NIST SPECIAL PUBLICATION 1800-43

Genomic Data Threat Modeling:

An Implementation for Genomic Data Sequencing and Analysis

Includes: Executive Summary (A)

Ronald Pulivarti
Justin Wagner
Isabelle Brown-Cantrell
Brett Kreider
Patrick Pape
Scott Ross
Stuart S. Shapiro
Jared Sheldon
Julie Nethery Snyder
Philip Whitlow
Kevin E. Wilson
Martin Wojtniak

August 2025

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/cybersecurity-and-privacy-genomic-data

NIST
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-43

Genomic Data Threat Modeling: An Implementation for Genomic Data Sequencing and Analysis

Includes Executive Summary (A)

Ronald Pulivarti
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Justin Wagner
Materials Measurement Laboratory
National Institute of Standards and Technology

Brett Kreider
Stuart S. Shapiro
Julie Nethery Snyder
Kevin E. Wilson
Martin Wojtyniak
The MITRE Corporation

Philip Whitlow
Scott Ross
HudsonAlpha Institute for Biotechnology

Isabelle Brown-Cantrell
Patrick Pape
Jared Sheldon
The University of Alabama in Huntsville

DRAFT

August 2025

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST SPECIAL PUBLICATION 1800-43A

Genomic Data Threat Modeling:

An Implementation for Genomic Data Sequencing and Analysis

Volume A:
Executive Summary

Ronald Pulivarti
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Justin Wagner
Materials Measurement Laboratory
National Institute of Standards and Technology

Brett Kreider
Stuart S. Shapiro
Julie Nethery Snyder
Kevin E. Wilson

Martin Wojtyniak
The MITRE Corporation

Philip Whitlow
Scott Ross
HudsonAlpha Institute for Biotechnology

Isabelle Brown-Cantrell
Patrick Pape
Jared Sheldon
The University of Alabama in Huntsville

August 2025

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/cybersecurity-and-privacy-genomic-data

Executive Summary

Genomic data is a digital representation of the DNA in a biological sample. DNA encodes hereditary information for cells to function, but this same information poses cybersecurity and privacy challenges as it can reveal potentially sensitive details about an individual's kinship, traits, and health status. Genome sequencing refers to the laboratory process of converting a physical sample to digital format using purpose-built equipment. The data output for common sequencing experiments ranges from multiple gigabytes to terabytes, which is then analyzed for research or in clinical diagnostics. Genomic data processing systems can include proprietary sequencing equipment or utilization of genome sequencing service providers followed by genomic analysis computations occurring on premise or in a cloud environment. Given the varied landscape of genome data processing systems, this Special Publication (SP) 1800-series from the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) describes a threat modeling exercise—methodical analysis of cybersecurity and privacy risks to system components and data transfers across a product or environment lifecycle—on an example genomic data workflow.

CHALLENGE

From a cybersecurity perspective, the size and compute requirements for genomic data analysis make it difficult to ensure the confidentially, integrity, and availability of computing environments. Regarding privacy engineering, since genomic data represents immutable personal information, designing and maintaining data processing systems with the objectives of predictability, manageability, and disassociability is complex. These challenges are compounded by the involvement of multiple stakeholders which can include researchers, healthcare providers, and third-party vendors.

This SP 1800-series can help your organization:

- **Understand** how to conduct threat modeling for cybersecurity and privacy
- **Establish a cybersecurity and privacy baseline** by leveraging the methodology and dataflows described in this guide
- **Identify and mitigate** threats with security controls and privacy safeguards

SOLUTION

To gain insights into actual processes and system designs, the NCCoE collaborated with stakeholders to solution illustrate how to perform threat modeling in a real-world genomic data processing scenario. The project used a multi-step approach to analyze system components and dataflows for possible threats, then map threats to taxonomies of tactics, techniques, and procedures. Privacy threat modeling analyses utilized the NIST Privacy Risk Assessment Methodology (PRAM) as well as LINDUNN. For cybersecurity threat modeling, the STRIDE technique identified threats to components and dataflows. These analysis findings were mapped to known taxonomies for cybersecurity and privacy resulting in a structured view of threats along with possible mitigations.

The approaches used in the solution support security and privacy standards and guidelines such as the NIST PRAM, NIST Privacy Framework, and NIST SP 800-53r5. This SP 1800-series uses technology and security capabilities (shown below) from our project partners.

SHARE YOUR FEEDBACK

You can view or download the SP 1800-series at https://www.nccoe.nist.gov/projects/cybersecurity-and-privacy-genomic-data. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for implementing the processes associated with this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at genomic_cybersecurity_nccoe@nist.gov.