Welcome to the National Cybersecurity Center of Excellence

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Wednesday, May 18, 2022, 1:00 PM – 3:30 PM (EDT)

We will begin shortly.

This meeting will be recorded.

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Ron Pulivarti
NIST NCCoE

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Eric Lin
Director, Material Measurement Laboratory, NIST

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Robel Worku
Montgomery County Economic Development Corporation

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Priming the County's Economic Engine

Presented by Robel Worku
Economic Development Specialist

Montgomery County Economic Development Corporation

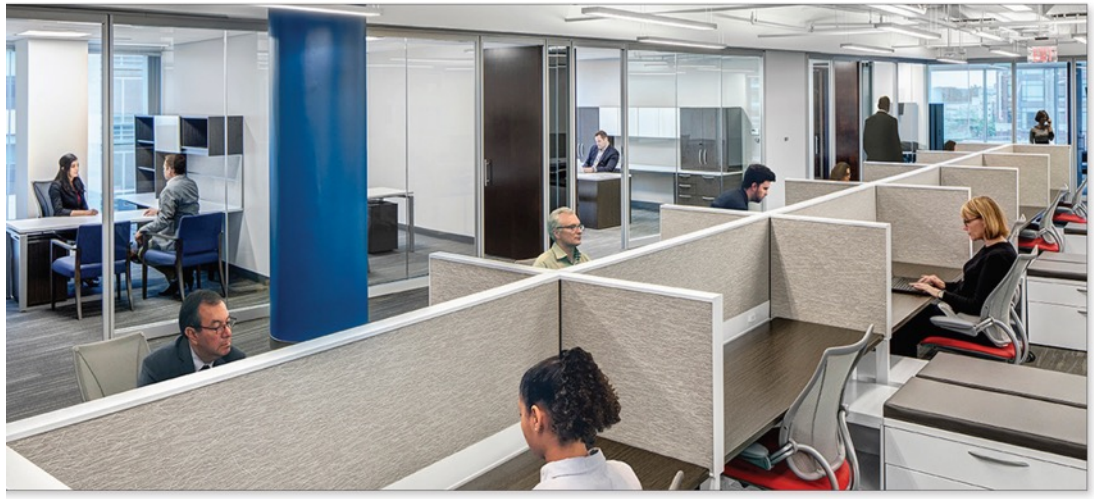
May 18th, 2022

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

About MCEDC

The **official public-private economic development organization** representing Montgomery County, MD

Led by a board of directors, our mission is to **help businesses start and grow in the county, or help companies relocate here**



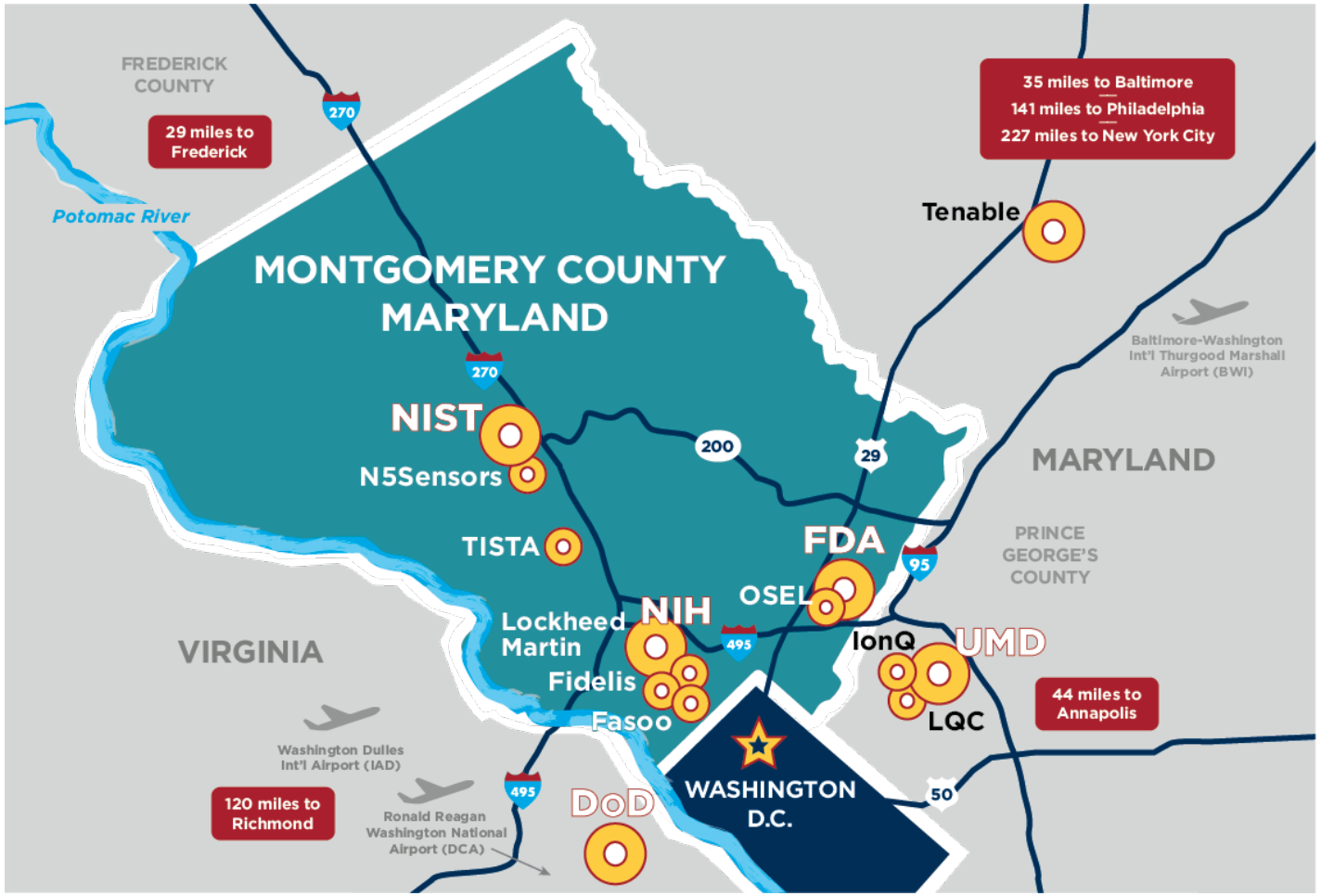
How does MCEDC help?
We help make connections to:

- Gain market intelligence
- Link business owners to aligned partnerships
- Find the ideal business address
- Explore available incentives
- Attract talent and help with workforce training
- Help companies relocate here

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

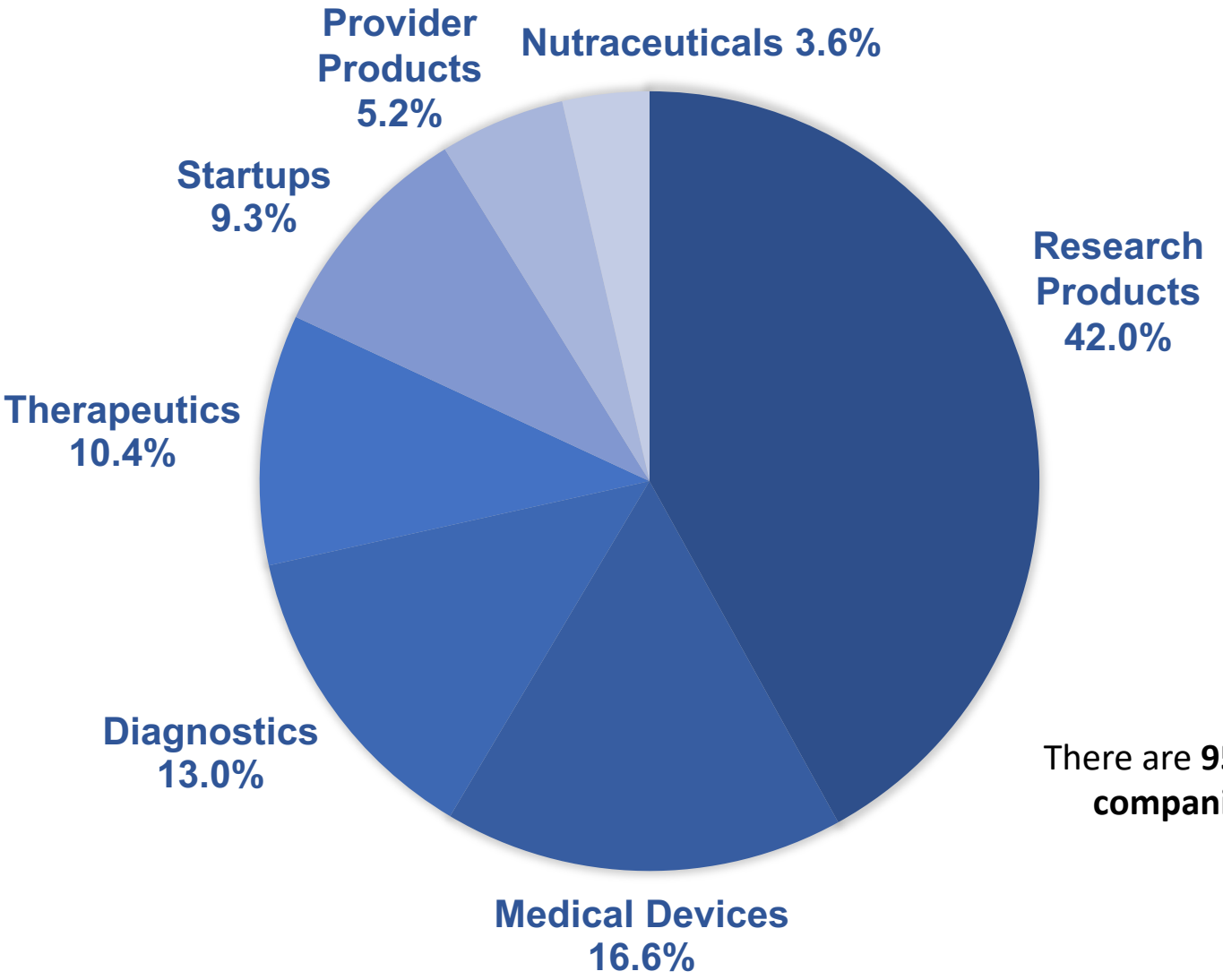
Big Data Capital Next to the Nation's Capital

Partial list of federal assets and local companies



MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

Distribution of 800+ BioHealth Companies in Montgomery County



There are **95+ Medical Device companies** in Maryland

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

MONTGOMERY COUNTY
LIFE SCIENCES INVESTMENTS

Over **$1 billion** in Venture Capital raised since 2015

Over **$245 billion** market cap of companies with global or U.S. headquarters in Montgomery County

gsk GlaxoSmithKline
QIAGEN
AstraZeneca
PRECIGEN
ADAPTIVE PHAGE THERAPEUTICS
janssen
INSILICO MEDICINE
United Therapeutics
BeneVir
NEURALY
VIELABIO
CERECOR
Senseonics
emergent biosolutions
Vigene Biosciences
REGENXBIO
ARCELLX
sirnaomics Advancing RNAi Therapeutics
Supernus Pharmaceuticals

Examples of companies using Big Data

COMPANY USING SUPERCOMPUTERS IN DRUG DISCOVERY

Gain Therapeutics is a preclinical biotechnology company focused on developing new medicines for protein misfolding diseases. Gain's supercomputer-driven, target-based drug discovery platform, "SEE-Tx™," is a novel approach that uses a convergence of Computational Biology and Supercomputing to discover previously unidentified allosteric binding sites.

COMPANY LOOKING FOR ADVANCED COMPUTATIONAL METHODS AND HARDWARE TO SOLVE BIG DATA PROBLEMS IN BIO

EzBiome The Gaithersburg company uses data and databases-driven precision taxonomy with the world's largest curated reference database, and advanced computational platform built-on cutting-edge genomic intelligence.

Helping in Pandemic Recovery Efforts

During the pandemic, in addition to ongoing business support, MCEDC has pivoted to help the economic recovery for our businesses. Support grant programs include:

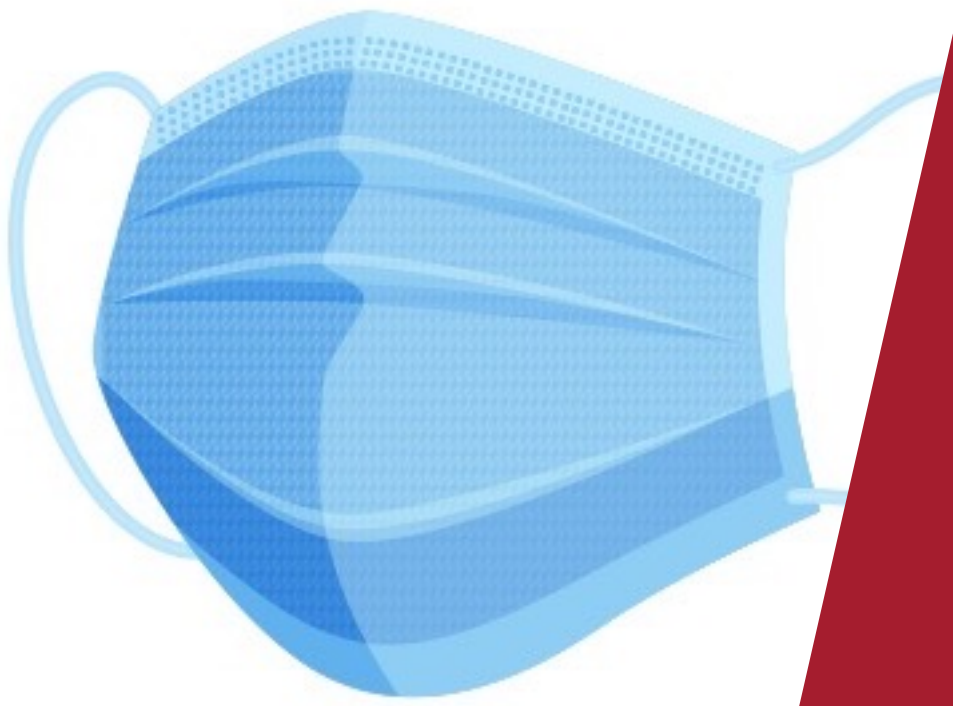
Bio Lab Pilot – $96,000 grant program to six small life science companies (administered pre-pandemic)

Restaurant Relief Fund – 3 rounds of relief for a total of $16.5M dollars distributed to over 900 restaurants

Telework Fund – $1M to help businesses purchase telework equipment and software

Local Production Fund – $200,000 fund to help businesses pivot to making Personal Protection Equipment (PPE) to support local pandemic needs

3R Initiative Restaurant & Retail Grants – $1M program to assist restaurants and retailers before the 2020 holiday season and winter



Major Industries

thinkmoco.com/key-industries

BioHealth and Life Sciences

Cybersecurity

Tech & Quantum Computing

Advanced Manufacturing

Hospitality & Tourism

Financial Services

Agribusiness

Nonprofits

Click on images to download

MONTGOMERY COUNTY, MARYLAND (MoCo)

THE IMMUNIZATION CAPITAL NEXT TO THE NATION'S CAPITAL

FUNDING MAGNET

$365 Billion market cap of companies with global or U.S. HQs in MoCo

$8 Billion in 2020 funding secured by MoCo Bio companies

THE POWER OF OUR FEDERAL PRESENCE

$1 Trillion annual budget Centers for Medicare and Medicaid Services (CMS) nearby in Baltimore, MD

$41 Billion annual budget National Institutes of Health (NIH)

$5 Billion annual budget Food and Drug Administration (FDA)

18 Federal Agency Headquarters located in Montgomery County, Maryland

$1.6 Trillion annual spend from the Hub of Global Healthcare

$3 Billion+ invested in MoCo biotech companies for coronavirus vaccine development and production

THE TALENT CAPITAL

300+ Bio companies

40,000 life science workers

59% of adults over 25 have a Bachelor's Degree or higher

#1 Maryland has the highest concentration of STEM jobs of any state in the U.S.

#2 Maryland is one of the top states for professional and technical workers

31.8% of adults over 25 with a Master's Degree or higher (highest of all counties with more than 1M residents)

Reach out to us to grow in Montgomery County, Maryland

connect@thinkmoco.com

MONTGOMERY COUNTY ECONOMIC DEVELOPMENT CORPORATION MARYLAND

1801 Rockville Pike, Suite 320, Rockville, MD 20852 | 240.641.6700 | thinkmoco.com

CYBER INNOVATION THRIVES HERE

MONTGOMERY COUNTY, MARYLAND

Grow with us in the region that's home to the nation's top security agencies and powerful intelligence communities. Draw from our top talent. Maryland is #1 in concentration of STEM jobs and one of the highest density locations for cyber engineers. We have the resources, technology and network to help your company serve federal institutions and private companies.

Our prime location is central to NSA, CIA, DoD and numerous other federal and military institutions. We are a top state for cyber talent. It's all here next to the nation's capital Montgomery County, Maryland.

#1 STEM job concentration*

#1 share of all high-tech businesses*

17 certified NSA/DHS CAEs*

$558M VC cyber investment in '20*

Top names in cybersecurity call Maryland their home in 2020

NORTHROP GRUMMAN, leidos, LOCKHEED MARTIN, tenable, TIBITS, KOOLSPAN, Fidelis, FAS00, ZEROFOX, Booz | Allen | Hamilton

ACCESS OUR FEDERAL ASSETS

IN MONTGOMERY COUNTY

18 Federal Agency HQs Including NIST, NIH & FDA

38 Federal Labs

The National Cybersecurity Center of Excellence (NCCoE)

IN GREATER MD, D.C. AND VA

60 Federal Government Agencies

The U.S. Cyber Command Center

The National Security Agency

The Central Intelligence Agency

74 Federal Labs

20 Military Facilities

FEDERAL SPENDING

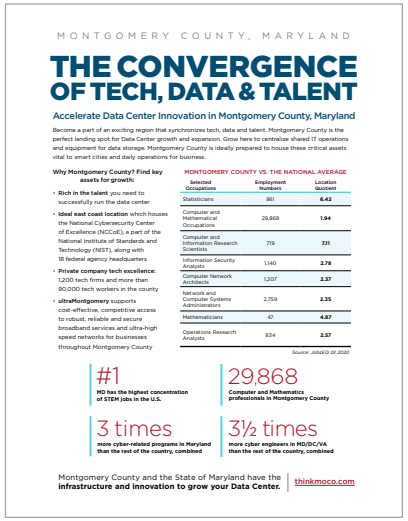
$17.4 Billion* Cyber-related activities

$9.6 Billion* Largest is Dept. of Defense

Gain proximity to major federal agencies

MONTGOMERY COUNTY ECONOMIC DEVELOPMENT CORPORATION MARYLAND

*Maryland Commerce *Federal FY 2020 Cybersecurity Funding



MONTGOMERY COUNTY, MARYLAND

THE CONVERGENCE OF TECH, DATA & TALENT

Accelerate Data Center Innovation in Montgomery County, Maryland

Become a part of an exciting region that synchronizes tech, data and talent. Montgomery County is the perfect landing spot for Data Center growth and expansion. Grow here to centralize shared IT operations and equipment for data storage. Montgomery County is ideally prepared to house these critical assets vital to smart cities and daily operations for business.

Why Montgomery County? Find key assets for growth:

- **Rich in the talent** you need to successfully run the data center
- **Ideal east coast location** which houses the National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), along with 18 federal agency headquarters
- **Private company tech excellence:** 1,200 tech firms and more than 90,000 tech workers in the county
- **ultraMontgomery** supports cost-effective, competitive access to robust, reliable and secure broadband services and ultra-high speed networks for businesses throughout Montgomery County

MONTGOMERY COUNTY VS. THE NATIONAL AVERAGE

Selected Occupations	Employment Numbers	Location Quotient
Statisticians	861	6.43
Computer and Mathematical Occupations	29,868	1.94
Computer and Information Research Scientists	719	7.11
Information Security Analysts	1,140	2.78
Computer Network Architects	1,207	2.37
Network and Computer Systems Administrators	2,759	2.35
Mathematicians	47	4.87
Operations Research Analysts	834	2.57

Source: JobsEQ Q1 2020

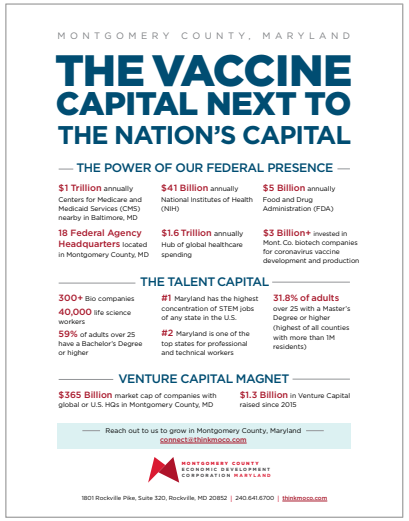
#1 MD has the highest concentration of STEM jobs in the U.S.

29,868 Computer and Mathematics professionals in Montgomery County

3 times more cyber-related programs in Maryland than the rest of the country, combined

3½ times more cyber engineers in MD/DC/VA than the rest of the country, combined

Montgomery County and the State of Maryland have the **infrastructure and innovation to grow your Data Center.** | thinkmoco.com



MONTGOMERY COUNTY, MARYLAND

THE VACCINE CAPITAL NEXT TO THE NATION'S CAPITAL

THE POWER OF OUR FEDERAL PRESENCE

$1 Trillion annually Centers for Medicare and Medicaid Services (CMS) nearby in Baltimore, MD

$41 Billion annually National Institutes of Health (NIH)

$5 Billion annually Food and Drug Administration (FDA)

18 Federal Agency Headquarters located in Montgomery County, MD

$1.6 Trillion annually Hub of global healthcare spending

$3 Billion+ invested in Mont. Co. biotech companies for coronavirus vaccine development and production

THE TALENT CAPITAL

300+ Bio companies

40,000 life science workers

59% of adults over 25 have a Bachelor's Degree or higher

#1 Maryland has the highest concentration of STEM jobs of any state in the U.S.

#2 Maryland is one of the top states for professional and technical workers

31.8% of adults over 25 with a Master's Degree or higher (highest of all counties with more than 1M residents)

VENTURE CAPITAL MAGNET

$365 Billion market cap of companies with global or U.S. HQs in Montgomery County, MD

$1.3 Billion in Venture Capital raised since 2015

Reach out to us to grow in Montgomery County, Maryland

connect@thinkmoco.com

MONTGOMERY COUNTY ECONOMIC DEVELOPMENT CORPORATION MARYLAND

1801 Rockville Pike, Suite 320, Rockville, MD 20852 | 240.641.6700 | thinkmoco.com

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

THANK YOU

Visit us at thinkmoco.com

robel@thinkmoco.com

Sign up for our newsletter for ongoing business news and support
Send us your updates so we can help promote your business — email us at connect@thinkmoco.com

Workshop Overview

Ron Pulivarti, NIST NCCoE

WHO WE ARE

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

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe a procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE.

PAST WORK: NCCOE VIRTUAL WORKSHOP ON THE CYBERSECURITY OF GENOMIC DATA

https://www.nccoe.nist.gov/projects/cybersecurity-genomic-data

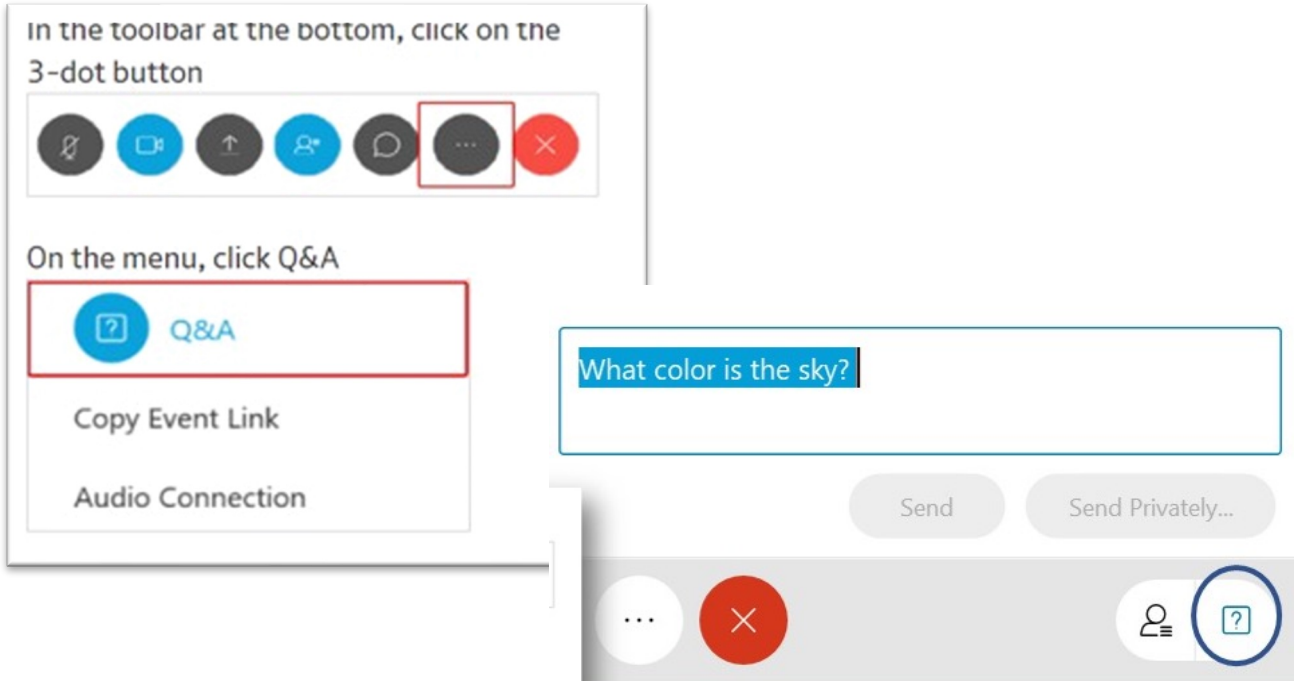
AGENDA: MAY 18

Segment	*Time (EDT)*
Workshop Overview	1:00 PM – 1:15 PM
Session One: Genomic Sequencer Device Security	1:15 PM – 2:15 PM
Break	2:15 PM – 2:30 PM
Session Two: Securing Sensitive Human Data in support of Genomics Research	2:30 PM – 3:25 PM
Wrap Up	3:25 PM – 3:30 PM

Audience Engagement

Please use the Q&A window to enter your questions for today's workshop. We will do our best to answer the questions in real time.

1. On the right side, click on Q&A header to open the Q&A panel.
2. Type your question in the box, along with your name and organization.
3. Click **send**.
4. We will answer as many questions as we are able during Q&A sessions.



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 a 15-minute break planned for the day.

- We want audience engagement.
  - Please pose your questions for today's workshop using the Q&A window.

- We intend to share our learnings today.
  - We are recording this session for future post on the NCCoE Website.
  - We will post the speaker slides and recording on the NCCoE Website.

This meeting is being recorded.

Genomic Sequencer Device Security

Paul Watrobski (NIST)
Blaine Mulugeta (MITRE)
Charles Fracchia (BIO-ISAC)
Phillip Whitlow (HudsonAlpha)

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Session Overview

Segment	*Time*
Overview and Introduction of Panelists	20 minutes
NIST/NCCoE IoT/MUD Project Overview	
Bio-ISAC Introduction	
HudsonAlpha Introduction	
Panel Discussion • Current approaches to bio-security of devices • Future use of MUD for sequencers • Future need for sequencer security baselines	30 minutes
Q&A	10 minutes

Cybersecurity Challenges

Securing Genetic Sequencers

What's driving the need for solutions?

Sequencers are essentially IoT devices connected to the enterprise network

- Accessible and remotely managed
- Connected systems and infrastructure
- Proprietary hardware and software
- Limited configuration standards
- Increased complexity and data volumes

Panelists

Paul Watrobski – NIST
Blaine Mulugeta – MITRE
Charles Fracchia – BIO-ISAC
Phillip Whitlow – HudsonAlpha

National Cybersecurity Center of Excellence

NCCoE Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

- Paul Watrobski (NIST)
- Blaine Mulugeta (MITRE)

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

What is/Why MUD?

MITIGATING NETWORK-BASED ATTACK USING MUD

Challenge

- Internet connected devices that are not intended to be used for general purpose computing tasks and have a very specific purpose aren't always capable of protecting themselves (e.g., Genomic Sequencers, IoT devices, etc.)
- Device security may not be a priority due to processing, timing, memory, and power constraints
- Typically, these devices are given full connectivity to the internet by default
- Networked devices can be detected within minutes and exploited due to known security flaws, leading to easily scalable attacks

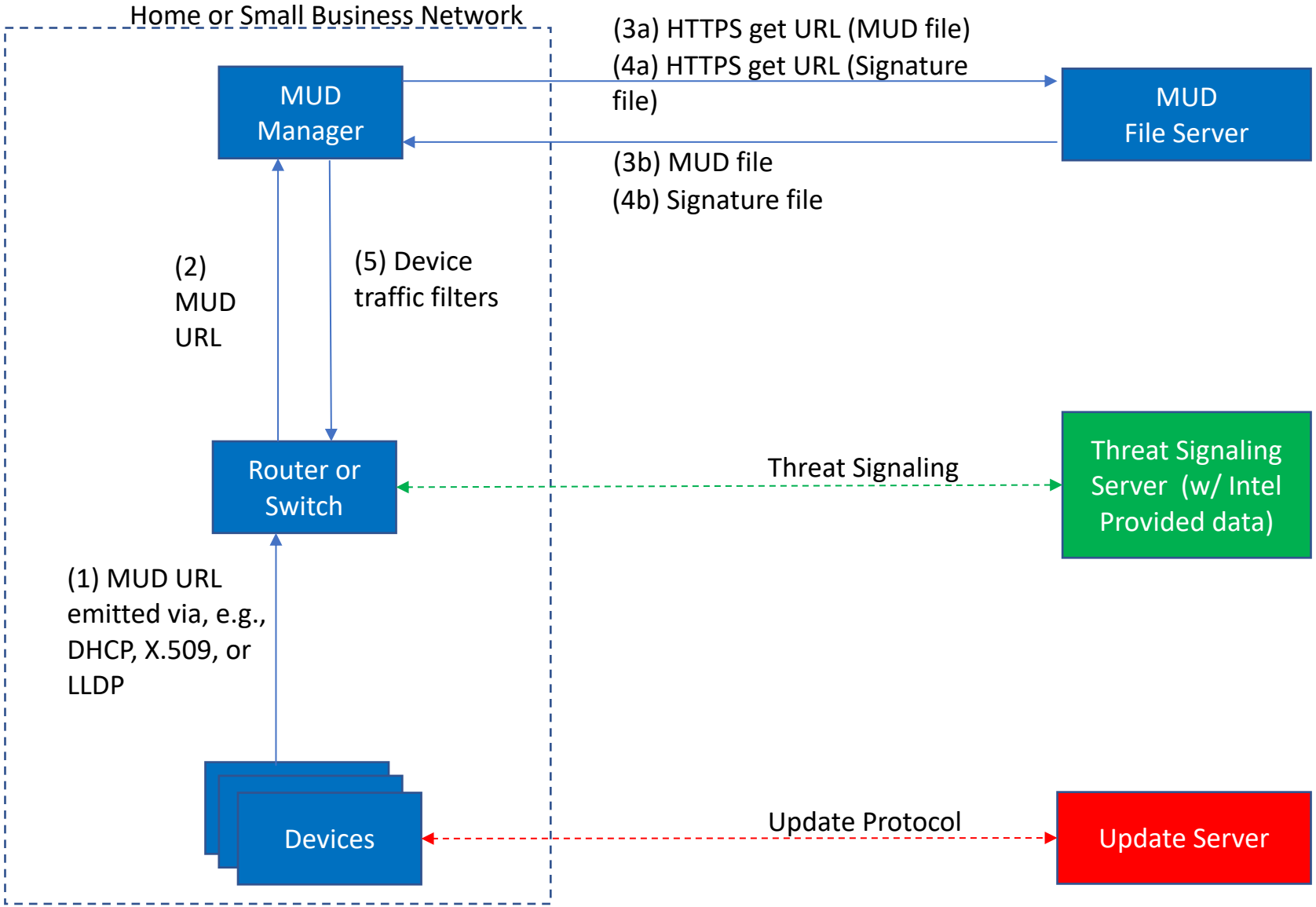
Solution

- Since these devices have a small number of communication patterns which follows from those small number of uses, the combination of these two statements has been coined Manufacturer Usage Description (MUD) that can be applied at various points within a network.
- MUD enables a network to limit a device's communication within the local network and externally to only those needed and intended by the manufacturer's design.
- MUD primarily addresses threats to the device rather than treating the device as a threat
- Use network gateway components and security-aware devices that leverage the MUD Specification (RFC 8520)

Reference: https://datatracker.ietf.org/doc/html/rfc8520

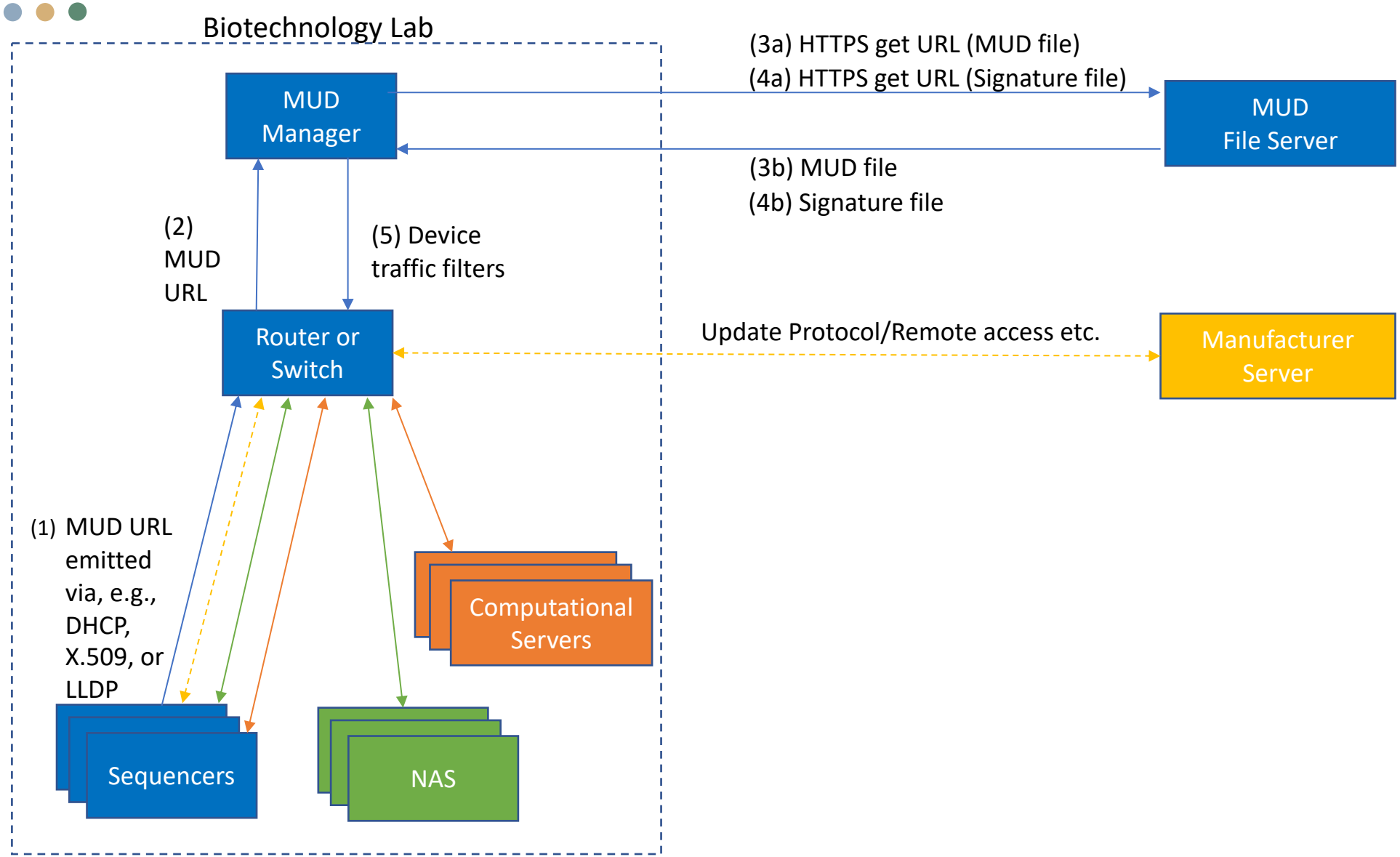
Architecture Overview

MITIGATING NETWORK-BASED ATTACKS USING MUD - REFERENCE ARCHITECTURE



Reference: https://www.nccoe.nist.gov/projects/securing-home-iot-devices-using-mud

SEQUENCER EXAMPLE ARCHITECTURE



BIO-ISAC

Securing the bioeconomy

Charles Fracchia

bioisac
Creating Collaborative Threat Intelligence for the Bioeconomy

NIST NCCOE
18 MAY 2022

Overview: BIO-ISAC

BIO-ISAC was founded to address the demand & meet the rising needs of the bioeconomy community.

BIO-ISAC is an international organization that addresses threats unique to the bioeconomy and enables coordination among stakeholders to facilitate a robust and secure industry. **https://isac.bio**

BIO-ISAC Mission - in a nutshell

Provide concrete solutions to “all hazards” affecting the bioeconomy.

BIO-ISAC Benefit - Free Emergency Threat Hunting

WIRED SIGN IN

LILY HAY NEWMAN SECURITY MAY 12, 2022 8:30 AM

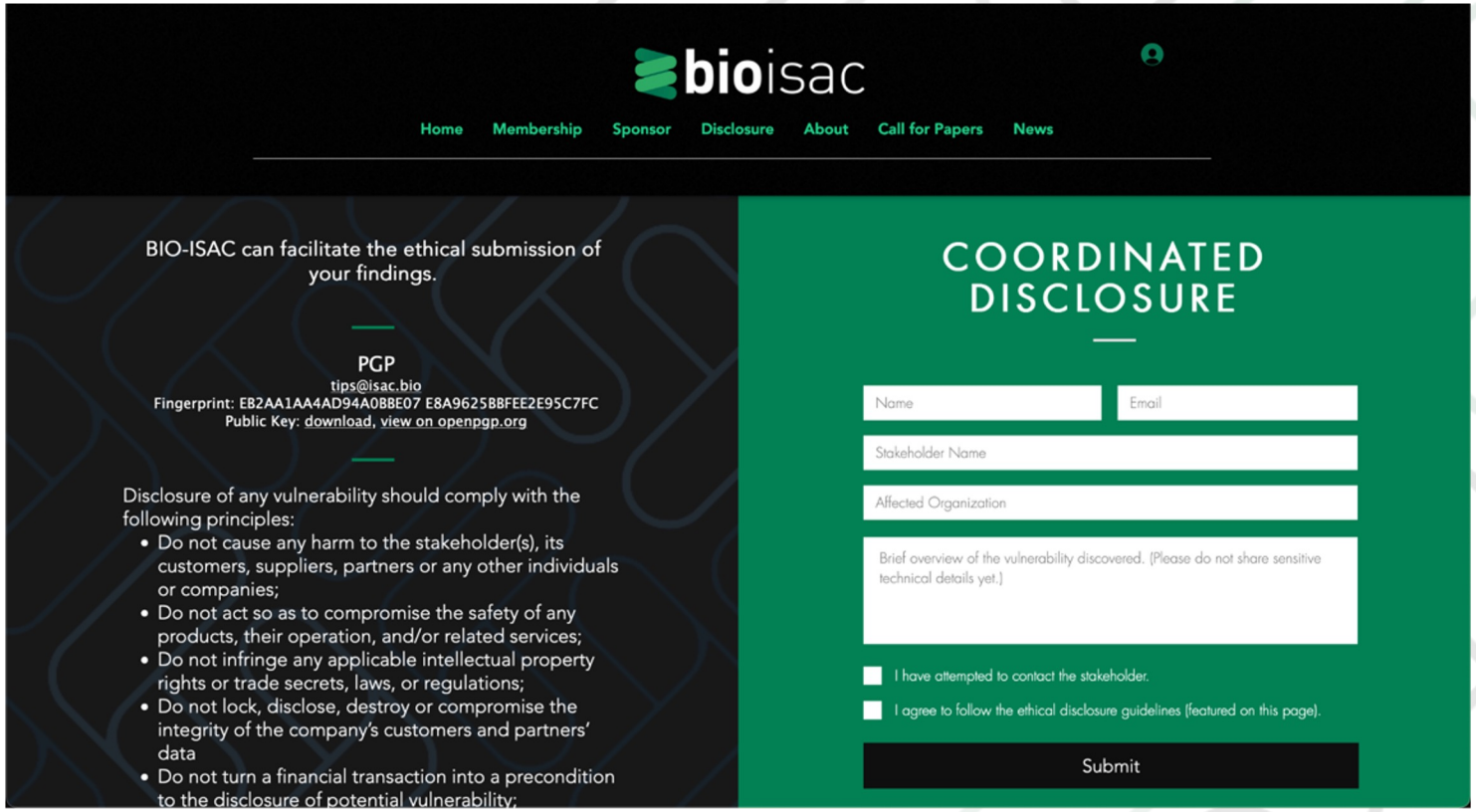
The Hidden Race to Protect the US Bioeconomy From Hacker Threats

A biotech threat intelligence group is gaining supporters as urgency mounts around an overlooked vulnerable sector.

Contribute disclosures

Have discovered a vulnerability or issue with your bioindustrial, lab, agro, analytical, pre-clinical or other systems?

BIO-ISAC can help you responsibly disclose the vulnerability and get it addressed.



https://isac.bio/disclosure

Thank you

bioisac
Creating Collaborative Threat Intelligence for the Bioeconomy

Prepared for NIST NCCOE
18 MAY 2022

HUDSONALPHA
INSTITUTE FOR BIOTECHNOLOGY

Phillip Whitlow

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Who is HudsonAlpha?

HudsonAlpha Institute for Biotechnology is a nonprofit institute founded in 2008 and is a national and international leader in genetics and genomics research and biotech education.

Tens of thousands of genomes (human and non-human) sequenced per year on campus

Sequencing use cases include:

- Genetic testing and whole genome sequencing to diagnose patients with rare and/or hard to diagnose genetic illnesses
- Clinical genome sequencing for labs, healthcare institutions, and physicians for diagnostics and treatment of patients
- Developing customized genomic screening programs for patient and employee populations of health systems, physician networks, and self-insured employers
- Original sequencing of plants to facilitate improvements in food production and biofuel research among others

We also host more than 50 associate companies on our campus - all of them involved in bioscience and many performing genomic sequencing in their own labs

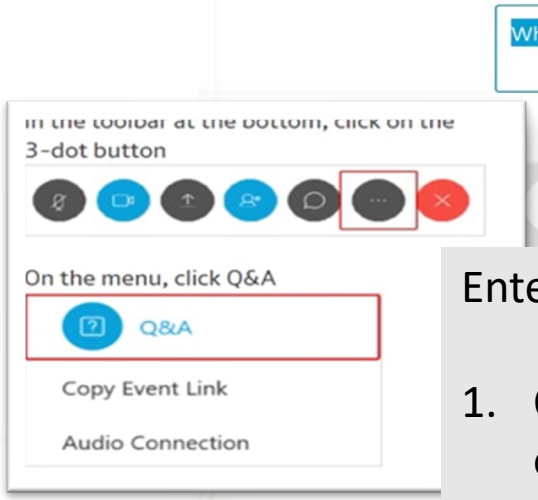
HUDSONALPHA
INSTITUTE FOR BIOTECHNOLOGY

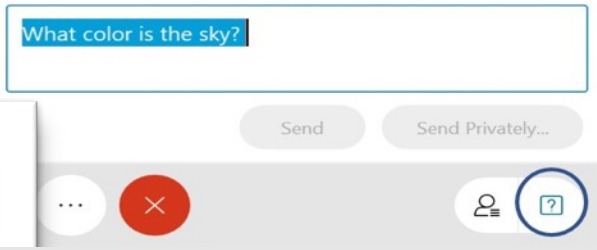
Panel Discussion

Paul Watrobski - NIST
Blaine Mulugeta - MITRE
Charles Fracchia - BIO-ISAC
Phillip Whitlow - HudsonAlpha

Genomic Sequencer Device Security

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.

Break

Enjoy your break.
We'll start again soon!

2:30 PM

Coming up next!

TOPIC	PRESENTERS
Session Two: Securing Sensitive Human Data in support of Genomics Research	Mike Feolo (NIH) Kurt Rodarmer (NIH)

Welcome Back!

This meeting is being recorded.

Securing Sensitive Human Data in support of Genomics Research

Mike Feolo (NIH)
Kurt Rodarmer (NIH)

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Securing Sensitive Human Data in support of Genomics Research

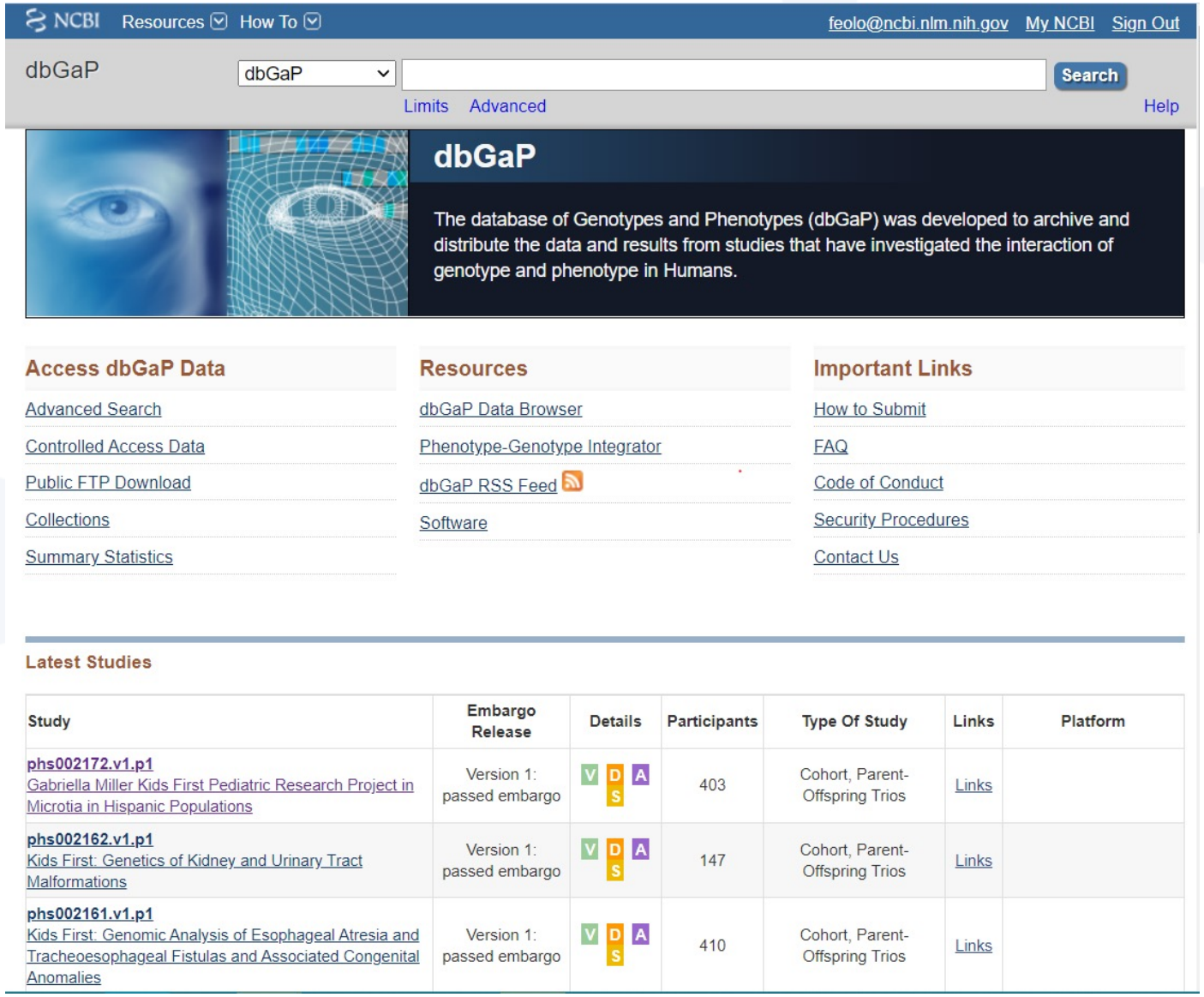
May 18, 2022

Michael Feolo
dbGaP Team Lead
NIH/NLM/NCBI

Kurt W. Rodarmer
RAS Security Advisory Group
National Institutes of Health, NLM/NCBI

dbGaP: The database of Phenotypes and Genotypes

- Permanent Archive
- Versioned Releases
- Public Metadata
- Controlled Access



High Level Data Model

A dbGaP Study

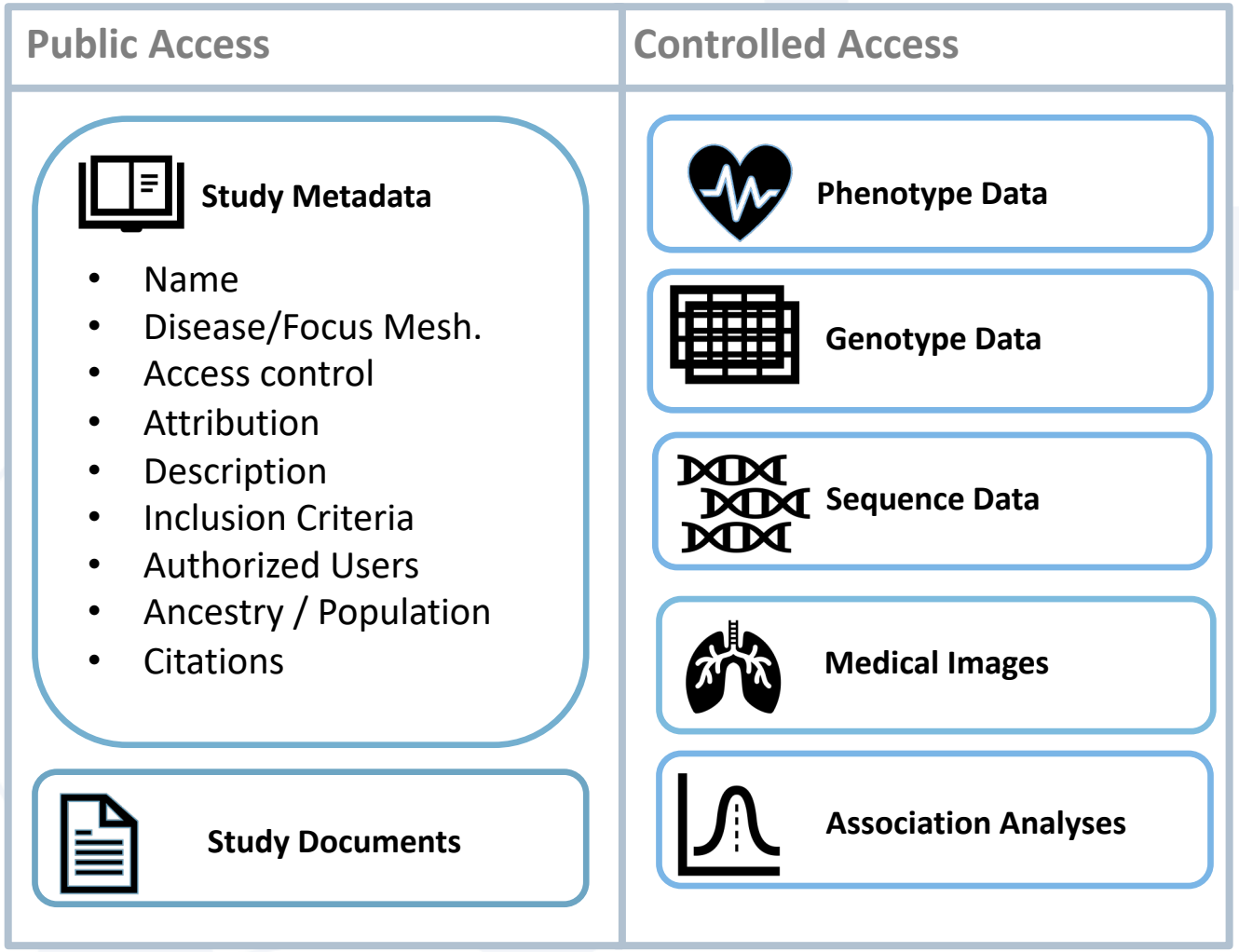
- Data collected from the same funding, Research Focus, Cohort

Public Access

- Study Level Metadata
- Study Documents
- Summaries and Metadata

Controlled Access

- Individual Level
- Sensitive Association Analysis

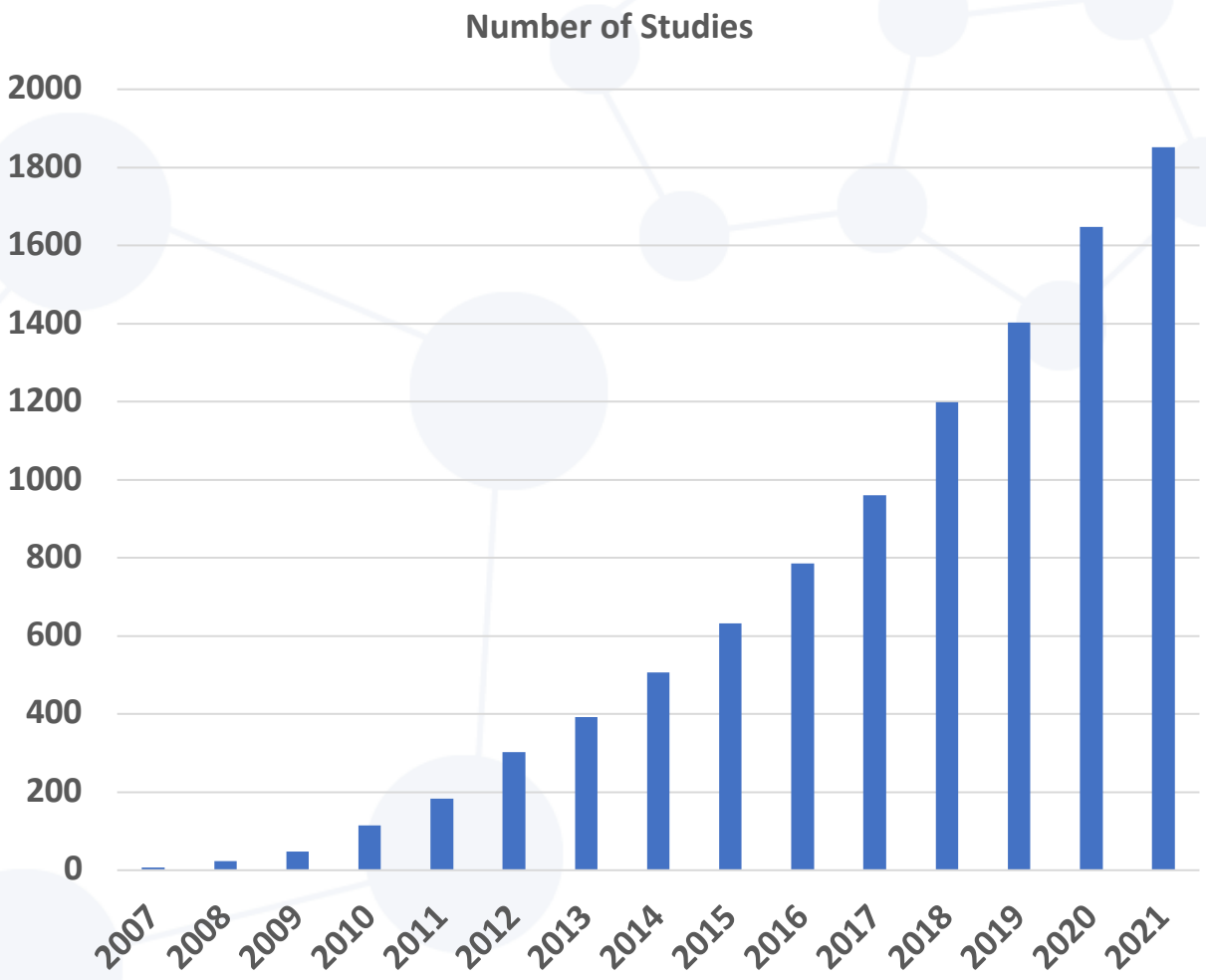


Why Do this?

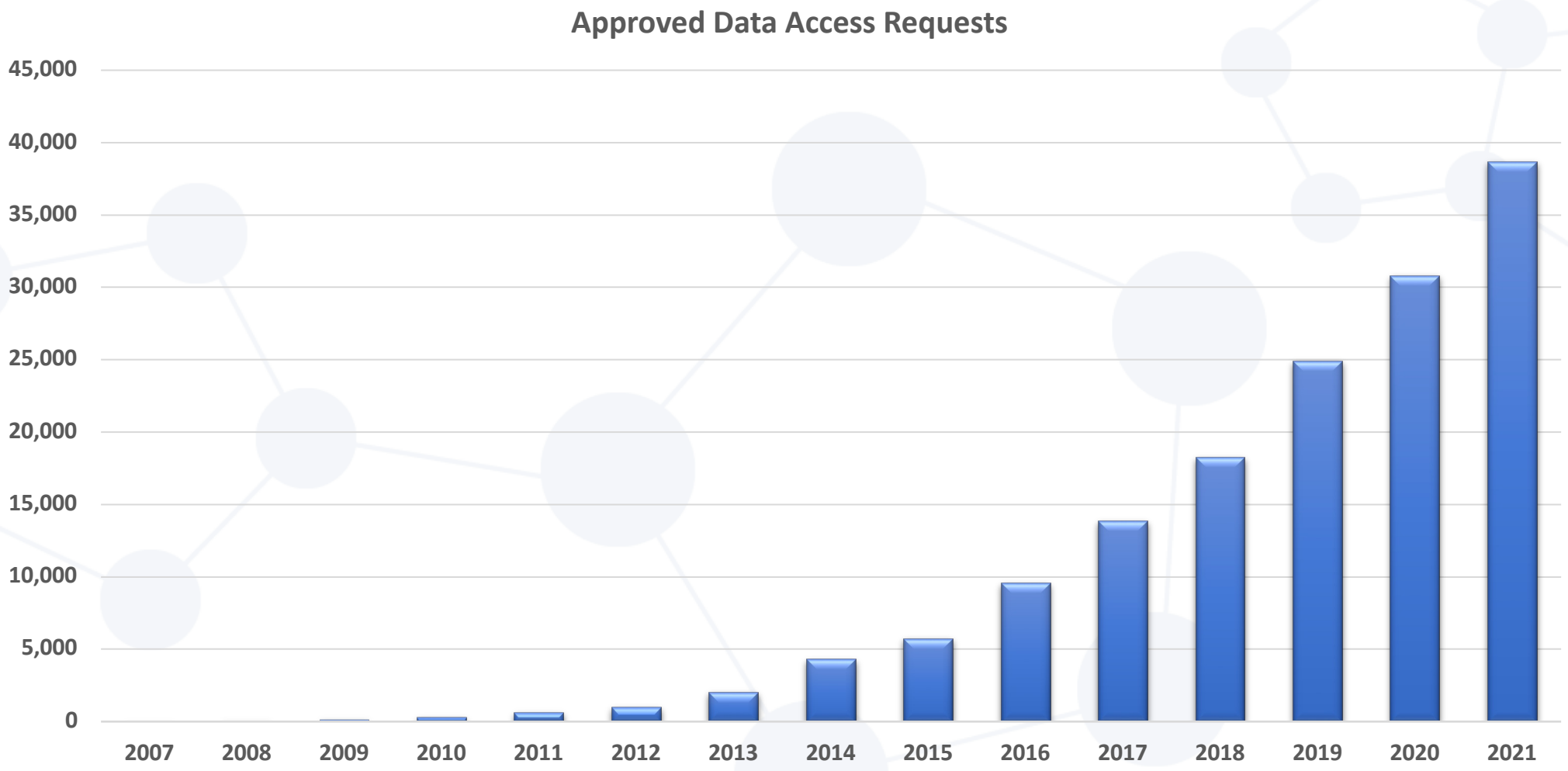
- A library of research Data
- Each Study is analogous to a Book
- Scientists from around the world can use these data to augment their research and make new discoveries

Data Available in Archive

Studies	1,972
Subjects	~2.9 Million
Samples	~3.4 Million
Phenotype: Variables	371,436
Values	~2.5 Billion
Study Documents	7,149
Association Analyses	7,913
Genotype Assays (array)	~2 Million
Genotype Assays (imputed)	543,137
Genotype Assays (seq derived)	399,269
Sequence (WGS SRA)	178,288
Sequence (WXS SRA)	271,447
Sequence (RNAseq SRA)	86,879
Epigenomic (SRA)	~35,000



Requests for the data



Delicate Balance

- Extensive corpus of sensitive human data
- Obligation to shield subject identity
- Value to humanity lies in ability to share within research community
- How to be a resource for the advancement of science while maintaining confidentiality?

Threats

- Data are stripped of PII
  - But a person's genome is the ultimate PII and is easy to obtain
- Re-identification
  - individuals, families, populations
- Example
  - Politician has a family member within a schizophrenia study

Threats

Traditional

- User is traditional threat
  - Legal agreements
  - Institutional liability
  - Penalties for violation

Threats
Expanded

- Intermediate actors present greater threat
  - Systems, networks, clouds
  - Software, workflows
  - None are controlled by user authentication
  - None are affected by legal agreements or penalties

Threats

Expanded

- Open-source software chain
  - Tradition of running amateur software
  - All built upon open source of unknown and unverified provenance
  - Few if any pay attention to SBOM

Threats

Expanded

- Bringing “compute” to the data
  - Has become a mantra in big data
- Who authorizes the code?
  - Researcher provided
  - Environment provided
- What environments can safely accept unknown code?

Security Models

- Authority-vs-Identity
  - Traditional identity-based methods prevail
  - NIH is pursuing authority-based models

Security Models

Identity-based Security

- Context-free
  - Who you are
- Excess authority
  - All available permissions
- Identity theft
  - Programs use researcher identity
  - Potential for catastrophic consequences
- Poor federation
  - Every system must know every user

Security Models

Authority-based Security

- Context-sensitive
  - What you intend to do
- Least authority
  - Only required permissions
- Identity not exploitable
  - Programs restricted to provided permissions
  - Bad or malicious software can be contained
- Good federation
  - Systems recognize source of authority not individual

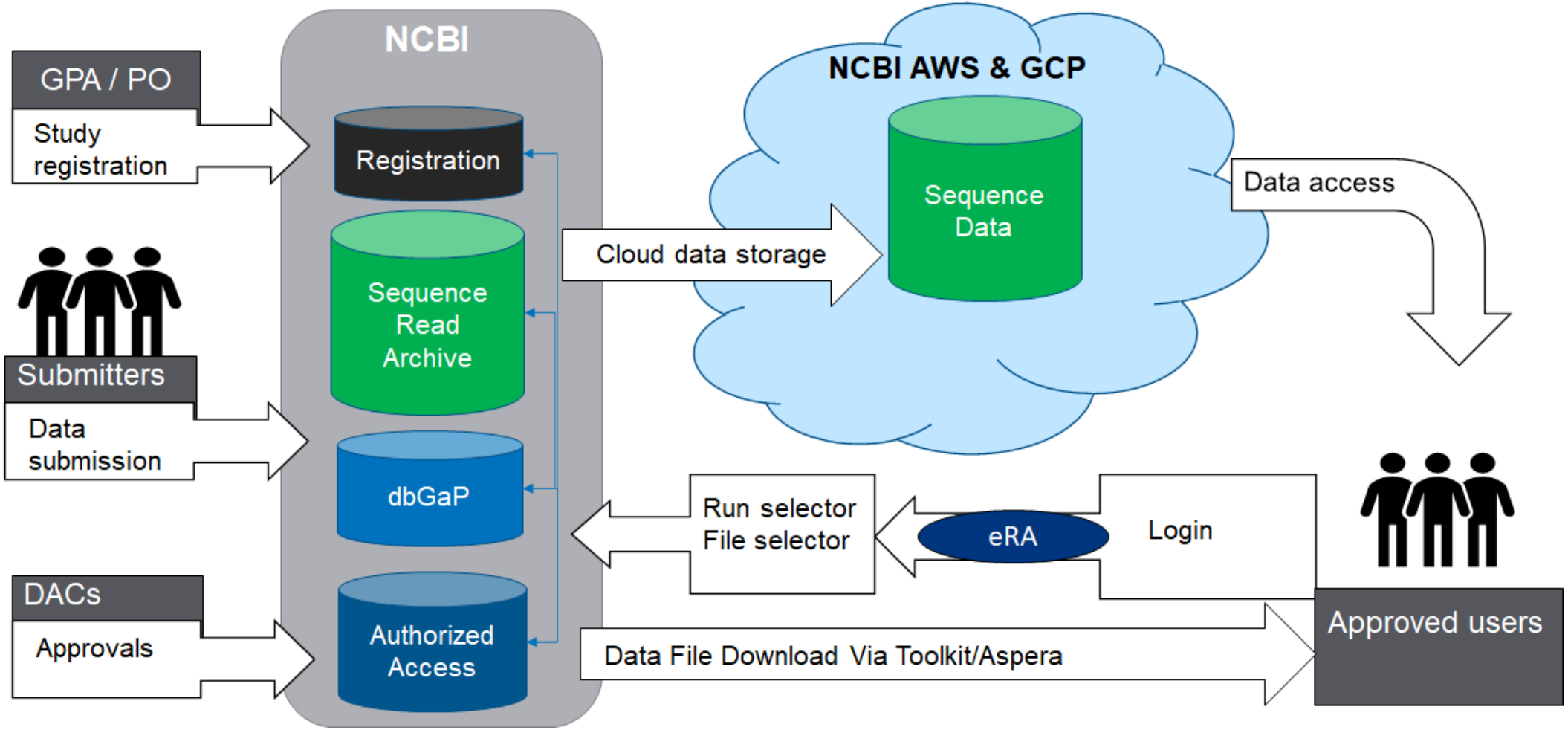
Security Models

Compatibility Challenges

- Models do not mix well

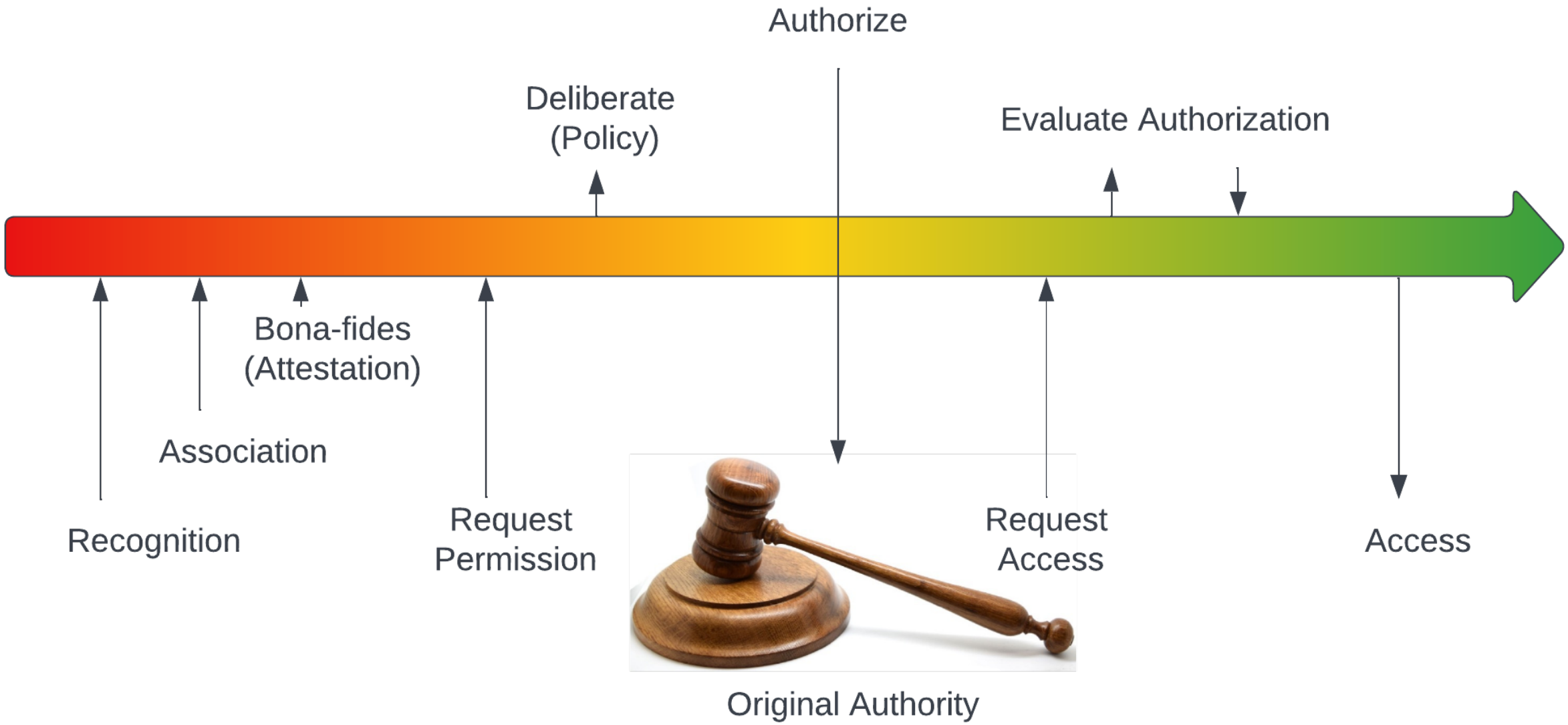
- Overwhelming investment in identity-based model

Journey
Submission



Journey

Access



Authorization

Request Access Permissions

- Consent
- Data access request, usage limitations
- Committee approval
- Grant, storage

Authorization

Retrieve Permissions

- Grant retrieval
  - Authentication for retrieval of stored authorizations

- NIH-signed Token from RAS
- Token duration
  - Associated with live user

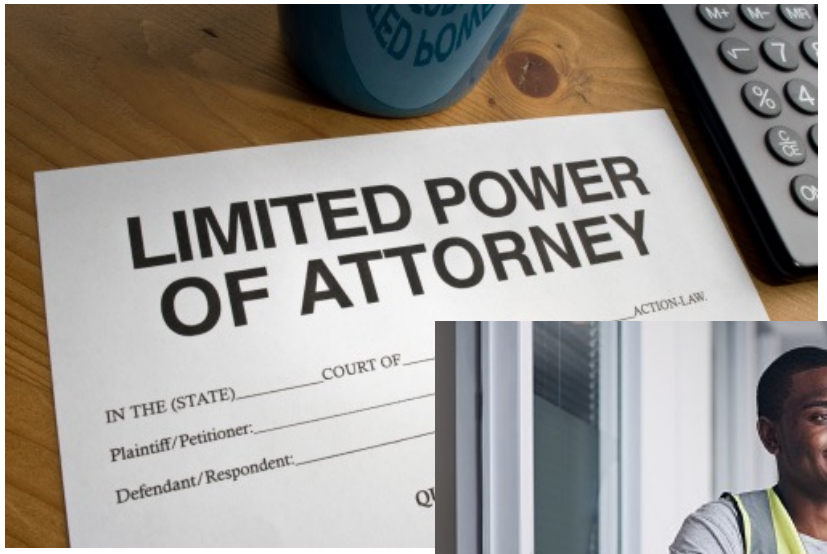
Computation

Task Description

- What to work on
- Least Authority within tokens
- Context-specific limitations

Computation

Delegation



- POLA Token
- User not present
- Assign Power of Attorney
  - For program instances
  - For systems
- Worker Authentication
- Token duration

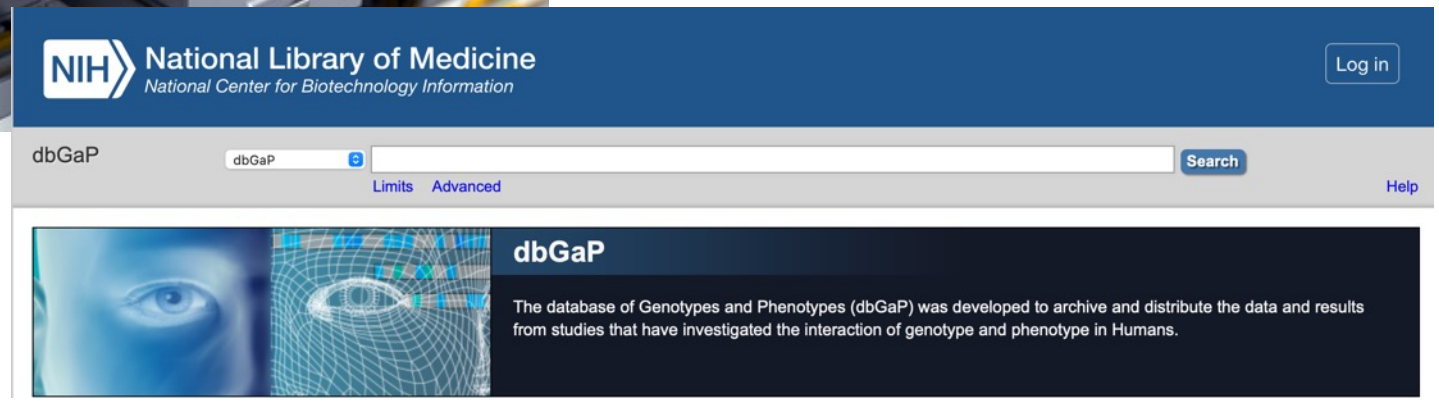
Zero Trust

Supported by Token Protocol

- System – mTLS
- API – API Token
  - Program to API
  - Bound to system TLS certificate
  - Specific permission subset
- Content – Task-specific Token
  - Delegated user authorizations
  - Assigned to compute environment

System Components

Data Governance Authority



- dbGaP Authorized Access (AA)
  - Data access requests (DAR)
  - Manages authorization process
  - Stores access authorizations
  - Supplies AuthZ to RAS process

System Components

Researcher Auth Service (RAS)

- Researcher authentication
  - Anonymized identity
  - 12-hour duration
- Issues signed token
  - Carries authorizations
  - Retrieved from dbGaP
- GA4GH passport
  - Interoperable

System Components

Data Locators

- Validates RAS token
- Locate objects by id
- DRS
  - GA4GH emerging standard
  - See: https://locate.be-md.ncbi.nlm.nih.gov/ga4gh/drs/v1/
- IDX
  - Convert accessioned object ids to DRS ids
- SDL
  - NCBI SRA established standard

System Components

Cloud Storage

- Pre-signed URLs
- Authority vs Identity
  - Require authority-based resource server
  - Employs ACL-based access to objects
- Auth and billing models
  - Unix roots make them inextricably bound
  - Resource servers are billed to provider instead of user
- Surrender of control to CSP
  - Attempts to use CSP IAM bypass tokens

System Components

Logging

- Token retrieval at authentication
- Derivation of task-specific token
- Token usage at Data Locator
- Token usage at Resource Server
- Pre-signed URL and bucket logs

System Components

Audit, Response, Recovery

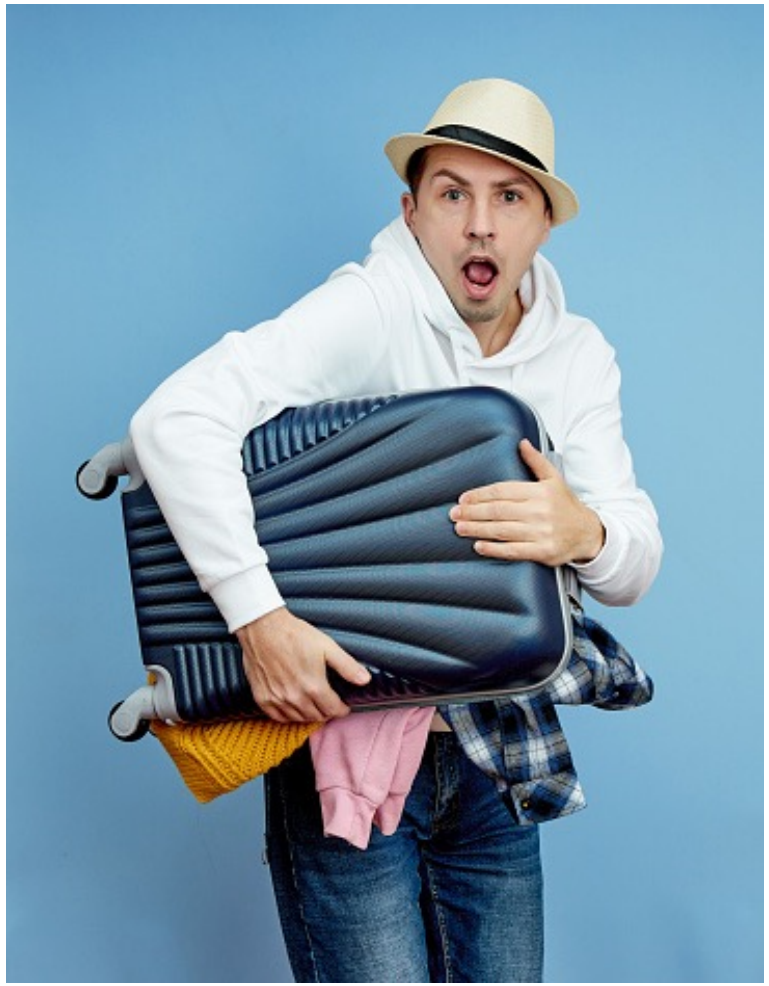
- Events related by RAS token transaction id
- Raw log ETL and event correlation
- Specific issue detection
- Usage pattern and anomaly detection

The Confinement Problem

- Prevent leakage after access has occurred
- Accidental leakage
  - Stored insecurely
- Intentional leakage
  - Human relay
- Covert communication
  - Software communications
  - Steganography
- Geographical confinement

The Confinement Problem

Genomic Analysis Platform



- Plaintext visibility
- User-provided executables
- Egress
  - Block all egress
  - Filter by content
  - Monitor for violation

The Confinement Problem

Secret Store

- No direct visibility
- Predefined executables
  - Difficulties in verification
  - Potential covert channels
- Researcher-defined workflow

The Confinement Problem

Cloud Service Providers

- Sponsored projects
  - Created/configured by trusted authority
- Monitored projects
  - Created/configured by user
  - Monitored by trusted authority
- Relies upon cloud IAM
  - May bypass token controls

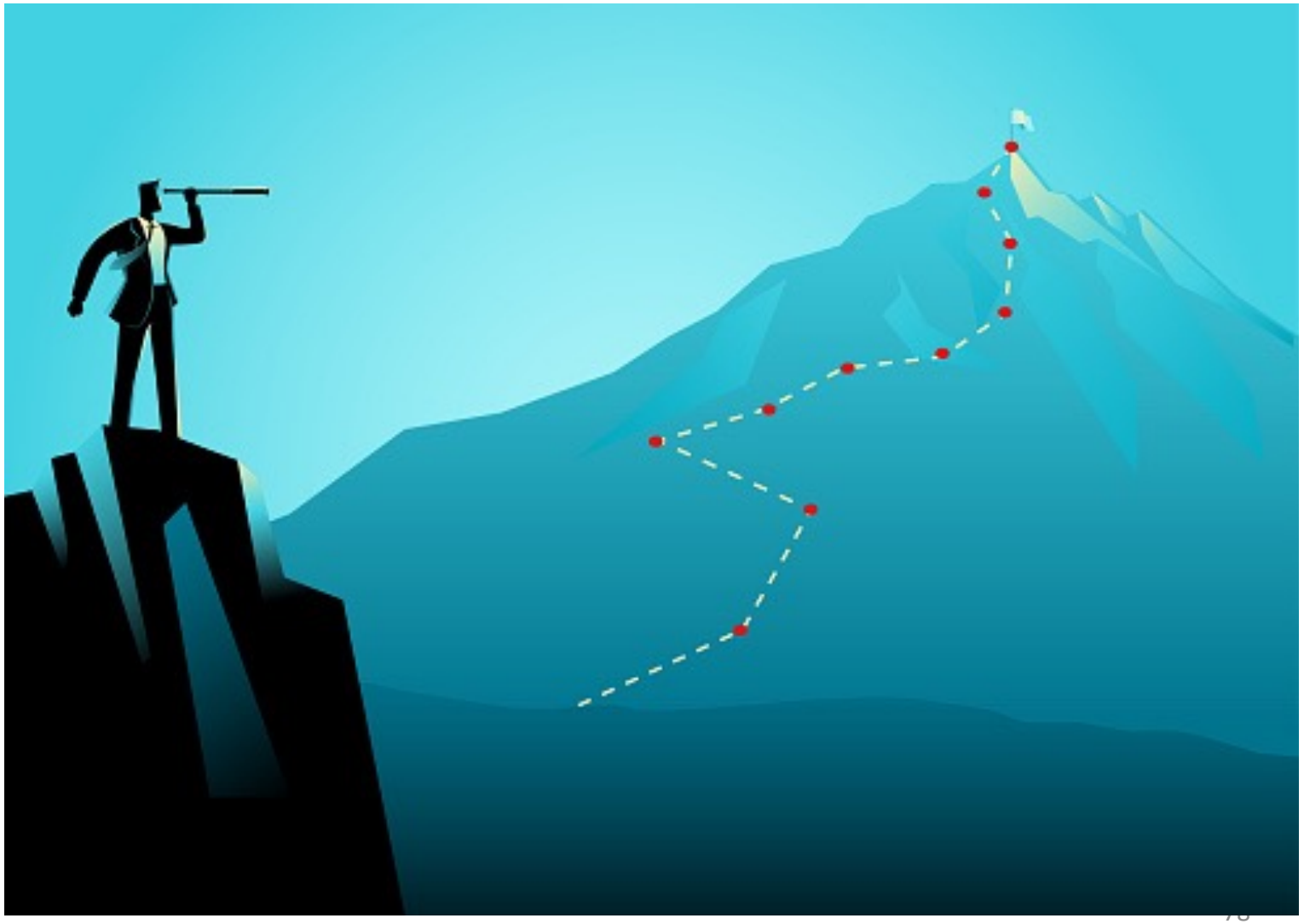
The Confinement Problem

Encryption

- Object encryption
- Personalized encryption
- Homomorphic encryption

Future Directions

- Normalize use of API Tokens
- Greater levels of categorization by sensitivity
- Improve interoperability between CSP and NIH-governed content management



Acknowledgements

NIH/NLM

Michael Feolo
Andrew Russette
Brandi Kattman
Bart Trawick
Kim Pruitt
Steven Sherry
Dar-Ning Kung
Patricia F. Brennan
dbGaP team

NIH/OD

Susan Gregurick
Larry Reed

NIH/CIT

Andrea Norris
RAS team

NIH/NHLBI

Alastair Thompson

NIH/NCI

Jeffrey Shilling

NIH/NHGRI

Heidi Sofia

NIH/NICHD

Rebecca Rosen

- GA4GH
  - AAI & DURI teams
- NCCoE
  - Natalia Martin
  - Ron Pulivarti
  - Frederick Byers
- NIST
  - Justin Wagner
  - Samantha Maragh
  - Justin Zook
- MITRE
  - Ann-Marie France
  - Martin Wojtyniak
  - Sallie Edwards
  - Kevin Wilson

Contact

Michael Feolo

feolo@ncbi.nlm.nih.gov

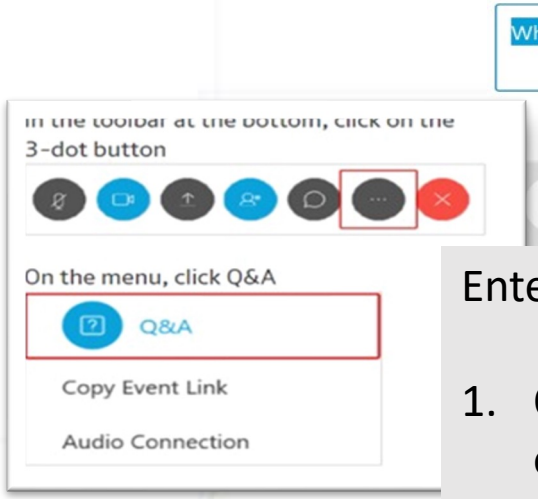
Kurt W. Rodarmer

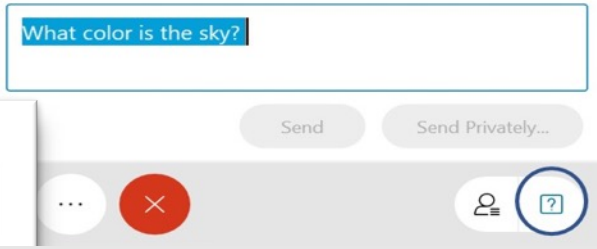
rodarmer@ncbi.nlm.nih.gov

Thank You!

Securing Sensitive Human Data in support of Genomics Research

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.

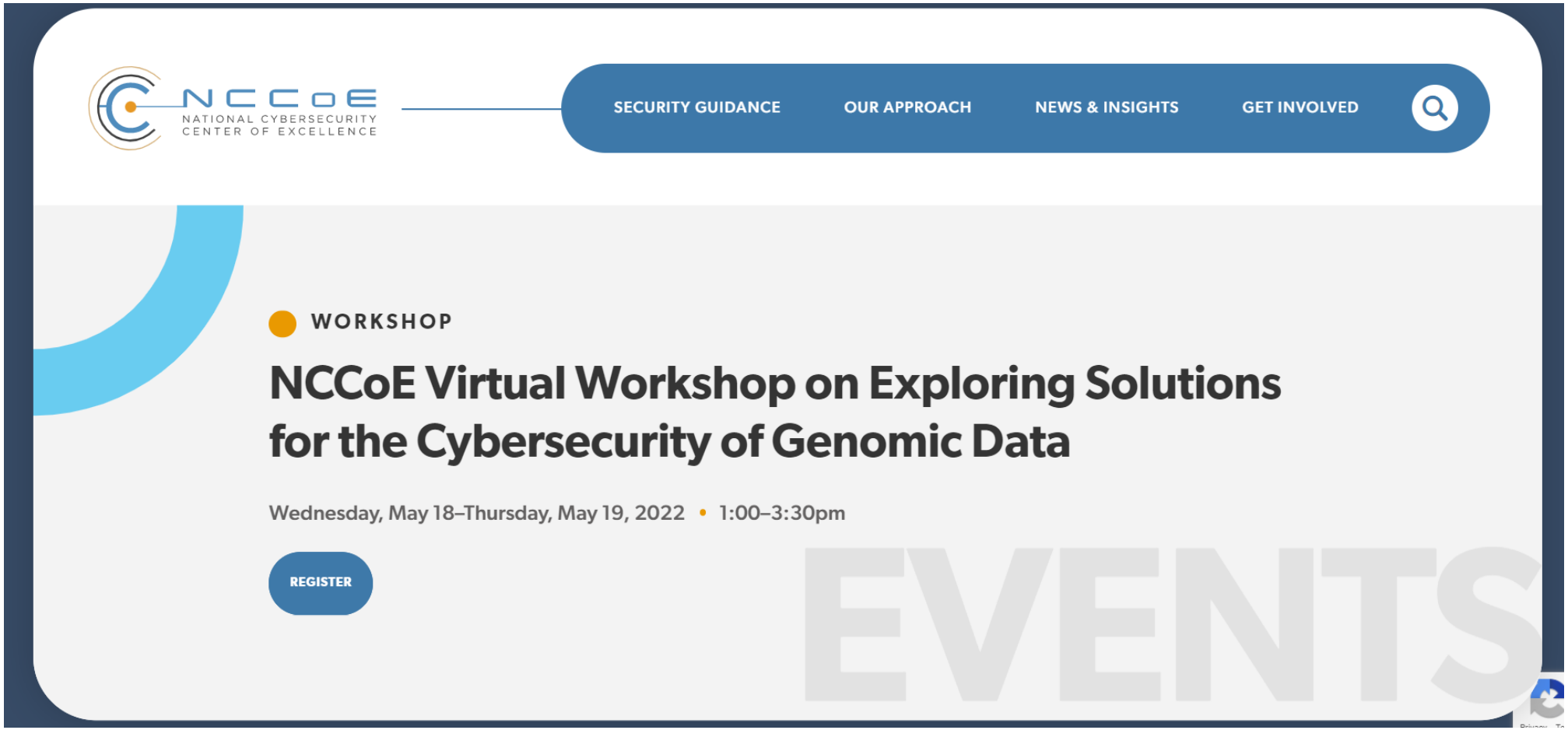
Workshop Close Out

Ron Pulivarti, NIST NCCoE

AGENDA: MAY 19

Segment	*Time (EDT)*
Workshop Day 1 Reflections	1:00 PM – 1:10 PM
Session Three: Genomic Data Security Through Risk Management	1:10 PM – 2:10 PM
Break	2:10 PM – 2:25 PM
Session Four: Genomic Data Security in Electronic Health Records	2:25 PM – 3:25 PM
Wrap Up	3:25 PM – 3:30 PM

LINK FOR MAY 19 WORKSHOP



https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-virtual-workshop-exploring-solutions-cybersecurity-genomic-data

Please join us tomorrow!

Contribute to the conversation

Email genomic_cybersecurity_nccoe@nist.gov