Report in Brief
Date: Septmeber 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 OIG 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.

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 OIG Did This Audit

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 OIG 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 OIG Recommends and CMS' 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.