National Cybersecurity Center of Excellence

NCCoE Virtual Workshop on Cybersecurity of Genomic Data

Wednesday, January 26, 2022, 11:00 AM – 4:30 PM (ET)

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

National Cybersecurity Center of Excellence

NCCoE Virtual Workshop on Cybersecurity of Genomic Data

Wednesday, January 26, 2022, 11:00 AM – 4:30 PM (ET)

This webinar is being recorded.

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

AGENDA

Segment	*Time*
Segment 1: Workshop Overview and Background	11:00 AM – 11:40 AM
Segment 2: Keynotes	11:40 AM – 12:20 PM
Segment 3: Challenges from the Field	12:20 PM – 12:50 PM
Intermission	12:50 PM – 1:30 PM
Segment 4: Challenges Sessions	1:30 PM – 2:25 PM
Break	2:25 PM – 2:35 PM
Segment 4 (Continued): Challenges Sessions	2:35 PM – 3:45 PM
Break	3:45 PM – 3:50 PM
Segment 5: Open Lightning Round	3:50 PM – 4:20 PM
Segment 6: Next Steps	4:20 PM – 4:30 PM

Welcome to the NCCoE Virtual Workshop on Cybersecurity of Genomic Data

Natalia Martin, NIST

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Virtual Workshop on the Cybersecurity of Genomic Data

Natalia Martin, Acting Director for National Cybersecurity Center of Excellence (NCCoE), NIST

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

About the NCCoE

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

WHO WE ARE

A **solution-driven**, **collaborative** hub addressing complex cybersecurity problems

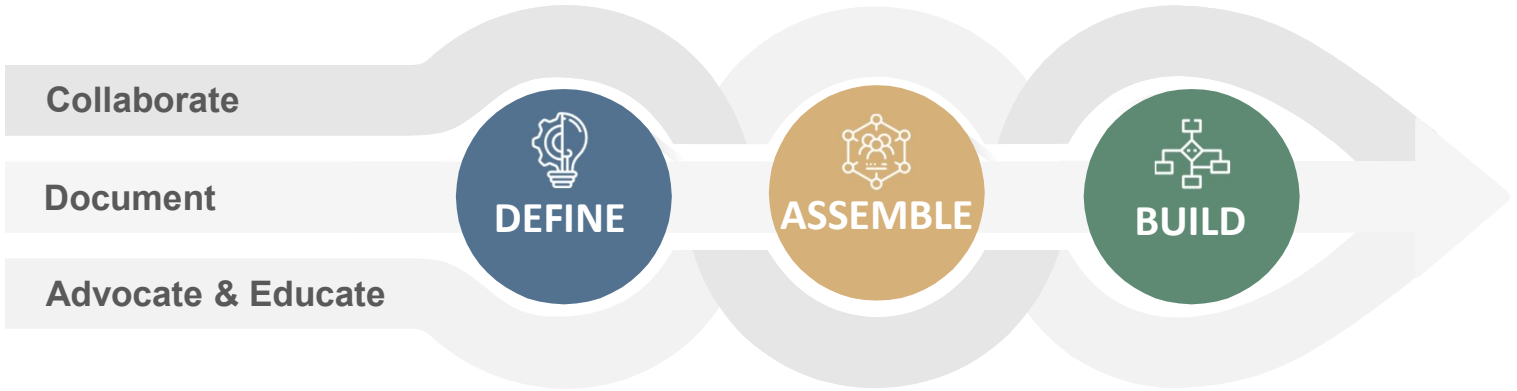
OUR GOALS

Improve cybersecurity for businesses and commerce

Lower the learning curve for cybersecurity

Spark innovation in secure technology

OUR APPROACH



Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

Build a practical, usable, repeatable implementation to address the cybersecurity challenge

Virtual Workshop on the Cybersecurity of Genomic Data

Workshop Overview

Ron Pulivarti, NIST

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Housekeeping

- We support the health and well being for all.
  - We are supporting virtual collaboration.
  - We have three breaks planned for the day.

- We want audience engagement.
  - Please pose your questions for today's workshop using the Q&A window.
  - Please voice your insights in the Open Lightening Round from 3:50 – 4:30 PM.

- We intend to share our learnings today.
  - We are recording this session for future post on the NCCoE Website.
  - We will summarize key insights.

NIST Experiences in Genomics, Cybersecurity, and Privacy

Samantha Maragh (NIST)
Naomi Lefkovitz (NIST)
Ron Pulivarti (NIST)

National Institute of Standards and Technology
U.S. Department of Commerce

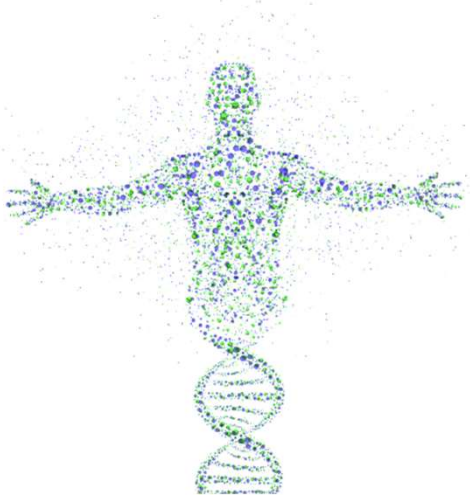
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Human Genomics at NIST

Samantha Maragh
Leader, Genome Editing Program

National Institute of Standards and Technology
U.S. Department of Commerce

The Human Genome



- The instruction code for humans
- ~6.4 billion letters long
- Present in each cell of a person
- ~ Half inherited from each biological parent
- Code is highly similar between people, but each person has a unique identifiable sequence

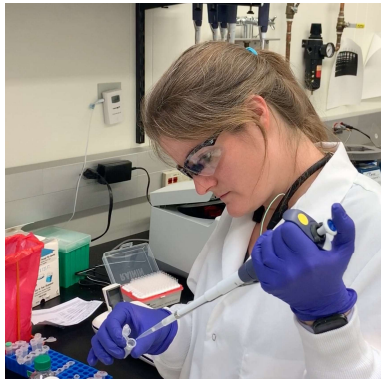
(Credit: Elymas/Shutterstock)

Uses of human genomic information

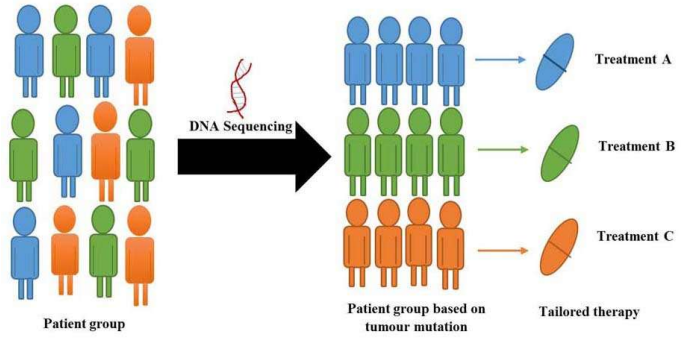
Human Identification

Population Diversity and Ancestry

Human Health: Diagnostics

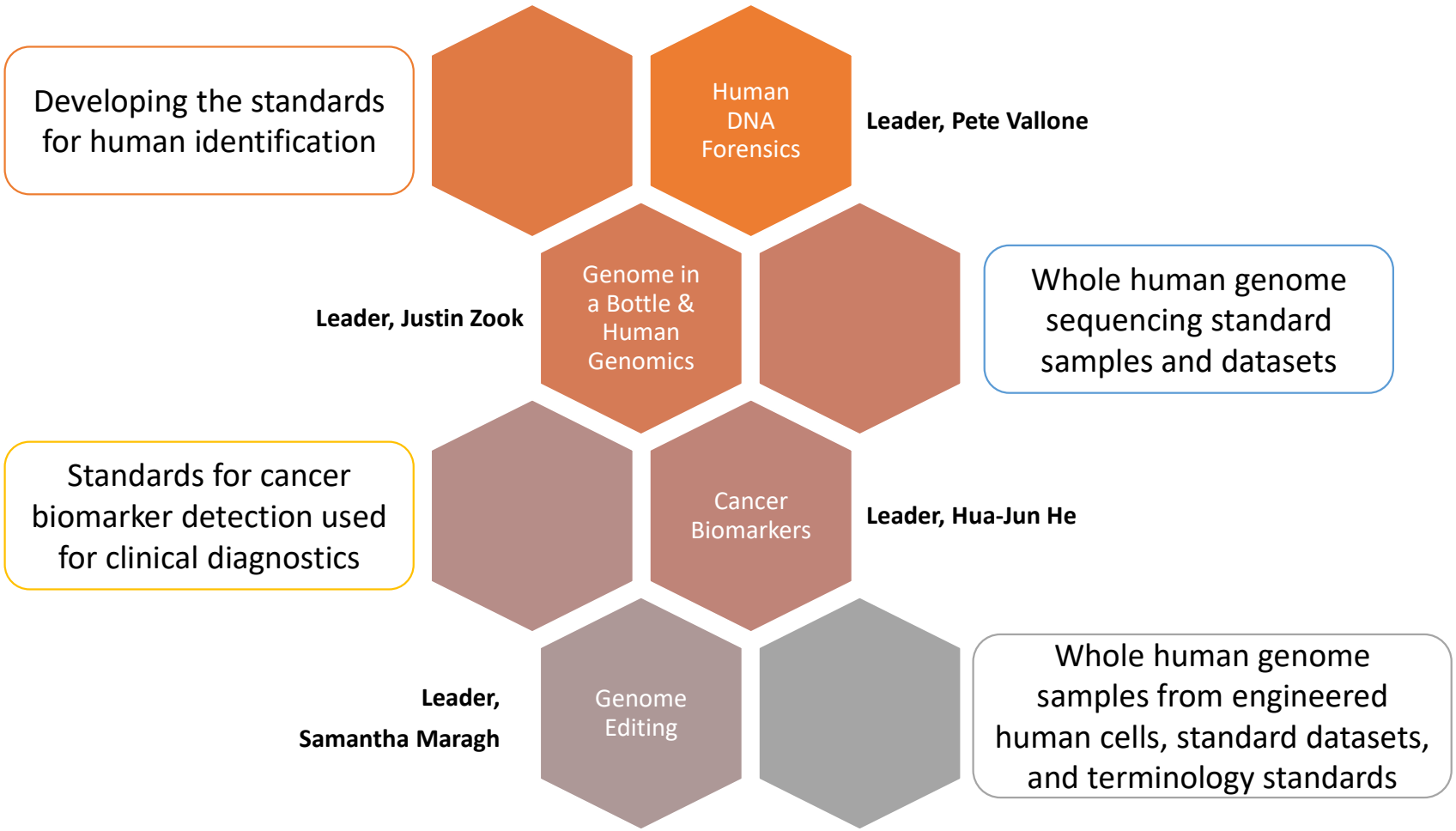


Scientific Research



Human Health: Treatment

NIST expertise with human genomics



NIST formed the Genome in a Bottle Consortium in 2012

GIAB has characterized variants in 7 human genomes and released NIST whole genome DNA standards

Pilot Genome NA12878

HG001*

AJ Trio

HG003* HG004*

HG002*

Chinese Trio

HG006 HG007

HG005*

National Institute of Standards & Technology

Report of Investigation

Reference Material 8391

Human DNA for Whole-Genome Variant Assessment
(Son of Eastern European Ashkenazim Jewish Ancestry)

This Reference Material (RM) is intended for validation, optimization, and process evaluation purposes. It consists of a male whole human genome sample of Eastern European Ashkenazim Jewish ancestry, and it can be used to assess performance of variant calling from genome sequencing. A unit of RM 8391 consists of a vial containing human genomic DNA extracted from a single large growth of human lymphoblastoid cell line GM24385 from the Coriell Institute for Medical Research (Camden, NJ). The vial contains approximately 10 µg of genomic DNA, with the peak of the nominal length distribution longer than 48.5 kb, as referenced by Lambda DNA, and the DNA is in TE buffer (10 mM TRIS, 1 mM EDTA, pH 8.0).

nature biotechnology

Resource | Published: 01 April 2019

An open resource for accurately benchmarking small variant and reference calls

Justin M. Zook, Jennifer McDaniel, Nathan D. Olson, Justin Wagner, Hemang Parikh, Haynes Heaton, Sean A. Irvine, Len Trigg, Rebecca Truty, Cory Y. McLean, Francisco M. De La Vega, Chunlin Xiao, Stephen Sherry & Marc Salit

nature biotechnology

Analysis | Published: 11 March 2019

Best practices for benchmarking germline small-variant calls in human genomes

Peter Krusche, Len Trigg, Paul C. Boutros, Christopher E. Mason, Francisco M. De La Vega, Benjamin L. Moore, Mar Gonzalez-Porta, Michael A. Eberle, Zivana Tezak, Samir Lababidi, Rebecca Truty, George Asimenos, Birgit Funke, Mark Fleharty, Brad A. Chapman, Marc Salit, Justin M. Zook & the Global Alliance for Genomics and Health Benchmarking Team

nature biotechnology

Resource | Published: 15 June 2020

A robust benchmark for detection of germline large deletions and insertions

Justin M. Zook, Nancy F. Hansen, [...] Marc Salit

PLOS COMPUTATIONAL BIOLOGY

OPEN ACCESS PEER-REVIEWED

RESEARCH ARTICLE

A crowdsourced set of curated structural variants for the human genome

Lesley M. Chapman, Noah Spies, Patrick Pai, Chun Shen Lim, Andrew Carroll, Giuseppe Narzisi, Christopher M. Watson, Christos Proukakis, Wayne E. Clarke, Naoki Nariai, Eric Dawson, Garan Jones, Daniel Blankenberg, [...], Justin M. Zook

Reference samples

The Harvard Personal Genome Project
seracare
NIST
Coriell Institute for Medical Research
horizon
ThermoFisher Scientific

Clinical Laboratories

INVITAE
AMP Association for Molecular Pathology
Personalis

Academic Laboratories

Baylor College of Medicine
Stanford Medicine
Johns Hopkins University
Harvard T.H. Chan School of Public Health

NGS technology developers

ThermoFisher Scientific
Oxford Nanopore Technologies
illumina
bionano Genomics
Complete Genomics
PacBio
10X Genomics
Nabsys

Government

National Institutes of Health
FDA*
NIST*
CDC

* Funders

Bioinformatics developers

Google
SevenBridges
Sentieon Precision Data for Precision Medicine
Arvados
verily
Roche
DNAnexus

***NIST RMs developed from large batches of DNA**

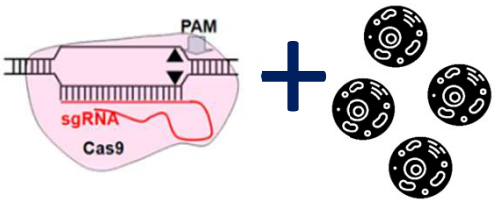
CRISPR technologies and uses

CRISPR-Cas

CRISPR - **C**lustered **R**egularly **I**nterspaced **S**hort **P**alindromic **R**epeats

Cas - **C**RISPR **as**sociated protein

CRISPR-Cas system were identified in nature as bacterial immune systems and have been pivoted to enable modification of the genetic code within cells at designed target positions (**genome editing)**

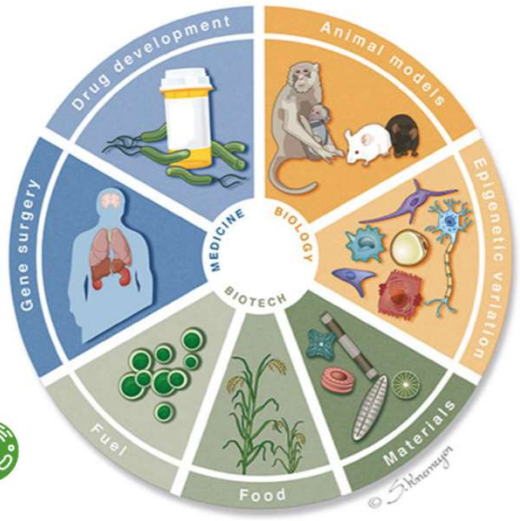


Genome Editing System (e.g., CRISR-Cas) designed to target genome sequence

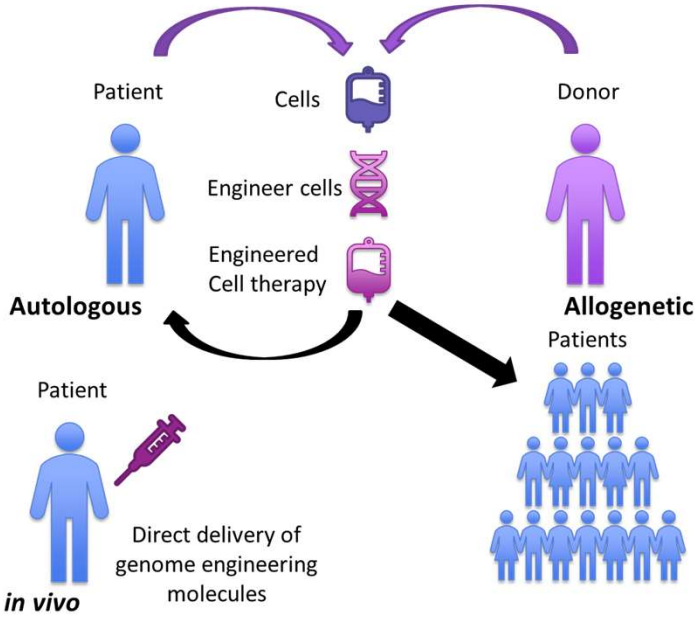
Cells of interest

DNA sequence change

Engineered/edited functional cells



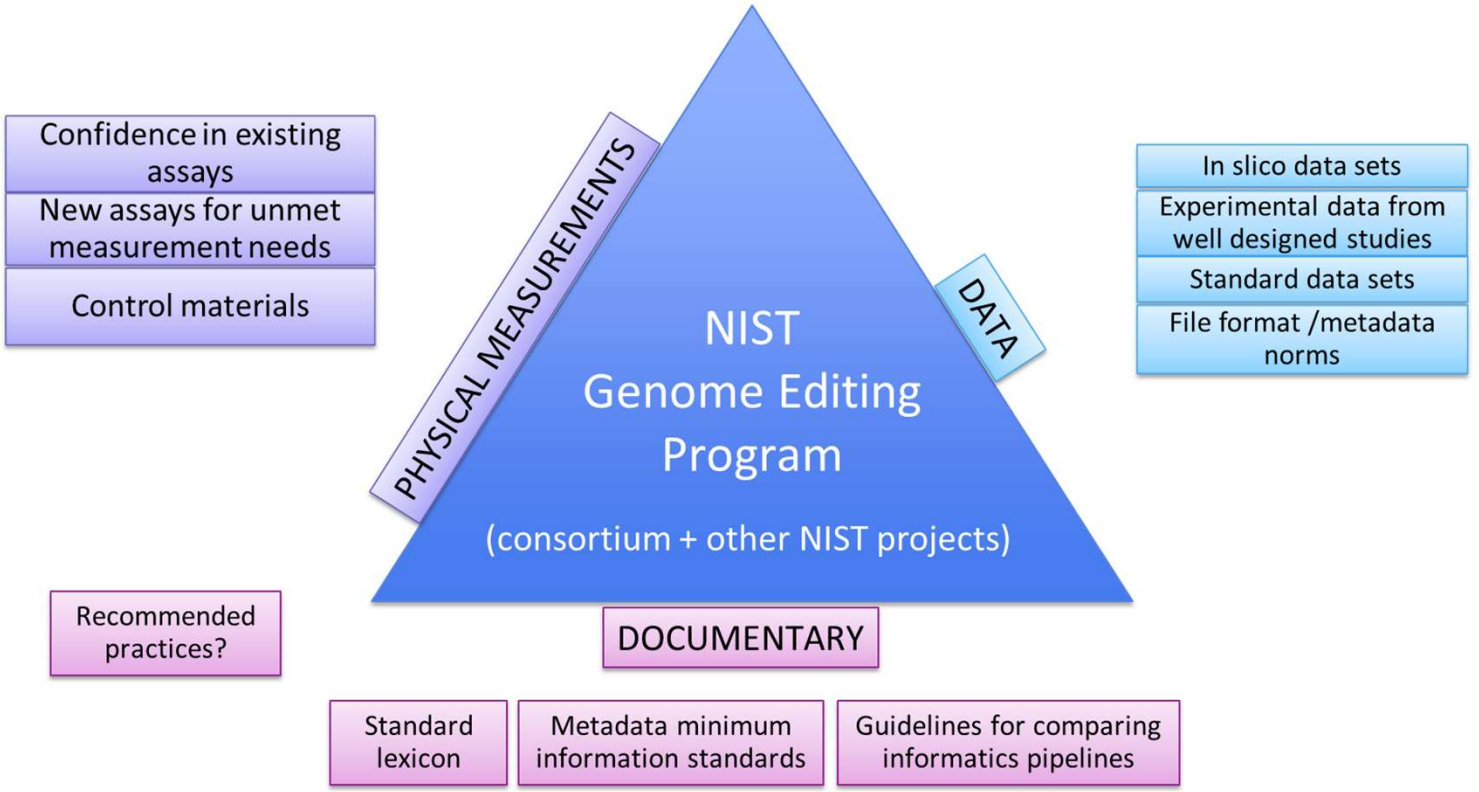
Human Gene Therapy applications



NIST experience with CRISPR technologies

Vision: Support quality in measurements for translating genome edited product to market

Goal: Develop measurement tools standards to increase the confidence of utilizing genome editing technologies in research and commercial products.

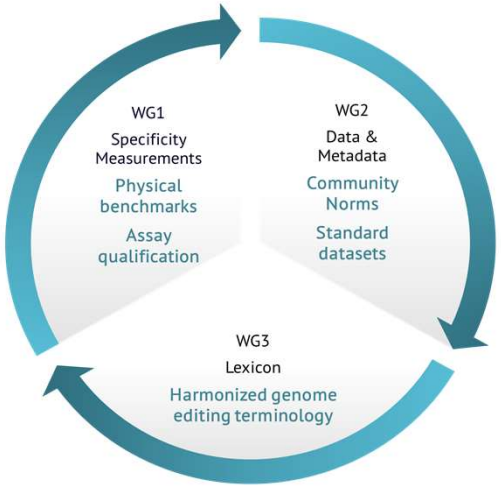


NIST Genome Editing Consortium
(launched October 2018)

MISSION

Convene experts across academia, industry, non-profit & government to addresses the measurements and standards needed to increase confidence of utilizing genome editing technologies in research and commercial products

ORGANIZATION



MEMBER BENEFITS

- Access to a neutral forum for addressing pre-competitive needs
- Participation in the development of experimental benchmarks, guidelines and terminology
- Access to tools developed by the consortium ahead of public release

MEMBERS

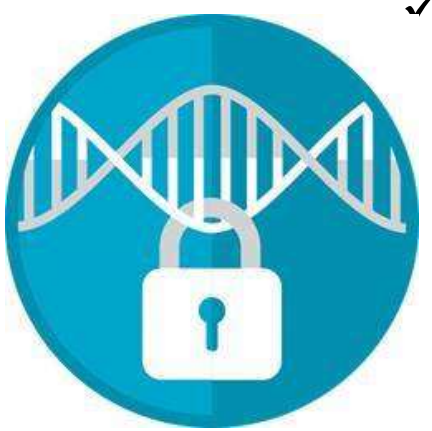
- Agilent
- Aldevron
- Applied StemCell
- AstraZeneca
- Bionano Genomics
- Bio-Rad
- Bluebird bio*
- Caribou Biosciences
- Catalytic Data Science
- Cergentis
- COBO Technologies
- **College of American Pathologists (CAP)**
- CRISPR Therapeutics
- DARPA
- DowDuPont Agroscience (Corteva)*
- Editas Medicine
- EMBL-EBI
- **FDA CBER**
- Genomic Vision
- Horizon Discovery
- Illumina
- Inscripta
- Integrated DNA Technologies
- Intellia Therapeutics
- KromaTiD
- Lonza
- Macrogen
- Mass General Hospital
- Mission Bio
- Novartis
- New England Biolabs
- NIH/NINDS
- NIH SCGE
- Precision Biosciences
- Sangamo Therapeutics
- SeQure Dx
- St. Jude Children's Research Hospital
- Synthego
- ThermoFisher Scientific
- Twinstrand Biosciences
- UCSC
- WhiteLab Genomics

NIST coordinates with FDA and Center for Veterinary Medicine (CVM)

Cost sharing model. All members contribute $20,000 annually or *in-kind*

* Former members

Importance of securing human genomics data



- ✓ Data integrity
- ✓ Data reliability
- ✓ Maintain limited access to individual genomic information
- ✓ Protect knowledge / intellectual property
- ✓ Data reusability / prevent loss
- ✓ Prevent against nefarious use or misuse
- ✓ Privacy

Credit: mcmurryjulie

Contact Us

Thank You!

Contact

Samantha Maragh
Leader, Genome Editing Program

Email address

samantha@nist.gov

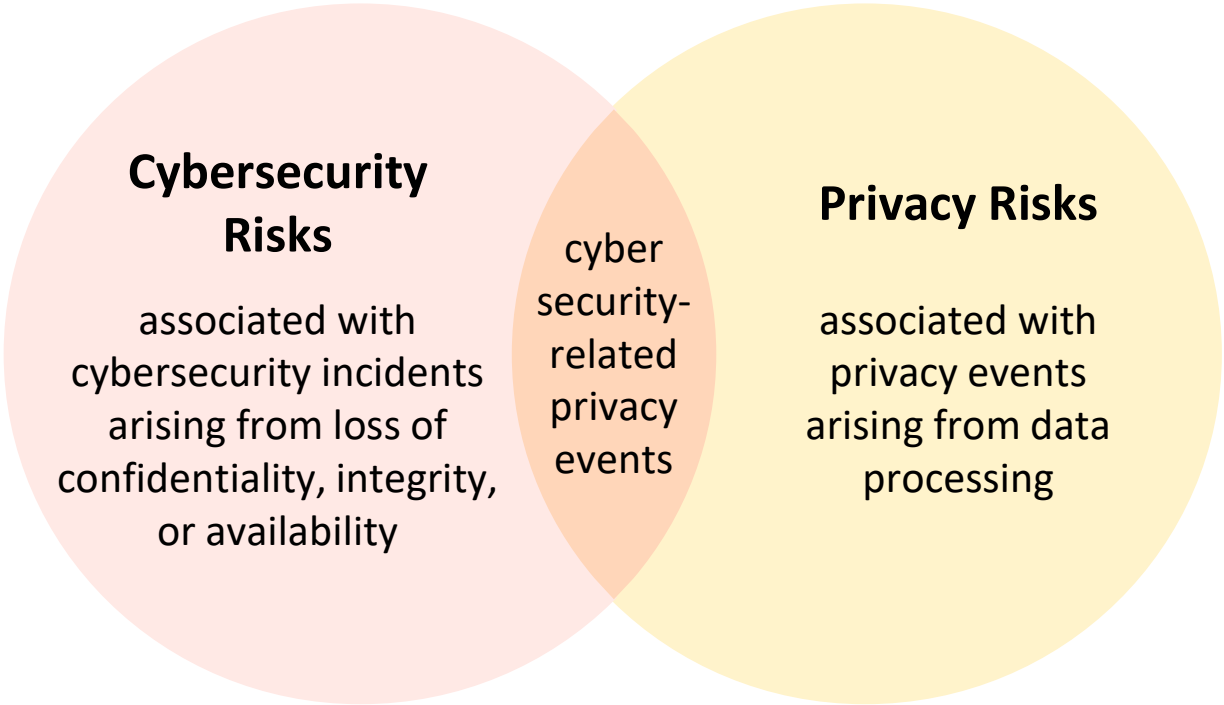
National Institute of Standards and Technology
U.S. Department of Commerce

Privacy at NIST

Naomi Lefkovitz

National Institute of Standards and Technology
U.S. Department of Commerce

Relationship Between Cybersecurity and Privacy Risk



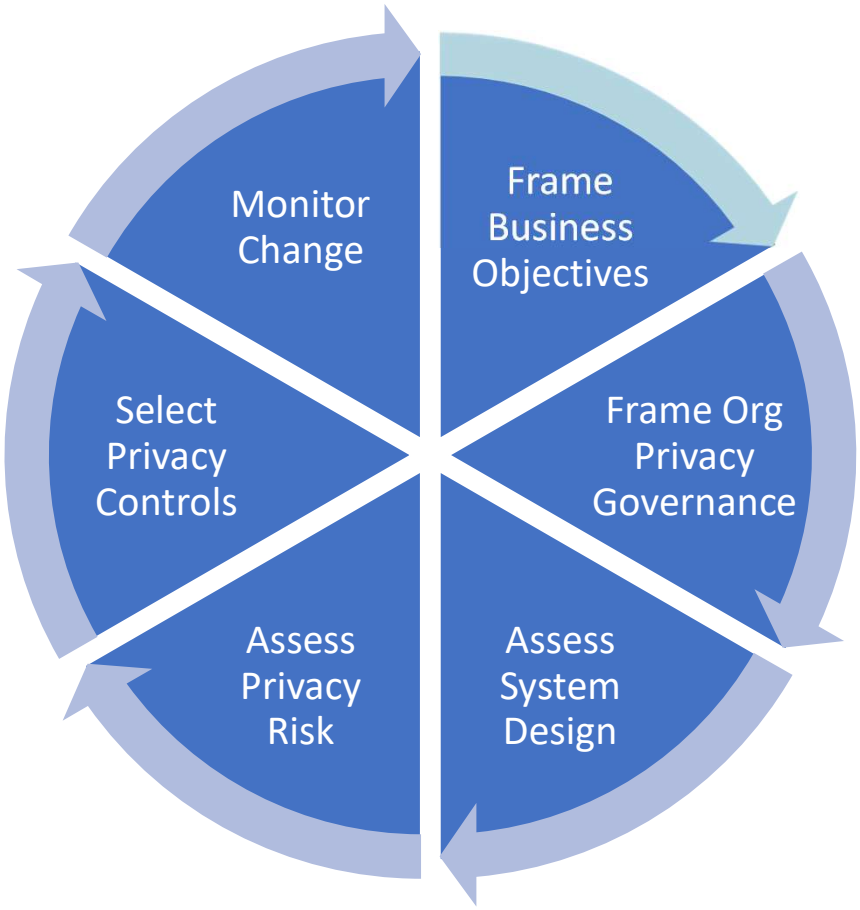
Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

NIST Privacy Risk Assessment Methodology (PRAM)



Catalog of Problematic Data Actions and Problems

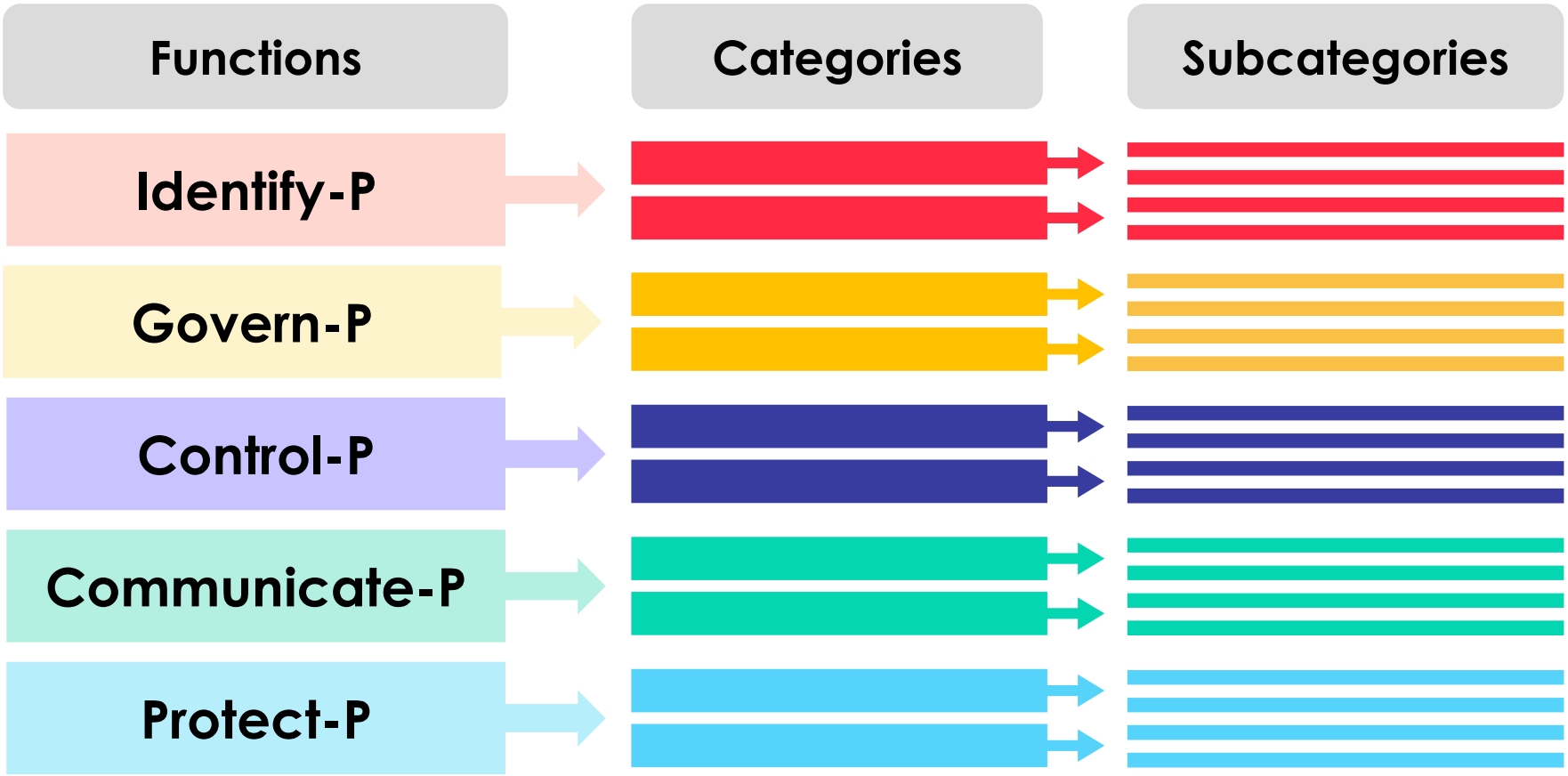
NIST Privacy Engineering Objectives

Predictability: enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service.

Manageability: providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.

Disassociability: enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

NIST Privacy Framework Core



Resources

Websites

https://www.nist.gov/privacyframework

Mailing List

List.nist.gov/privacyframework

Contact Us

PrivacyFramework@nist.gov

National Institute of Standards and Technology - Cybersecurity

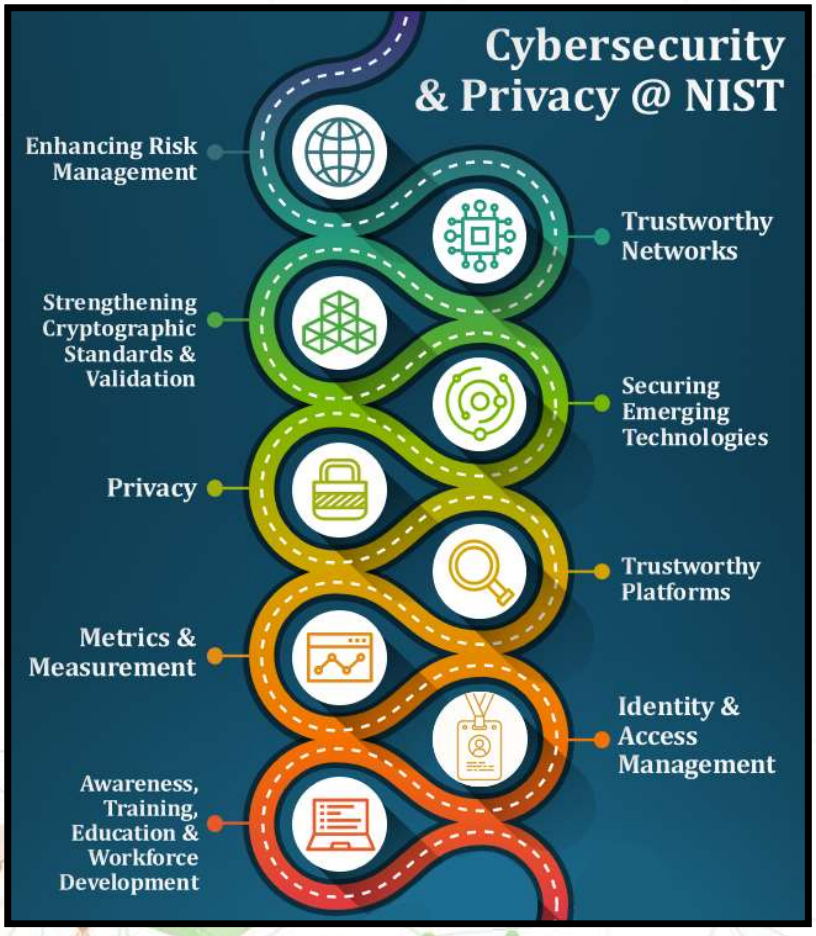
Ron Pulivarti, Senior Cybersecurity Engineer for the Healthcare Sector at the National Cybersecurity Center of Excellence (NCCoE), which is part of NIST

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



NINE PRIORITY AREAS:

Enhancing Risk Management

Trustworthy Networks

Strengthening Cryptographic Standards & Validation

Securing Emerging Technologies

Privacy

Trustworthy Platforms

Metrics & Measurement

Identity & Access Management

Awareness, Training, Education & Workforce Development

2014

Cybersecurity Framework released; Cybersecurity Enhancement Act assigns NIST workforce, other responsibilities

2016

NIST launches public key Post-Quantum Cryptography Standardization initiative

2018

Law designates NIST to Federal Acquisition Security Council, produce supply chain guidance

2019

NIST launches Small Business Cybersecurity Corner website following 2018 statute

2020

NIST produces IoT guidance per IoT Cybersecurity Improvement Act; NIST issues Security and Privacy Controls, Rev 5; NIST updates NICE strategic plan

2021

NIST launches effort to enhance software supply chain security in response to Executive Order and technology supply chain partnership

NIST Cybersecurity Framework 1.1

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

NIST Special Publication 800-160, Volume 2
Revision 1

Developing Cyber-Resilient Systems:

A Systems Security Engineering Approach

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

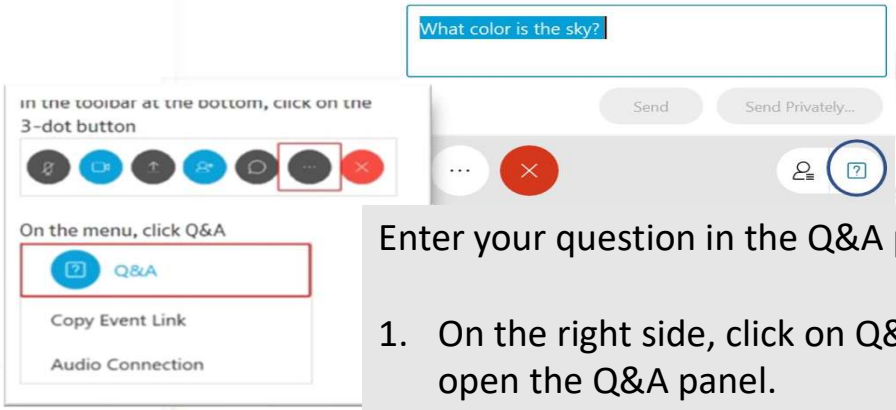
Thank You.


National Institute of
Standards and Technology
U.S. Department of Commerce


NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

NIST Experiences in Genomics, Cybersecurity, and Privacy

Moderated Questions and Answers



Enter your question in the Q&A panel.

1. On the right side, click on Q&A header to open the Q&A panel.
2. Type in the box **your name, organization and question**.
3. Click send.

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE