COSMOS
Navigate the Compliance Universe

Report on Research Compliance Volume 19, Number 11. October 27, 2022
RRC E-Alerts: October 20, 2022

By Theresa Defino

OIG Finds Security Weaknesses at NIH; Agency Says No Changes Needed

NIH is unable to "ensure grants have appropriate cybersecurity provisions" and should make nearly a half-dozen changes, according to auditors for the HHS Office of Inspector General (OIG). Yet, NIH said it had already made the recommended improvements—an assertion auditors disputed. CliftonLarsonAllen LLP "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." Auditors also "reviewed a sample of 75 grants to determine if risk-based cybersecurity provisions were included for the grants" and "completed a review of 3 grantees to determine if post-award monitoring of grantee cybersecurity compliance by NIH was taking place." Auditors found NIH has "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," and also has "inadequate policies because the *NIH Grants Policy Statement* [NIHGPS] does not include specific, risk-based provisions on cybersecurity." The agency also lacks "post-award monitoring to ensure grantees maintain effective cybersecurity," according to the report.

Auditors said 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." Among the recommendations are that NIH should "determine which grants should require additional cybersecurity protections due to research potentially including sensitive and confidential data or NIH intellectual property or both" and what those controls should be; "establish clear and measurable standards for cybersecurity protections"; and "strengthen its post-award process to confirm that cybersecurity protections have been implemented to adequately safeguard sensitive and confidential data." However, auditors wrote that 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," the report states. "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."

Link to audit