Report in Brief
Date: February 2024
Report No. A-18-22-03300

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

NIH Generally Implemented System Controls Over the Sequence Read Archive But Some Improvements Needed

Why We Did This Audit

The Department of Health and Human Services (HHS), Office of Inspector General (OIG) has identified securing HHS data and systems to positively impact the cybersecurity posture of HHS and the sectors HHS influences as a key component within HHS's top management challenges.

The National Institutes of Health (NIH) Sequence Read Archive (SRA), which is hosted by National Library of Medicine (NLM), is the largest publicly available repository of high throughput sequencing data used for genomic research. The SRA holds diverse genomic data, including early COVID-19 sequencing, and is part of the International Nucleotide Sequence Database Collaboration.

The objective was to determine whether NIH has adequate controls in place to ensure data integrity of the NCBI Sequence Read Archive. OIG engaged the independent certified public accounting firm Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct this audit.

How We Did This Audit

To accomplish our objective, Brown & Company interviewed NIH officials, reviewed NIH's SRA information security policies and procedures, tested system controls; and examined 50 samples of the SRA data normalization and SRA Lite files to determine if the files were normalized as intended.

What We Found

Brown & Company found that NIH adequately implemented most of the system and information integrity controls that ensure the integrity of the SRA data. However, control weaknesses were identified that should be addressed to improve the security of the SRA and its data.

While NIH stated the overall security categorization for the SRA was low impact, NIH did not document the rationale for the security categorization as is required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 1, Revision 1.

NIH also did not conduct an SRA system-level risk assessment to identify threats and vulnerabilities as required by NIH's policy. However, NIH was required by NIST SP 800-53, Revision 4, to perform a system-level risk assessment for the SRA before it was authorized to operate and put into production.

In addition, the SRA data normalization policy lacked the assignment of roles and responsibilities to ensure the integrity of the SRA and its data.

What We Recommend and NIH Comments

Brown & Company recommends that the NIH implement the recommendations below to improve controls over its SRA.

1. Complete the security categorization in accordance with FIPS Pub 199 to include documenting results and supporting rationale in the security plan.
2. Conduct a system-level risk assessment for the SRA in accordance with NIST SP 800-53 requirements and NIH polices.
3. Ensure that the data normalization policy and procedures comply with Federal requirements to include defining roles and responsibilities.

In written comments on our draft report, NIH concurred with all the recommendations and described actions it plans to take to implement the recommendations.