systems, history of performance, reports and findings from previous audits, and the grant applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on non-Federal entities. Criteria to be evaluated must be described in the announcement of funding opportunity (45 CFR § 75.205(c)). Last, the HHS awarding agency may impose specific award conditions as needed in accordance with 45 CFR § 75.207.

Inadequate Policies and Procedures To Assess Cybersecurity Risk Before Grant Award

As part of the pre-award review of grant applicants, GPAM, Part F, Chapter 4 requires NIH to determine the adequacy and acceptability of each grant applicant's financial and business management systems that will support the expenditure of and accountability for NIH funds. Based on the results of the review, NIH may take appropriate action, as necessary, to protect the Federal government's interests, including, but not limited to, the use of specific terms and conditions.

Additionally, the NIHGPS § 8.2.3.3 states that all grant applications, regardless of the amount requested, proposing research that will generate large-scale genomic data, are expected to include a genomic data sharing plan. All grant applicants who wish to use cloud computing for storage and analysis are required by the NIHGPS to indicate in their Data Access Request that they are requesting permission to use cloud computing and identify the cloud service provider or providers that will be employed. The grant applicants will also need to describe how the cloud computing service will be used to carry out their proposed research. According to the NIHGPS, grant applicants are responsible for ensuring the protection of the data and assume responsibility for any failure in the oversight of using cloud computing services for controlled-access data.

NIH's grant pre-award process does not include, as standard procedure, an assessment of cybersecurity risk present in the grant applicants' IT system environments. Although the grant pre-award process assesses risks, such as financial stability, by reviewing certain information submitted by applicants, the current grant pre-award process standard procedure does not require grant applicants to submit information or documentation (e.g., audit reports, certifications) that support the current state of applicants' cybersecurity controls. Additionally, the GDS policy encourages use of third-party providers (e.g., cloud service providers); however, the current genomic data sharing grant pre-award process does not include assessment or require information on how grant applicants screen the cybersecurity controls of significant third-party providers or consider how the grant applicant plans to oversee significant third-party providers.

This weakness existed because the NIHGPS and funding opportunity announcements do not specifically identify and address how cybersecurity risk will be evaluated as a requirement of the pre-award process. As a result, cybersecurity risks to sensitive and confidential data or NIH intellectual property may not have been identified and mitigated before grant funds were awarded.

NIH'S CYBERSECURITY PROVISIONS IN NOTICES OF AWARD TO GRANTEES

Federal Requirements

Before making a Federal award, the operating division (OPDIV, e.g., NIH) must develop a process for conducting pre-award risk assessments to determine the risk an applicant poses to meeting federal programmatic and administrative requirements by taking into account issues such as financial instability, insufficient management systems, non-compliance with award conditions, the charging of unallowable costs, and inexperience (GPAM Chapter 4 b. Policy).[9] If an applicant is found to pose a risk, the OPDIV must either make the award with specific award conditions, or decline to make the award.

When making a Federal award, the HHS awarding agency may include any terms and conditions necessary to communicate requirements that are in addition to the requirements outlined in the HHS awarding agency's general terms and conditions. Whenever practicable, these specific terms and conditions also should be shared on a public website and in notices of funding opportunities (as outlined in 45 CFR § 75.203) in addition to being included in a Federal award (45 CFR § 75.210(c)). Specifically, the announcement should inform potential applicants about special requirements that could apply to particular Federal awards after the review of applications and other information, based on the particular circumstances of the effort to be supported (e.g., if human subjects were to be involved or if some situations may justify special terms on intellectual property, data sharing or security requirements) (45 CFR Part 75, Appendix I § F.2. "Federal Award Administration Information: Administrative and National Policy Requirements").

[9] Management systems refers to the accounting, budgeting, human resources, property management, and procurement management systems and associated policies, procedures, and internal controls maintained by an organization (GPAM Part B, Chapter 2: Definitions).

Limited Cybersecurity Provisions and No Special Terms of Award to Ensure Grantees Protect Sensitive and Confidential Data and NIH's Intellectual Property

The NIHGPS is incorporated by reference in terms and conditions of NIH grant awards. Current provisions with implications for cybersecurity found in the NIHGPS are summarized below:

- 4.1.9 FISMA
  - FISMA applies only to grantees that collect, store, process, transmit, or use Federal data.
  - In all cases, "the recipient retains the original data and intellectual property, and is responsible for the security of this data, subject to all applicable laws protecting security, privacy, and research."
- 8.2.3.3 GDS Policy / Policy for Genome-Wide Association Studies (GWAS)
  - States an expectation of grantee compliance with the GDS Policy and references a best practices document (previously covered in the Background section of this report).
- 2.3.12 Protecting Sensitive Data and Information Used in Research
  - Advises grantees not to store personally identifiable, sensitive, and confidential information on portable electronic devices, to restrict access to such information and to transmit research data (i.e., recorded factual material that validates research findings) once the grantee has determined the security of the recipient's systems is satisfactory.
- 8.1 Changes in Project and Budget
  - States an expectation that grantees will inform NIH when any adverse conditions affect their ability to meet the objectives of the grant awards.

NIH has only established limited cybersecurity provisions in the NIHGPS, which is incorporated into all Notices of Award. Additionally, we noted none of the Notices of Award for the 75 grants we sampled for testing included special terms or conditions related to cybersecurity protections to safeguard sensitive and confidential data and NIH's intellectual property. We also noted that in their grant applications, the 75 grantees in our sample generally did not include descriptions of internal controls over cybersecurity. Further, we observed inconsistent cybersecurity practices by the three grantees for which we conducted security control reviews, driven by varying interpretations of limited cybersecurity provisions in the current NIHGPS.

The limited requirements listed above are not sufficient to ensure that the data is fully protected because they are generic and do not establish clear and measurable standards for safeguards proportionate to the potential assessed level of cybersecurity risk, if conducted, during the pre-award process. In addition, decisions on cybersecurity are left to the grantees with little or no guidance from NIH on what is proper data security, how to communicate and coordinate response to data breaches, and what is effective internal control (i.e., a baseline such as GAO *Green Book*, NIST SP 800-53, etc.) over cybersecurity.

NIH'S POST-AWARD MONITORING AND REPORTING ON GRANTEES' CYBERSECURITY

Federal Requirements

GPAM, Part H, Chapter 2 requires NIH to conduct post-award monitoring for all grants on a regular basis. In accordance with NIHGPS § 8.4 Monitoring, to fulfill its role in regard to the stewardship of Federal funds, NIH monitors their grants to identify potential problems and areas where technical assistance might be necessary. This active monitoring is accomplished through review of reports and correspondence from the grantee, audit reports, site visits, and other information available to NIH. Specific to report and correspondence from the grantee, NIHGPS § 8.4.1 Reporting requires that grantees periodically submit financial and progress reports. Other required reports may include annual invention utilization reports, lobbying disclosures, conflict of interest reports, audit reports, reports to the appropriate payment points (in accordance with instructions received from the payment office), and specialized programmatic reports.

NIH Did Not Adequately Monitor To Ensure Cybersecurity Protections Were Maintained by Grantees

We determined that NIH was not conducting post-grant award monitoring (e.g., special programmatic reports, audits) of cybersecurity at two of the three grantees we selected for security control reviews. NIH did conduct monitoring once at the other grantee in our sample with parts focused on multi-factor authentication and access controls. However, it was an ad-hoc review that was neither required by the NIHGPS nor the grant award.

This weakness existed because cybersecurity is not part of the scope of current post-award process for grants described in the NIHGPS. Instead, NIH relies solely on its grantees to design, implement, maintain, and monitor the effectiveness of their cybersecurity controls in protecting the confidentiality, integrity, and availability of data. As a result, NIH may not be able to identify potential problems with protecting sensitive and confidential data (e.g., proprietary information, personal health information, personally identifiable information, detailed genomic data from human subjects) and NIH's intellectual property. Without identifying those potential problems, NIH may not be able to provide timely technical assistance.

RECOMMENDATIONS

CLA recommends that the National Institutes of Health management implement the recommendations below to enhance cybersecurity controls over its grant program.

1. Assess its grant award programs to determine which grants should require additional cybersecurity protections due to research potentially including sensitive and confidential data or NIH intellectual property or both.

2. Based on results of NIH's risk assessment of grant applicants, include in the funding opportunity announcements or grant terms and conditions or both the cybersecurity controls that should be implemented.

3. Strengthen the NIHGPS to establish clear and measurable standards for cybersecurity protections.

4. Strengthen its pre-award process to identify and address how cybersecurity risk will be assessed.

5. Strengthen its post-award process to confirm that cybersecurity protections have been implemented to adequately safeguard sensitive and confidential data.

NIH COMMENTS AND CLA RESPONSE

In written comments to our draft report, NIH did not indicate concurrence or nonconcurrence with our recommendations. NIH considers the five recommendations closed and implemented through existing NIHGPS requirements, published best practice recommendations, and published the planned addition of Data Management and Sharing (DMS) policy statements to the NIHGPS. Based on our review of NIH's comments, we determined that the actions described do not sufficiently address the identified cybersecurity risks. As such, we maintain that our findings and recommendations are accurate and valid. We encourage NIH to implement our recommendations to enhance cybersecurity controls over its grant program. Listed below is a summary of NIH's comments and CLA's responses. NIH also provided technical comments, which we addressed as appropriate. NIH's general comments are included in their entirety in Appendix C.

Recommendation 1

NIH Comments

NIH stated that it assesses which grants should require additional cybersecurity protections, and it has included additional security protections in Notices of Award (NOA) for specific grants, as appropriate. NIH stated it expects recipients to follow best practices and has issued best practice resources. NIH has also updated its DMS Policy, which includes best practices for selecting a data repository including ensuring that repositories have controls related to confidentiality, security, and integrity.

CLA Response

The current pre-award process does not require grant applicants to submit information or documentation (e.g., audit reports, certifications, etc.) that supports the current state of applicants' cybersecurity controls. Also, CLA found that the NIHGPS, DMS Policy and funding opportunity announcements do not specifically identify and address how cybersecurity risks will be evaluated as a requirement of the pre-award process. We recommended that NIH assess its grant award programs to determine which grants should require additional cybersecurity protections due to research potentially including sensitive and confidential data or NIH intellectual property or both. Please see report section **NIH'S PRE-AWARD REVIEW OF GRANT APPLICANTS' CYBERSECURITY RISK AND CONTROLS** for more details.

Specifically, the OMB Memorandum (M)-16-17, Subject: Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 15, 2016: Section VII. Additional Considerations, subsection C. Managing Grants Risks in Federal Programs, states, in part: "the guidance in CFR Title 2 *Grants and Agreements* Part 200 *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*] 2 CFR 200.205 [and 200.206] requires Federal awarding agency [(e.g., NIH)] review of risk(s) posed by applicants, risk evaluation(s) whenever making new awards, and authorized use of a risk-based approach. Within each Federal Agency [(e.g., NIH)], there is a shared interest for management and oversight of Federal grant dollars from both a financial management and grants management perspective. Leveraging the risk-based perspective, the internal controls framework should

serve as a mechanism to ensure effective and efficient allocation and use of Federal grant dollars."

Based on our review of the examples provided by NIH in response to recommendation 1, we noted they do not provide specific cybersecurity requirements. For example, 2U24MH068457-11 to support the Center for Genomic Studies on Mental Disorders states, in part: "Recipient shall develop and maintain secure password-protected web sites…" However, it does not incorporate by reference Federal requirements for password generation (e.g., length, complexity, etc.) and maintenance (e.g., age, history, etc.) such as NIST SP 800-53.

For the other two examples provided in NIH's response, the best practices listed offer elective recommendations or expectations such as adopting a generally acceptable approach to cybersecurity. However, best practice recommendations may or may not be adopted at the discretion of the grantees. In contrast, standards set clear and measurable requirements for cybersecurity protections and gives NIH reasonable assurance that sensitive and confidential data or NIH intellectual property is protected.

We maintain that this recommendation and its related findings are valid.

Recommendation 2

NIH Comments

NIH stated that it issued the NIH DMS Policy in 2020 with an effective date of January 23, 2023. The NIH DMS Policy provides best practices for selecting data repositories with appropriate data management and security controls. This policy applies to all NIH-supported research that results in the generation of scientific data and will be incorporated via an update to the NIHGPS.

CLA Response

CLA found that NIH did not have an adequate pre-award risk assessment process because it does not require grant applicants to submit information or documentation (e.g., audit reports, certifications) that support the current state of applicants' cybersecurity controls. Also, the current grant pre-award process does not include an assessment of cybersecurity risk present in the grant applicants' IT system environments. Based on review of the DMS Policy documented above, it does not sufficiently address the security of data being shared or the security of data being generated and stored for sharing. We recommended that based on results of NIH's risk assessment of grant applicants, NIH management should include in the funding opportunity announcements or grant terms and conditions or both the cybersecurity controls that should be implemented. Please see report section **NIH'S PRE-AWARD REVIEW OF GRANT APPLICANTS' CYBERSECURITY RISK AND CONTROLS** for more details.

The DMS Policy states the following regarding data security: "We have removed the prompt for researchers to address provisions related to the security of scientific data. While we agree with the importance of appropriate data security measures, we believe that technical provisions regarding data security are more appropriately addressed by the institutions and repositories

preserving and sharing the scientific data. …we do not wish to burden the funded community with describing in-depth the data security processes of the data repositories preserving and sharing the data generated by their research. While data may remain with an institution prior to submission to a data repository, the DMS Policy is not designed to set any new standards for institutional data security practices."

The DMS Policy references the following supplemental information for more guidance on data security:
Supplemental Information to the NIH Policy for Data Management and Sharing: Selecting a Repository for Data Resulting from NIH-Supported Research, I. Desirable Characteristics for All Data Repositories, H. Security and Integrity states: "[The data repository under consideration for selection] Has documented measures in place to meet generally accepted criteria for preventing unauthorized access to, modification of, or release of data, with levels of security that are appropriate to the sensitivity of data."

Supplemental Information to the NIH Policy for Data Management and Sharing: Elements of an NIH Data Management and Sharing Plan states: "The final National Institutes of Health (NIH) Policy for Data Management and Sharing requires applicants to submit a Data Management and Sharing Plan (Plan) for any NIH-funded or conducted research that will generate scientific data. This supplemental information outlines the Elements to be addressed in a Plan within two pages or less." The Access, Distribution, or Reuse Considerations section states: "NIH expects that in drafting Plans, researchers maximize the appropriate sharing of scientific data generated from NIH-funded or conducted research, consistent with privacy, security, informed consent, and proprietary issues."

Recommendation 3

NIH Comments

NIH stated that in 2020 it issued the 2023 NIH DMS Policy, which provides best practices for selecting data repositories with appropriate data management and security controls. This policy applies to all NIH-supported research that results in the generation of scientific data and will be incorporated via an update to the NIHGPS.

CLA Response

CLA found that NIH did not have adequate policies because the NIHGPS and related documents (e.g., GDS, DMS) do not include specific, risk-based provisions for requiring cybersecurity. We recommended that NIH strengthen the NIHGPS to establish clear and measurable standards for cybersecurity protections. Please see report section **NIH'S CYBERSECURITY PROVISIONS IN NOTICES OF AWARD TO GRANTEES** for details.

While we appreciate NIH's efforts regarding the 2023 NIH DMS Policy and its planned incorporation into the NIHGPS, these changes do not define special requirements proportionate to the assessed level of cybersecurity risk. Specifically, the funding opportunity announcement should inform potential applicants about special requirements that could apply to particular Federal awards after the review of applications and other information, based on the particular

circumstances of the effort to be supported (e.g., if human subjects were to be involved or if some situations may justify special terms on intellectual property, data sharing or security requirements) (45 CFR Part 75, Appendix I § F.2. "Federal Award Administration Information: Administrative and National Policy Requirements").

Decisions on what is required for cybersecurity are left to the grantees with little or no guidance from NIH on what is proper data security, how to communicate and coordinate response to data breaches, and what is effective internal control (i.e., a baseline such as GAO Green Book, NIST SP 800-53, etc.) over cybersecurity. We maintain that this recommendation and its related findings are valid.

Recommendation 4

NIH Comments

NIH stated that for all NIH-supported activities where a DMS plan is required, it recommends that the DMS plan address a number of factors, including privacy and confidentiality protections. NIH also stated that it will assess the plan as part of the pre-award risk-assessment process, and if proposed controls are insufficient, it will negotiate revisions or apply specific award conditions in accordance with NIHGPS, section 8.5.1, "Specific or Special Award Conditions- Modification of the Terms of Award."

CLA Response

CLA found that the DMS policy does not sufficiently address cybersecurity protections. Also, NIHGPS and funding opportunity announcements do not specifically identify and address how cybersecurity risk will be evaluated as a requirement of the pre-award process. We recommended that NIH strengthen its pre-award process to identify and address how cybersecurity risk will be assessed. Please see report sections **NIH'S PRE-AWARD REVIEW OF GRANT APPLICANTS' CYBERSECURITY RISK AND CONTROLS** and **NIH'S CYBERSECURITY PROVISIONS IN NOTICES OF AWARD TO GRANTEES** for more details.

According to the DMS Policy, "Plans should explain how scientific data generated by research projects will be managed and which of these scientific data and accompanying metadata will be shared." Based on review of supplemental guidance to the DMS Policy on what to include in the plans, they do not cover in sufficient breadth and depth the cybersecurity protections that have been implemented to safeguard sensitive and confidential data.

Specifically, the DMS Policy references the following supplemental information for more guidance on data security:
Supplemental Information to the NIH Policy for Data Management and Sharing: Selecting a Repository for Data Resulting from NIH-Supported Research, I. Desirable Characteristics for All Data Repositories, H. Security and Integrity states: "[The data repository under consideration for selection] Has documented measures in place to meet generally accepted criteria for preventing unauthorized access to, modification of, or release of data, with levels of security that are appropriate to the sensitivity of data."

Supplemental Information to the NIH Policy for Data Management and Sharing: Elements of an NIH Data Management and Sharing Plan, Access, Distribution, or Reuse Considerations section states: "NIH expects that in drafting Plans, researchers maximize the appropriate sharing of scientific data generated from NIH-funded or conducted research, consistent with privacy, security, informed consent, and proprietary issues."

We maintain that this recommendation and its related findings are valid.

Recommendation 5

NIH Comments

NIH stated that for all awards where the DMS Policy applies, the data management and sharing plan submitted by the applicant will be incorporated by reference as a term of award. NIH also stated that as a result, noncompliance will be subject to enforcement action in accordance with NIHGPS, section 8.5.2, "Remedies for Noncompliance or Enforcement Actions: Suspension, Termination, and Withholding of Support."

CLA Response

CLA found that neither the NIHGPS nor the DMS Policy's post-grant award monitoring process includes cybersecurity protections. We recommended that NIH strengthen its post-award process to confirm that cybersecurity protections have been implemented to adequately safeguard sensitive and confidential data. Please see report section **NIH'S POST-AWARD MONITORING AND REPORTING ON GRANTEES' CYBERSECURITY** for more details.

Without a process to review cybersecurity protections, NIH may not be aware of cybersecurity weaknesses and may not be able to enforce corrective actions consistently and accurately for a grantee's deficiencies related to cybersecurity or identify grantee noncompliance with terms of award to impose suspension, termination, or withholding of support of a grantee. Consequently, NIH relies solely on its grantees to design, implement, maintain, and monitor the effectiveness of their cybersecurity controls in protecting the confidentiality, integrity, and availability of data. As a result, NIH's existing post-award process may not separately identify potential weaknesses with protecting sensitive and confidential data (e.g., proprietary information, personal health information, personally identifiable information, and detailed genomic data from human subjects) and NIH's intellectual property.

We maintain that this recommendation and its related findings are valid.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

CLA limited the audit to NIH's policies, processes, and procedures regarding NIH Office of Extramural Research (OER) cybersecurity requirements related to grants. CLA reviewed a sample of 75 grants to determine if appropriate cybersecurity provisions were included for the grants. In addition, CLA completed a review of three grantees to determine whether post-grant award monitoring of cybersecurity was taking place and to determine whether grantees had implemented fundamental cybersecurity controls related to access control, contingency planning, physical and environmental protection, and system and communications protection.

Audit fieldwork was performed remotely from September 2020 to November 2021 due to COVID-19 health and travel related restrictions.

METHODOLOGY

To accomplish our objective, CLA:

- Reviewed applicable federal laws, regulations, and guidance.
- Interviewed NIH OER personnel and reviewed business objectives, processes, and requirements for OER and the grant program.
- Performed a review of NIH's OER cybersecurity provision monitoring and enforcement for the grant program.
- Reviewed sampled grants to determine if appropriate cybersecurity provisions were included, monitored, and enforced.
- Performed a review of three grantees to determine whether NIH specific cybersecurity requirements were defined in the areas of access control, contingency planning, physical and environmental protection, and system and communication protection.
- Reviewed public information available on NIH website.
- Discussed the results of the audit with NIH officials.

In selecting and testing for the adequacy and effectiveness of considering, including, monitoring, and enforcing cybersecurity provisions in grants, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In cases where the entire audit population was not selected, the results cannot be projected and if projected may be misleading.

CLA conducted this audit in accordance with performance auditing standards, as in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*, also known as the Yellow Book, which is issued by the Government Accountability Office (GAO). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS AND GUIDANCE

As a supplement to criteria cited in the report, below we present a summary of other relevant, specific Federal requirements and guidance we provided to NIH OER management under separate cover.

Office of Management and Budget (OMB) Memorandum (M)-16-17, Subject: Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016: Section VII. Additional Considerations, subsection C. Managing Grants Risks in Federal Programs, states, in part:

> "the guidance in [*Code of Federal Regulations* (CFR) Title 2 *Grants and Agreements* Part 200 *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*] 2 CFR 200.205 [and 200.206] requires Federal awarding agency [(e.g., NIH)] review of risk(s) posed by applicants, risk evaluation(s) whenever making new awards, and authorized use of a risk-based approach. Within each Federal Agency [(e.g., NIH)], there is a shared interest for management and oversight of Federal grant dollars from both a financial management and grants management perspective. Leveraging the risk-based perspective, the internal controls framework should serve as a mechanism to ensure effective and efficient allocation and use of Federal grant dollars."

OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017: Section V. Preparing for a Breach, Subsection C. Grants and Grantee Requirements for Breach Response states, in part, "When a grant recipient uses or operates a Federal information system or creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII within the scope of a Federal award, the agency shall ensure that the grant recipient has procedures in place to respond to a breach and include terms and conditions requiring the recipient to notify the Federal awarding agency in the event of a breach."

Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* (*Green Book*) Foreword on PDF p. 7 states, in part:

> "a key factor in improving accountability in achieving an entity's mission is to implement an effective internal control system. An effective internal control system helps an entity adapt to shifting environments, evolving demands, changing risks, and new priorities. As programs change and entities strive to improve operational processes and implement new technology, management continually evaluates its internal control system so that it is effective and updated when necessary."

In addition, *Green Book* Principle 15 Communicate Externally, Communication with External Parties, 15.05 on PDF p. 68 states:

"The oversight body receives information through reporting lines from external parties. Information communicated to the oversight body includes significant matters relating to risks, changes, or issues that impact the entity's internal control system. This communication is necessary for the effective oversight of internal control."

APPENDIX C: NIH'S MANAGEMENT COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

National Institutes of Health
Bethesda, Maryland 20892

www.nih.gov

DATE: July 10, 2022

TO: Amy J. Frontz
Deputy Inspector General for Audit Services, HHS

FROM: Acting Principal Deputy Director, National Institutes of Health

SUBJECT: NIH Comments in Response to Draft Report, *"National Institutes of Health Grant Program Cybersecurity Requirements Need Improvement (A-18-20-06300)"*

Attached are the National Institutes of Health's comments on the draft HHS Office of Inspector General (OIG) Draft Report, *National Institutes of Health Grant Program Cybersecurity Requirements Need Improvement (A-18-20-06300)*.

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

Tara A. Schwetz, Ph.D.

Attachments

The National Institutes of Health (NIH) appreciates the review conducted by OIG and the opportunity to provide clarifications on this draft report. NIH respectfully submits the following general comments.

OIG Recommendation 1:
Assess its grant award programs to determine which grants should require additional cybersecurity protections due to research potentially including sensitive and confidential data or NIH intellectual property or both.

NIH Response:
NIH considers this recommendation closed, implemented. NIH does assess which grants should require additional cybersecurity protections, and NIH has included additional security protections in Notices of Award (NOA) for specific grants, as appropriate. A few examples are as follows:

An NOA for cooperative agreement 2U24MH068457-11 to support the Center for Genomic Studies on Mental Disorders (which, in part, supports a data repository) included this term: Recipient shall develop and maintain secure password-protected web sites, in order to prevent misuse of data while permitting the rapid and efficient distribution of electronic data files to qualified investigators granted access by NIMH to the NIMH Human Genetics Initiative resource.

Additionally, NIH expects recipients to follow best practices and has issued best practice resources, as NIH provided to the OIG and as identified in the OIG draft report. For example, the FOAs for the following grant programs include this language about best practices:

- The NHGRI Genomic Data Science Analysis, Visualization, and Informatics Lab-space (AnVIL) (U24)

    - **Data security and access**
      Data security encompasses confidentiality, data integrity, and availability. While all three elements are important for the AnVIL, maintaining confidentiality of controlled access data is a particularly high priority. Confidentiality includes managing data access to maintain data security, and make data accessible to authorized users only for authorized purposes. Data security protection and proper stewardship of human genomic, phenotypic and other sensitive information stored and distributed by the AnVIL is of the utmost importance. The Notice for Use of Cloud Computing Services for Storage and Analysis of Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy (Ref: https://grants.nih.gov/grants/guide/notice-files/NOT-OD-15-086.html) allows investigators to perform genomic analyses on a cloud platform. The NIH security best practices and provisions (https://www.ncbi.nlm.nih.gov/projects/gap/pdf/dbgap_2b_security_procedures.pdf) should be implemented to protect the privacy and confidentiality of

research participants, and prevent unauthorized access to data. The resource is also expected to develop policies and procedures for notifying NHGRI, and managing, and mediating any loss of data or compromise of data confidentiality.

The AnVIL should conduct regular audits of its data security and protection processes, which should be validated by third party independent assessments. The Precision Medicine Initiative's Data Security Principles Implementation Guide provides an example for auditing and data security protection processes https://www.healthit.gov/sites/default/files/pmi_security_ig_v16-clean.pdf

The AnVIL will need to establish and maintain a user authentication system to allow secure access to the data and computing services of the AnVIL by individual researchers and groups of users with different access privileges. The user authentication system developed for the AnVIL should also be interoperable with established NIH authentication systems, such as the eRA Commons, for approved users of NIH data resources. Also, current NIH processes that authorize access to controlled access data through the NIH Data Access Committees should be supported.

The AnVIL is also expected to develop and implement streamlined technical and administrative processes to review and authorize controlled-access data requests, while taking into account the data use limitations of the studies hosted by the AnVIL. In addition, guidelines for the download of data from the AnVIL, including data derived from computational analyses of AnVIL's datasets performed by the users, should be developed and implemented to address any privacy concerns associated with the download of individual level data. These activities should be pursued in consultation with NHGRI staff (including the NHGRI Data Access Committee), the Data Steering Committee and External Advisory Committee (see below).

- Harnessing Data Science for Health Discovery and Innovation in Africa (DS-I Africa) Open Data Science Platform and Coordinating Center (U2C – Clinical Trial Not Allowed)

    - **Access & Security: The ODSP must address data security and privacy.**
    The ODSP is expected to address security requirements and support an existing, open authentication capability and/or provide resources to do remote identity proofing and credential distribution as per NIST Special Publication 800-63B for any community researcher that desires access to the data. Additionally, the ODSP must implement contingency procedures for incidents and breaches related to data loss or compromise.

      Privacy includes complying with data protection and anonymization requirements and adhering to data use limitations/agreements. The ODSP must comply with and implement NIH research authentication policy and services respectively to enable use of controlled-access data for approved users. These

requirements should be implemented in consultation with NIH program staff to ensure fit within the Common Fund data ecosystem.

The ODSP must provide for and govern data access guidelines, data use agreements and data sharing policies that are consistent with the NIH Data Sharing Policy and Implementation Guidance as well as with the NIH Genomics Data Sharing Policy (NOT-OD-14-124) and the NIH Notice for Use of Cloud Computing Services for Storage and Analysis of Controlled-Access Data Subject to the NIH Genomic Data Sharing Policy (NOT-OD-15-086), as applicable. The ODSP should also implement the NIH security best practices and provisions to protect the privacy and confidentiality of research participants and prevent unauthorized access to data.

And as previously shared with the OIG in 2020, NIH has already updated its Data Management and Sharing (DMS) Policy, which includes best practices for selecting a data repository effective for all applications with submission due dates on/after January 25, 2023 (and therefore incorporated by reference as a term and condition for all resulting NIH awards). These best practices for repository selection include ensuring that repositories have controls related to confidentiality, security, and integrity.

The 2023 NIH Data Management and Sharing Policy states:

- The policy applies to all NIH-supported research that results in the generation of scientific data, regardless of funding mechanism. See Research Covered Under the Data Management & Sharing Policy for more details.
- The DMS Policy does not apply to research and other activities that do not generate scientific data, for example: training, infrastructure development, and non-research activities.

OIG Recommendation 2:
Based on results of NIH's risk assessment of grant awards, include in the funding opportunity announcements or grant terms and conditions or both the cybersecurity controls that should be implemented.

NIH Response:
NIH considers this recommendation closed, implemented.

In 2020, NIH issued the 2023 NIH DMS Policy which provides best practices for selecting data repositories with appropriate data management and security controls. This policy applies to all NIH-supported research that results in the generation of scientific data, and will be incorporated via update to the NIHGPS.

OIG Recommendation 3:
Strengthen the NIHGPS to establish clear and measurable standards for cybersecurity protections.

NIH Response:
NIH considers this recommendation closed, implemented.

In 2020, NIH issued the 2023 NIH DMS Policy which provides best practices for selecting data repositories with appropriate data management and security controls. This policy applies to all NIH-supported research that results in the generation of scientific data, and will be incorporated via update to the NIHGPS.

OIG Recommendation 4:
Strengthen its pre-award process to identify and address how cybersecurity risk will be assessed.

NIH Response:
NIH considers this recommendation closed, implemented.

In 2020, NIH already issued the 2023 NIH DMS Policy. For all NIH-supported activities where a DMS plan is required, NIH recommends that the DMS plan address a number of factors, including privacy and confidentiality protections. NIH will assess the plan as part of the pre-award risk-assessment process, and if proposed controls are insufficient NIH will negotiate revisions or apply specific award conditions in accordance with NIHGPS Section 8.5.1 "Specific or Special Award Conditions- Modification of the Terms of Award"

OIG Recommendation 5:
Strengthen its post-award process to confirm that cybersecurity protections have been implemented to adequately safeguard sensitive and confidential data.

NIH Response:
NIH considers this recommendation closed, implemented.

In 2020, NIH already issued the 2023 NIH DMS Policy. For all awards where this DMS Policy applies, the plan submitted by the applicant will be incorporated by reference as a term of award, and therefore noncompliance will be subject to enforcement action in accordance with NIHGPS Section 8.5.2 "Remedies for Noncompliance or Enforcement Actions: Suspension, Termination, and Withholding of Support."