NIST Internal Report
NIST IR 8467 ipd

Cybersecurity Framework Profile for Genomic Data

Initial Public Draft

Natalia Martin
Ronald Pulivarti
Justin Wagner
Samantha Maragh
Jennifer McDaniel
Justin Zook
Andrew Bennett
Brett Kreider
Christina Sames
Julie Snyder
Bob Stea
Kevin Wilson
Martin Wojtyniak

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8467.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8467 ipd

Cybersecurity Framework Profile for Genomic Data

Initial Public Draft

Natalia Martin
Ronald Pulivarti
National Cybersecurity Center of Excellence
Information Technology Lab

Justin Wagner
Samantha Maragh
Jennifer McDaniel
Justin Zook
Material Measurement Laboratory

Andrew Bennett
Brett Kreider
Christina Sames
Julie Snyder
Bob Stea
Kevin Wilson
Martin Wojtyniak
MITRE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8467.ipd

June 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:
Martin N, et al. (2023) Cybersecurity Framework Profile for Genomic Data. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) 8467 ipd. https://doi.org/10.6028/NIST.IR.8467.ipd

Author ORCID iDs
Natalia Martin: 0000-0003-0531-7114
Ron Pulivarti: 0000-0002-8330-3474
Fred Byers: 0009-0005-7865-2628
Samantha Maragh: 0000-0003-2564-9589
Justin Wagner: 0009-0003-8903-0504
Justin Zook: 0000-0003-2309-8402
Jennifer McDaniel: 000-0003-1987-0914

Public Comment Period
June 15, 2023 – July 17, 2023

Submit Comments
genomic_cybersecurity_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Low-cost genomic sequencing technologies facilitate collection, sequencing, and analysis of vast quantities of genomic data, fueling our nation's economic and health leadership posture. However, this valuable genomic information may not be protected with sufficient rigor commensurate with cybersecurity and privacy risks. In response, the National Institute of Standards and Technology (NIST) engaged genomic stakeholders across government, academia, and industry to inform the voluntary, risk-based guidance contained in this Cybersecurity Framework (CSF) Profile for Genomic Data. This Profile describes the primary Mission Objectives of organizations processing genomic data and identifies priority CSF Subcategories that can help organizations select and implement cybersecurity capabilities that support their mission. While this Profile shows intersections between cybersecurity and privacy risk management considerations for processing genomic data, it is focused only on the cybersecurity aspects of those intersections. Future work is planned to address broader privacy risk management considerations. The Profile is meant to supplement, not replace, current cybersecurity and privacy standards and industry guidelines that organizations already use to secure their genomic data.

Keywords

Cybersecurity Framework Profile; DNA sequencing; executive order; genomics; genomic data; genomic sequencing; human genome; informed consent.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Supplemental Content

Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified; see the NIST IR 8467 (draft) publication details.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: genomic_cybersecurity_nccoe@nist.gov.

Table of Contents

List of Tables

List of Figures

Executive Summary

The National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) engaged stakeholders across government, academia, and industry to better understand the current state of the cybersecurity challenges facing the genomics community. This collaboration led to NIST publishing NIST Internal Report (NISTIR) 8432, *The Cybersecurity of Genomic Data*, an overview of the challenges and opportunities with genomic data cybersecurity. As a follow-on effort, the NCCoE collaborated with a diverse subset of stakeholders to conduct working sessions focused on gathering the information needed to develop this Cybersecurity Framework (CSF) Profile for Genomic Data.

The CSF Profile for Genomic Data provides voluntary guidance to help organizations manage and reduce cybersecurity risks for systems, networks, and assets (collectively referred to as 'systems' in the document[1]) that process any type of genomic data. Human genomic data plays a significant role in the bioeconomy. While the focus of this CSF Profile is cybersecurity, whenever human genomic data is processed, privacy risk management considerations must also be addressed. As a result, privacy is referenced in multiple places throughout this CSF Profile where cybersecurity and privacy risks overlap. NIST plans to address the broader privacy landscape for genomic data by creating a Profile using the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management ("Privacy Framework"). Once created, the Privacy Framework Profile for Genomic Data should be used as a complementary tool to this CSF Profile.

This CSF Profile identifies 12 genomic-related Mission Objectives and the prioritized relevant CSF Subcategories to help organizations protect genomic data throughout the data lifecycle. Prioritizing cybersecurity capabilities based on their organization's Mission Objectives can inform cybersecurity decision-making. The Profile is intended to supplement, not replace, existing cybersecurity activities, practices, policies, and guidance. Organizations should consider their unique obligations, operating environment, and Mission Objectives when prioritizing and implementing cybersecurity capabilities and controls.

Cyber attacks targeted at systems that process genomic data could impact the confidentiality, integrity, and availability of that data, introducing economic, privacy, discrimination, and national security risks. Organizations rely on genomic data sharing to advance scientific and medical research, improve health outcomes, and compete within the bioeconomy and thus genomic data often needs to be aggregated from multiple sources. The selection of cybersecurity and privacy capabilities for genomic data is complicated by the broad and diverse nature of the genomics community, including biopharmaceutical research, healthcare, law enforcement, and agriculture. In addition, organizations that share data with stakeholders in multiple countries may have requirements for protecting genomic data or the cross-border transfer of data.

Organizations processing genomic data can use this Profile to:

- Understand genomic data cybersecurity considerations

[1] The CSF uses the term asset to describe "the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes" (ID.AM).

- Assess current organizational cybersecurity practices to identify gaps and areas of improvement for existing practices or infrastructure
- Develop individualized organizational Current (As-Is) and Target (To-Be) Profiles
- Prioritize investments in cybersecurity capabilities aligned to the CSF Subcategories identified as most important to support organizational Mission Objectives
- Understand the relationship between cybersecurity and privacy risk management

1. Introduction

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides guidance to help organizations manage, reduce, and communicate cybersecurity risks.[2] The CSF, created through collaboration with a diverse range of stakeholders, uses a standardized format and a risk-based approach to address cybersecurity issues. Although the Framework presents a variety of mitigations, a Profile such as this tailors and prioritizes mitigations for a specific sector or industry.

The NIST National Cybersecurity Center of Excellence (NCCoE) engaged stakeholders from government, academia, and industry to better understand the current state of the cybersecurity challenges facing the genomics community. In 2022, the NCCoE conducted two public workshops [1][2]—the first concentrating on the challenges faced or anticipated by the community and the second focusing on solutions to help address those challenges. NIST published NIST Internal Report (NISTIR) 8432, *The Cybersecurity of Genomic Data* [3], to further explore and document the concepts identified in the workshops, including the concerns and challenges associated with processing genomic data, the current state of relevant cybersecurity risk management practices[3], gaps in implementing genomic data protections, and potential solutions along with areas for further research. NISTIR 8432 can be used as a supplement to this document, providing context and background for better understanding the current state of cybersecurity practices when processing genomic data.

As a follow-on effort, the NCCoE collaborated with a diverse subset of those same stakeholders to conduct working sessions designed specifically to generate the information needed to develop this CSF Profile for Genomic Data.

1.1. Purpose

This CSF Profile for Genomic Data provides voluntary guidance to help organizations manage cybersecurity risks for systems that process genomic data. The Profile helps organizations prioritize cybersecurity capabilities based on their Mission Objectives, which can inform cybersecurity decision making. The Profile is intended to supplement, not replace, existing cybersecurity activities, practices, policies, and guidance. Organizations should consider their own obligations, operating environment, and Mission Objectives when prioritizing and implementing cybersecurity capabilities and controls.

[2] The NIST Privacy Framework provides similar guidance for privacy.
[3] The focus of the workshops was on cybersecurity, but many participants noted the importance of privacy, too.

The selection of cybersecurity capabilities for genomic data is complicated by the broad and diverse nature of the genomics community, including biopharmaceutical research, healthcare, law enforcement, and agriculture. Cyber attacks targeted at systems that process genomic data could impact the confidentiality, integrity, and availability of that data, introducing economic, privacy, discrimination, and national security risks. While the purpose of the Profile is to provide cybersecurity guidance, it also acknowledges the intersection of cybersecurity with privacy (see Sec. 2.3).

Organizations processing genomic data can use this Profile to:

- Understand genomic data cybersecurity considerations
- Assess current organizational cybersecurity practices to identify gaps and areas of improvement for existing practices or infrastructure
- Develop individualized organizational Current (As-Is) and Target (To-Be) Profiles
- Prioritize investments in cybersecurity capabilities aligned to the CSF Subcategories identified as most important to support organizational Mission Objectives
- Understand the relationship between cybersecurity and privacy risk management

Executive Order (EO) 14081, Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy, was issued on September 12, 2022 [EO 14081]. The order seeks to implement a whole-of-government approach for bolstering biotechnology and biomanufacturing, which includes advancing a biological data ecosystem that spurs innovation while adhering to security and privacy standards. The EO directs the Secretary of Homeland Security, in coordination with the Secretary of Commerce (acting through the Director of NIST) and other government agencies, to identify and recommend cybersecurity best practices for biological data stored on Federal Government information systems. Genomic data is one form of multipurpose, high-value biological data used by Federal Government agencies as well as the private sector. Section 4 of the EO calls for establishing a "Data for the Bioeconomy Initiative (Data Initiative)" that will identify data types and sources critical to the bioeconomy. The EO addresses genomic data, its role in the bioeconomy, and the need to develop data protection plans that address security, privacy, and risks to this data and other related data types. This Profile serves as one source for identifying and recommending cybersecurity best practices for protecting the security of genomic data. This Profile also provides a subset of privacy-related cybersecurity best practices, but it does not address the entirety of privacy risk management. Additional work is needed to develop a complementary Privacy Framework Profile to address privacy risks. For example, the Privacy Framework more fully contemplates the privacy aspect of data provenance and other privacy risk management capabilities like disassociated processing.

1.2. Scope

Genomic information, which may be processed from microbial, fungus, plant, and animal species, including humans, exists in different forms throughout its lifecycle, which may include the following phases: sample collection, sample preparation, data generation, and data analysis. **Fig. 1** illustrates this lifecycle, identifying the primary scope for this Profile to be genomic data generated via sequencing or other techniques, as well as data generated by subsequent analyses, highlighted in blue [4].

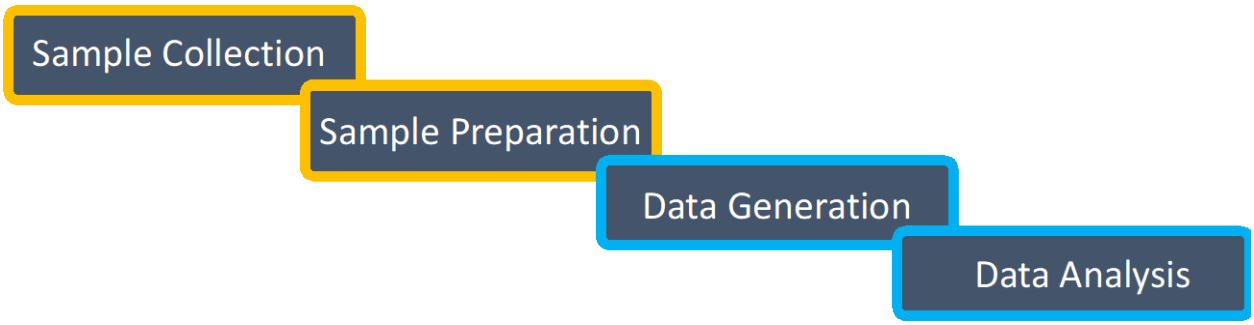

Fig. 1. Genomic Data Lifecycle Phases; Naveed et al. [4]

While this CSF Profile addresses cybersecurity risk, it also addresses some aspects of privacy risk where the two areas overlap (see Sec. 2.3 for a discussion regarding the relationship between cybersecurity and privacy). Organizations processing human genomic data consider the privacy protections not only of donors, but also relatives, whose privacy may be impacted because of the unique and lasting potential for identifying individuals and their relatives through deoxyribonucleic acid (DNA) samples. When human genetic material is processed, the sample preparation, data generation, and data analysis phases can be subject to privacy considerations, such as notice and informed consent, that are initially addressed during sample collection. Due to the impact of these privacy considerations on the steps that are in scope, this Profile also includes cybersecurity guidance for protecting the privacy-related processes that are initiated during earlier phases in the genomic data lifecycle. Additional guidance is needed to address the full scope of privacy considerations and is beyond the scope of this Profile.[4]

1.3. Audience

The intended audience for the Profile includes organizations across public and private sectors who process genomic data. This CSF Profile for Genomic Data can be used by organizations to identify and communicate cybersecurity expectations with internal and external parties. The Profile can also be used by organizational leadership to generate priorities tailored to the operational aspects of the organization.

1.4. Document Structure

This document is organized into the following sections:

- Section 2 provides an overview of genomic data and a description of the relationship between cybersecurity and privacy.
- Section 3 presents additional information on the NIST CSF, CSF Profiles, and their application.
- Section 4 describes the methodology used to develop this Profile.
- Section 5 discusses genomics community organizational Mission Objectives and their prioritization.

[4] Future NCCoE work is planned to create a companion Privacy Framework Profile for Genomic Data.

- Section 6 prioritizes CSF Subcategories for each Mission Objective and provides the rationale for prioritization.
- The References section contains cited resources.
- Appendices include acronyms and abbreviations and a glossary.

2. Overview of Genomic Data

A genome contains the full set of instructions, generally in the form of DNA, to form an organism. Instructions are encoded in the sequence of the nucleotide subunits (also called bases), adenine (A), cytosine (C), guanine (G), and thymine (T), that comprise the DNA molecule. A segment of bases containing the instructions for making a product, like a protein, is called a gene. An individual organism's DNA sequence is largely unchanged throughout its life. Variations in the number and kinds of genes across a population underpin the diversity of life on earth. Some genes give rise to observable traits, termed phenotypes, like flower color, cell shape and size, resistance to chemicals (e.g., pesticides, insecticides), hair or eye color, blood type, and facial features. Other phenotypes may include the presence of or susceptibility to certain medical conditions. Genomic data is unique, immutable, associative, and conveys important health, phenotype, and personal information about individuals and their kin (past and future).

DNA sequencing is a key method researchers use to understand genomic information. Sequencing identifies the order of bases across a stretch of DNA or even the whole genome. The procedure begins with sample collection, followed by DNA purification and processing to build a technology-specific DNA library suitable for sequencing. The prepared sample is then applied to a specially designed substrate, like a glass flow cell, used by the sequencing instrument to read the order of the DNA bases. The sequencer typically outputs raw data in the form of sequence reads (e.g., DNA sequences read by the instrument), identifiers (i.e., information about the sample and the read), and quality scores for each base call. The resulting data may be processed further to filter out low-quality reads, align to a reference genome, identify variants, or annotate genomic regions. Further analyses of the genomic data differ based on intended application and may include:

- Using genetic information to prevent, diagnose, or treat disease
- Understanding genetic diversity of plants and animals in the environment
- Identifying individuals for genealogical or law enforcement purposes

Genomic sequencing data files are often large and stored on-premises or in the cloud for processing and analysis. Sensitive genomic data may be subject to access controls or encrypted to preserve security and privacy. Non-sensitive genomic data may be uploaded to public or limited-access databases, like the sequence read archive (SRA) or the database of Genotypes and Phenotypes (dbGaP) that are run by the National Center for Biotechnology Information (NCBI) at the National Institutes of Health (NIH). Genomic data may also reside in other formats that summarize only key information. For instance, genomic data in electronic health records may focus on identifying known variants of medical significance. Genomic data can be at risk of being intercepted, corrupted, overwritten, or deleted at each stage in its lifecycle. The impacts of these risks span all forms of genomic information and include compromising confidentiality

(leaking of personal or institutional data), integrity (providing false or inconclusive results), and availability (rendering devices, processes, services, or facilities unavailable).

2.1. The Genomic Data Ecosystem and Bioeconomy

The term bioeconomy describes the economic activity derived from biotechnology and biomanufacturing. The bioeconomy spans multiple public and private sectors, including universities, associations or nonprofits, governmental agencies, industry, and data subjects. Individuals and organizations in these sectors operate across multiple industries, including healthcare, research and development, agriculture, law enforcement, genealogy, manufacturing, and direct-to-consumer services. Although the boundaries of the bioeconomy are not always clear, activities that use natural resources, but not biological products, are typically not part of the bioeconomy. Genomic data is a critical asset that supports the bioeconomy.

The complex genomic data ecosystem includes a variety of individuals and organizations from the sectors participating in the bioeconomy. Participants in the genomic data ecosystem may generate, curate, and/or analyze genomic data to support operations or make decisions. Examples in which genomic data factor into the ecosystem include:

- Sequencing service providers generating sequence DNA for customers
- Research institutes generating or using genomic data for fundamental or biomedical research
- Biotechnology and pharmaceutical industry generating or analyzing genomic information to research a disease or develop therapeutics
- Cloud service providers storing, transferring, or providing capabilities to analyze genomic data
- Law enforcement agencies using genomic data for identification purposes
- Healthcare providers generating and using genomic information to diagnose or treat health conditions

The genomic data ecosystem continues to evolve and may expand in the future as new technologies and applications are developed.

2.2. Genomic Data Security and Privacy Concerns and Challenges

Processing any type of genomic data often includes sharing and aggregation from multiple sources to advance scientific and medical research, improve health outcomes, and compete within the bioeconomy. Processing human genomic data requires additional security and privacy protections, such as providing information about processing practices for transparency, managing data in accordance with differing preferences and consents expressed by the subjects, and providing adequate technological and policy controls that implement these requirements while also meeting genomic data processing needs. Responsible data sharing and analytics facilitate

commerce, technological development, and research while protecting security and privacy (e.g., respecting informed consent and protecting individuals from potential privacy problems[5]).

Concerns in protecting genomic data include economic, privacy, discrimination, and national security. For example:

- Economic security concerns of the bioeconomy include intellectual property infringement due to exfiltration of genomic data or operational disruption due to the loss of availability of sequencing or processing services for genomic data.
- Privacy concerns result from the inherent value and immutable nature of genomic data. As use of genomic data expands, the value of a person's genomic data increases. A person's DNA remains unchanged throughout their lifetime and even closely resembles the DNA of relatives. Privacy concerns are exacerbated because human genomic data, even small fragments of a person's whole genome, can usually be re-identified. Even without the identifying metadata, genetic fragments may be re-identified when combined with available datasets, such as ancestry data, self-shared identified genomic data of distant relatives, surname inference, and age [5][6][7][8]. Identified or re-identified human genomic data can lead to emotional distress or discrimination based on disease risk, the revelation of hidden consanguinity or phenotypes including health, emotional stability, mental capacity, appearance, and physical abilities. Obtaining meaningful or informed consent and ensuring genomic data processing remains in synch with given consent over time, especially as data is shared and aggregated, helps individuals have some control to address their concerns, but can be challenging for organizations to manage.
- Discrimination can also stem from sample bias. Artificial intelligence and statistical techniques analyze large sets of genomic data to predict disease and treatment efficacy. Predominantly, these analyses currently use data sets where minority communities are underrepresented. Lack of sample diversity can impact the results and cause discrimination with corresponding potential harms to those not well represented in the sample set [9][10][11].
- National security concerns arise from genomic data's ability to uniquely identify individuals, their kinship to others, phenotypes, and mental and physical health risks. Concerns include its use for population surveillance or extortion of citizens, military, and intelligence personnel [12].

This Profile is designed to help organizations address the cybersecurity aspects of these concerns through identifying, prioritizing, and achieving the outcomes that are appropriate for their Mission Objectives and the sensitivity of the genomic data they are processing. Further work is planned to develop a Privacy Framework Profile to address the broader privacy aspects of these concerns. Section 2.3 describes the relationship between cybersecurity and privacy risk.

[5] Examples of the types of problems individuals may experience as a result of genomic data processing activities include dignity loss, discrimination, loss of autonomy, and loss of trust. See Section 2.3 of this CSF Profile for Genomic Data for further discussion regarding the cybersecurity and privacy risk relationship.

2.3. Cybersecurity and Privacy Risk Relationship

Cybersecurity and privacy are independent and separate disciplines. However, as shown by the Venn diagram in **Fig. 2**, some of their objectives do overlap and are complementary. Cybersecurity programs are responsible for protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) to provide confidentiality, integrity, and availability as well as ensuring organizations comply with applicable cybersecurity requirements. Privacy programs are responsible for managing the risks to individuals associated with data processing throughout the information lifecycle[6] to provide predictability, manageability, and disassociability[7] as well as ensuring organizations comply with applicable privacy requirements. **Fig. 2** illustrates this relationship between cybersecurity and privacy risks, showing both where they overlap and where they are distinct.

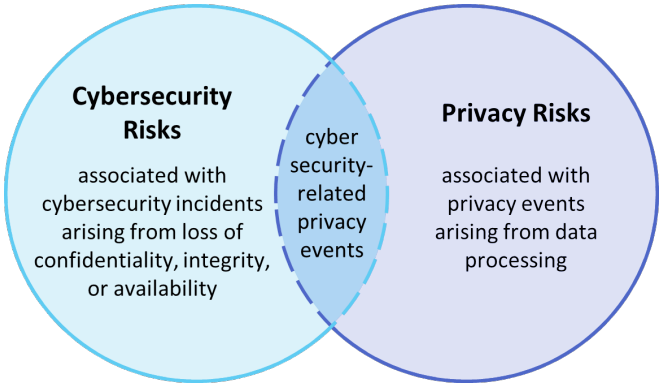

Fig. 2. Cybersecurity and Privacy Risk Relationship (from the NIST Privacy Framework)

While the overlap between cybersecurity and privacy risk management is important, the distinction between the two is also critical to understand. Managing cybersecurity risk contributes to managing privacy risk (e.g., controlling access to data protects against privacy breaches by limiting who can access data and the actions they can perform), but managing cybersecurity risk alone is not sufficient, as permitted data processing activities can introduce privacy risks that are unrelated to cybersecurity incidents. Some data processing activities and technologies inherently introduce privacy risk but may be necessary for valid business purposes. These privacy risks must be managed when they arise. For example, during data processing, genomic data that has been stripped of related metadata may be combined with data from other sources, such as genealogical databases or public records. Or genomic data may be combined with other contextual information, such as a hospital, geographical information, or medical condition. Activities like these that combine genomic data with other data can result in information that exposes a donor's identity. While there may be many valid reasons to combine data from multiple sources, doing so can lead to re-identification of donors. This does not mean that genomic data should not be combined with other data. Rather, it means that when this capability is provided, organizations should be aware of and manage the privacy risk introduced accordingly.

[6] The information lifecycle includes creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as "processing") of data that may impact privacy.
[7] Definitions for predictability, manageability, and disassociability, which are privacy engineering objectives, can be found in the NIST Privacy Framework.

This Profile only addresses privacy considerations in the overlap section of the Venn diagram. There are many privacy activities and outcomes in the remainder of the privacy circle that are outside of the scope of the CSF. For example, considering contextual factors that influence data processing in systems, products, and services. The NIST Privacy Framework can be applied in an analogous manner to address the full scope of privacy risk.

2.3.1. Privacy Risk Management Overview

Privacy risk can impact both individuals (donors or their kin) and organizations, including genomic data programs. Managing privacy risks requires genomic data programs to understand and apply privacy risk management concepts. Members of the genomic data community that are in roles that can impact privacy should also have a clear understanding of how to identify and address privacy risks that may arise during the performance of their role(s).

The NIST Privacy Framework is a tool to help organizations manage privacy risk. Just as genomics programs consider the risks associated with cybersecurity incidents, they should also consider privacy events (i.e., the occurrence or potential occurrence of problematic data actions[8]). Privacy events can occur at any point throughout the genomic data lifecycle from sample collection through data disposal. The privacy events that occur at an organization or in a system can lead to a variety of potential privacy problems that individuals experience. The NIST Privacy Framework describes privacy problems as ranging from dignity-type effects (such as embarrassment or stigmas) to more tangible harms such as discrimination, economic loss, or physical harm.[9] Privacy problems can arise from a donor's interaction with a genomics capability. Some problems can also arise for donors and relatives simply from their information being processed by genomics systems, products, and services, even when the data being processed is not directly linked to identifiable individuals.

A genomic data program may experience impacts that are a result of its role in contributing to privacy risks to individuals, such as noncompliance costs, revenue loss arising from customer abandonment of products and services, or harm to its external reputation or internal culture as a result of the privacy problems individuals may experience. Organizations typically manage these types of program impacts at the enterprise risk management level; by connecting problems that individuals experience to these well-understood program and organizational impacts, organizations can bring privacy risk into parity with other risks they are managing in their broader portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs. **Fig. 3** illustrates this relationship between privacy risk and organizational risk.

[8] A problematic data action is a data action or data processing activity that could cause an adverse effect for individuals.
[9] NIST published the Catalog of Problematic Data Actions and Problems to provide examples that help organizations understand and label the ways data processing activities can impact privacy ("problematic data actions") and examples problems that individuals could experience as a result. The catalogue is available at: PrivacyEngCollabSpace/catalog-PDAP.md at master · usnistgov/PrivacyEngCollabSpace · GitHub.

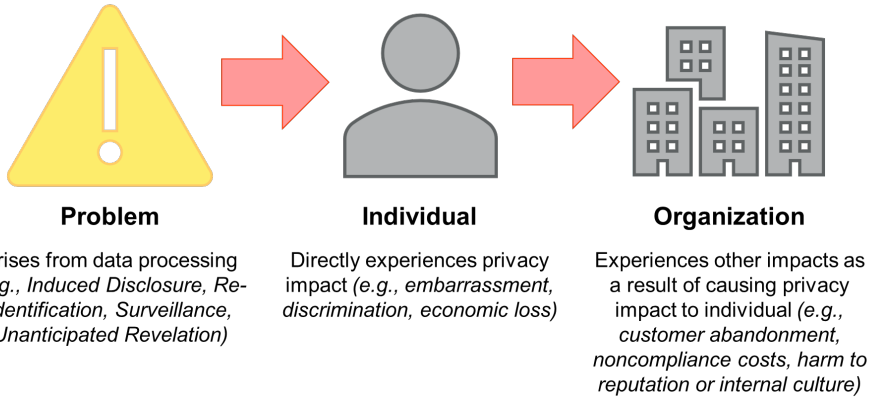

Fig. 3. Relationship Between Privacy Risk and Organizational Risk[10].

2.3.2. Cybersecurity and Privacy Risk Management for Genomic Data

Understanding the different origins of cybersecurity and privacy risks enables programs processing genomic data to effectively manage both areas of risks in the systems and services they design. NIST developed both the Cybersecurity Framework and the Privacy Framework to help organizations manage cybersecurity and privacy risk. These two frameworks work together and share some content where the needs of cybersecurity and privacy overlap.

In addition to the cybersecurity-focused CSF Profile for Genomic Data, NIST plans to develop a Privacy Framework Profile for genomic data. In the meantime, practitioners should also review the NIST Privacy Framework for additional Subcategories that may benefit their programs and the individuals they serve.

3. The NIST Cybersecurity Framework

Created through collaboration between industry and government, the NIST CSF provides prioritized, flexible, risk-based, and voluntary guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, reduce, and communicate cybersecurity risks. Although it was originally designed for organizations that are part of the U.S. critical infrastructure, many other organizations in the private and public sectors (including federal agencies) use the CSF. The CSF enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving security and resilience. It provides a common language for understanding, managing, and expressing cybersecurity risk and for conducting management-level cybersecurity communications among internal and external stakeholders and across an organization, regardless of cybersecurity expertise.

The NIST CSF consists of three main components[11]:

1. **The CSF Core** is a catalog of desired cybersecurity activities and outcomes using common language that is easy to understand regardless of cybersecurity expertise. The

[10] Adapted from NIST Privacy Framework, Figure 3, Catalog of Problematic Data Actions and Problems.
[11] The terms Core, Implementation Tiers, Profile, Mission Objectives, Function, Category, and Subcategory are capitalized when they are used to describe elements of the Cybersecurity Framework throughout this document.

Core guides organizations in managing and reducing their cybersecurity risks to complement an organization's existing cybersecurity and risk management processes.

2. **Implementation Tiers** provide context for how an organization views cybersecurity risk management. The Tiers help organizations understand whether they have a functioning and repeatable cybersecurity risk management process and the extent to which cybersecurity risk management integrates with broader organizational risk management decisions. (Although part of the CSF, for the purposes of this Profile further discussion on Implementation Tiers is excluded.)
3. **Profiles** are a customized alignment of organizational requirements, objectives, risk appetite, and resources against the desired outcomes of the CSF Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization within a specific industry or sector.

3.1. The Cybersecurity Framework Core

The CSF articulates cybersecurity activities and outcomes using common language that all levels of an organization, from the executive level to the individuals with operational roles, can understand. It also provides examples of available resources to help organizations achieve those outcomes. The Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational to the effective use of the CSF, enabling an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and business needs.
- **Protect:** Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact of a cybersecurity event.

The CSF Core identifies underlying Categories and Subcategories for each Function. **Table 1** presents the five Functions including 23 Categories of cybersecurity outcomes such as "Asset Management" and "Protective Technology."

614 **Table 1.** Cybersecurity Framework Functions and Categories.

Function	Function Identifier	Category Unique Identifier	Category
IDENTIFY	ID	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PROTECT	PR	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DETECT	DE	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RESPOND	RS	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RECOVER	RC	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

615 The Categories are further broken down into 108 Subcategories of specific technical or
616 management activities. Section 6 presents the CSF Profile for Genomic Data and prioritizes all
617 108 Subcategories for each Mission Objective, using one table for each of the 23 Categories.

618 The Core also identifies Informative References—existing standards, guidelines, and practices—
619 that provide practical guidance to help an organization achieve the desired outcome of each
620 Subcategory. The Informative References are now maintained in the NIST Cybersecurity and
621 Privacy Reference Tool (CPRT) [13], which offers a consistent format for accessing the
622 reference data of NIST cybersecurity and privacy standards, guidelines, and frameworks. **Fig. 4**
623 shows an example of the Subcategories and Informative References within the Business
624 Environment Category.

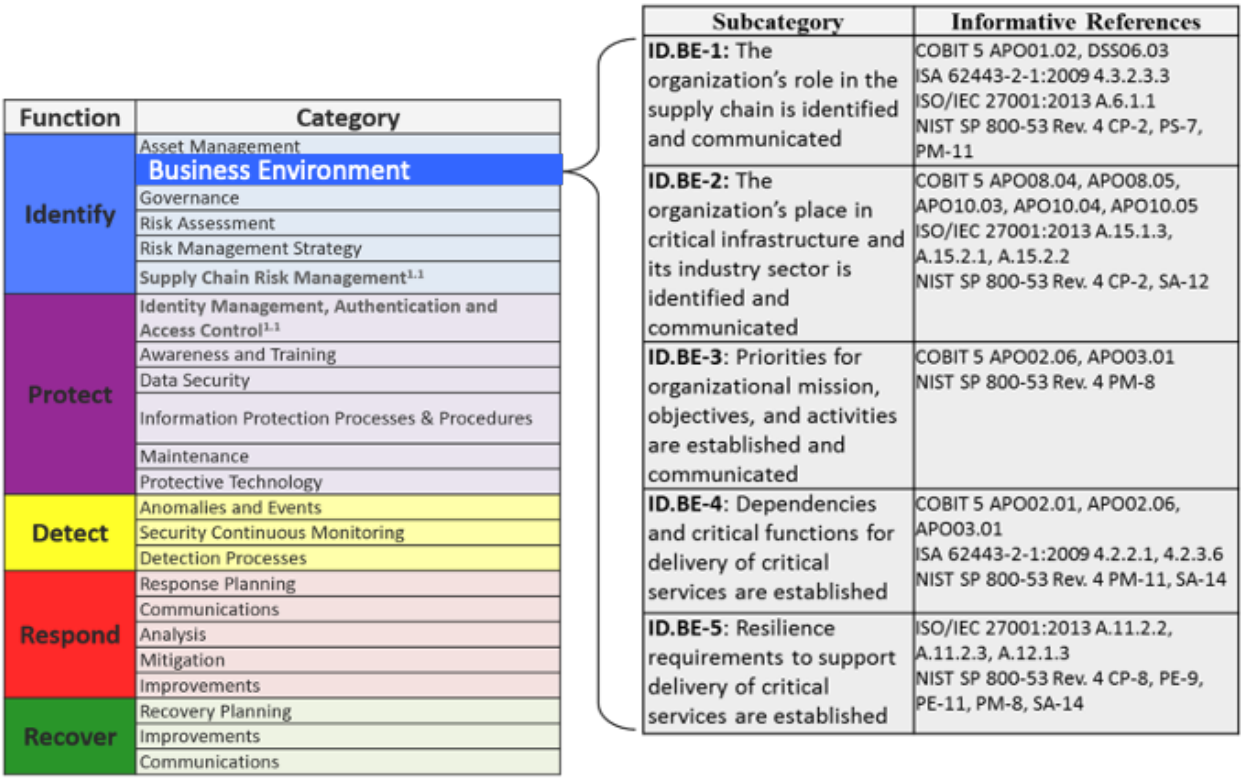

Fig. 4. NIST CSF Subcategories and Informative References Example[12].

3.2. CSF Profiles

A CSF Profile (Profile) is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization.[13] Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).

A Target Profile offers a prioritization of NIST CSF Subcategories based on priority mission and operational considerations for a specific community, industry, or group of stakeholders, such as the genomics community. Target Profiles serve as a useful starting point for identifying and engaging in discussions about cybersecurity activities and outcomes that are important to the Profile's user community. Within an organization, Target Profiles offer a consistent way to discuss cybersecurity objectives across organizational roles—from senior leadership to technical implementors—using common terminology. Individuals within the organization may use the Profile to prioritize the allocation of resources to cybersecurity improvements or to address areas of specific risk.

Profiles are oriented around an organization's Mission Objectives, high-level goals that must be achieved for the organization to succeed in meeting its primary mission. The Mission Objectives provide the necessary context for an organization to manage its cybersecurity risk as it relates to a specific mission need. Profiles identify the CSF Subcategories that are especially relevant to

[12] Adapted from: The Framework for Improving Critical Infrastructure Cybersecurity Presentation: https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview.
[13] NIST Cybersecurity Framework, Section 2.3.

each Mission Objective and suggest how those CSF Subcategories should be prioritized. An organization can adapt the Mission Objectives and CSF Subcategory prioritization to fit its unique needs.

Organizations use both Current and Target Profiles. Current Profiles describe the as-is status of an organization in achieving each Subcategory. Target Profiles described the desired to-be state the organization would like to achieve. Individuals within the organization may use the Current and Target Profiles to analyze the cybersecurity program and to prioritize allocation of resources to cybersecurity improvements.

3.3. Applying the Cybersecurity Framework to Genomic Data

This CSF Profile for Genomic Data prioritizes CSF Core Subcategories designed to help an organization protect genomic data throughout the data lifecycle (illustrated in **Fig. 1**). Organizations can use the Profile guidance, rationale, and considerations to examine and potentially improve their existing cybersecurity practices and activities.

Organizations may apply the CSF Profile to their organization by first identifying and describing their mission and business objectives. Section 5 details 12 Mission Objectives for the genomic data ecosystem developed with stakeholder input. Organizations may apply these or similar Mission Objectives or develop their own. Each organization should prioritize Mission Objectives based on their requirements and strategic goals.

Next, organizations can crosswalk their Mission Objectives to the CSF Profile's Subcategories, using the tables in Sec. 6 to identify priority Subcategories. They can use the General Rationale and Mission Objective Specific Considerations from Sec. 6 to prioritize the Subcategories for their organization. During this activity, organizations should consider any constraints or guidance (e.g., applicable state laws, policies, standards), risks, and other influencing factors. At each step, organizations can document rationale, considerations, and any additional informative references.

Based on those priorities and adjustments, organizations should examine their current cybersecurity activities and priorities. Organizations can then identify any gaps between current cybersecurity capabilities and the target state identified by the Profile's priorities or the organization's adjustment of the Profile's priorities. This gap analysis can help an organization determine if re-allocation of cybersecurity resources toward higher priority capabilities would help them achieve those prioritized Subcategories and therefore, better achieve their organization's Mission Objectives. Organizations that process human genomic data should also examine the Privacy Framework Subcategories to address privacy concerns more fully, such as managing donor consent preferences throughout data processing.

4. Profile Development Methodology

Developing a CSF Profile is a collaborative stakeholder-driven process. The input from a diverse group of stakeholders who are experts across the genomics community helps to ensure that the Profile aligns cybersecurity outcomes with business and mission requirements. This section describes how the NCCoE gathered input and garnered consensus from a diverse group of stakeholders to produce this Profile.

Between October 2022 and February 2023, the NIST NCCoE hosted five virtual working sessions with 33 genomics community stakeholders from government, universities, a non-profit think tank, and industry, including instrument manufacturers and cloud service providers. The working sessions sought to develop and prioritize Mission Objectives for the CSF Profile for Genomic Data and to prioritize CSF Categories for each Mission Objective. The NCCoE facilitated the working sessions to solicit input from the stakeholders, who served as subject matter experts to identify objectives specific to managing and maintaining genomic data ecosystems at their organization.

The first working session introduced stakeholders to the NIST CSF and provided an overview of the approach for developing this Profile. The next two working sessions included brainstorming and focused discussions to describe organizational Mission Objectives from the genomic data stakeholder community perspective and prioritize the Mission Objectives based on their importance to organizational operations. The resulting 12 prioritized Mission Objectives are described in Sec. 5 of this Profile. In the final two working sessions, the stakeholders conducted scoring activities designed to prioritize CSF Categories for each Mission Objective.

Following completion of the working sessions, the NCCoE team of subject matter experts in genomic data, cybersecurity, and privacy analyzed the outputs from the stakeholder Category prioritization and used them to inform CSF Subcategory priorities for each Mission Objective. During CSF Subcategory discussions, the NCCoE team documented general rationales for why an organization would prioritize a Subcategory along with specific rationale for prioritizing Subcategories for each Mission Objective. The details from this analysis are summarized in Sec. 6 of this document, serving as the primary content in this CSF Profile for Genomic Data.

5. Genomic Data Mission Objectives

The working session discussions resulted in 12 Mission Objectives that characterize high-level critical operational needs to an organization to meet its primary mission in the genomic data processing ecosystem. The Mission Objectives are operational imperatives. In some cases, the Mission Objectives are focused on cybersecurity or privacy needs, though the overall set of objectives are broader than cybersecurity or privacy. While this Profile focuses on cybersecurity activities and outcomes, many of these Mission Objectives also rely on privacy activities and outcomes that can be found in the Privacy Framework Core.

During the working sessions stakeholders ranked the Mission Objectives based on priority levels shown in **Table 2**. Their prioritization is meant to be informative rather than prescriptive. Each organization should consider its own goals and priorities when consulting this Profile and adjust how the organization may apply guidance accordingly. Descriptions for each Mission Objective follow, including rationale for the prioritization and a keyword used to identify the Mission Objective in the tables in Sec. 6.

720 **Table 2.** CSF Profile for Genomic Data Mission Objectives.

Priority	Mission Objective (Keyword)
1	Manage provenance and data integrity throughout the genomic data lifecycle (**Data**)
2	Preserve privacy of relatives (**Relatives**)
3	Identify, model, and address security and privacy risks to genomic data (**Risks**)
4	Manage informed consent throughout the genomic data lifecycle (**Consent**)
5	Preserve privacy of donors (**Donors**)
6	Manage authorized data access (**Access**)
7	Maintain trust and manage reputational risk (**Trust**)
8	Facilitate research and education to advance science and technology (**Research**)
9	Maintain compliance to laws and regulations (**Legal**)
10	Protect intellectual property (**IP**)
11	Enable and preserve sample diversity (**Diversity**)
12	Promote the use of secure platforms for the controlled sharing of genomic data (**Platforms**)
Note:	*This CSF Profile addresses cybersecurity aspects of these Mission Objectives; the Privacy Framework Profile will address the privacy aspects of these same Mission Objectives.*

721 ## 5.1. Objective 1: Manage provenance and data integrity throughout the genomic
722 data lifecycle

723 The complex genomic data lifecycle introduces challenges in maintaining the data integrity and
724 authenticity required for use by the genomics community. Effectively managing the genomic
725 data lifecycle improves data security, integrity, and provenance. Provenance describes the source
726 and processing of the genetic information including sequence information, annotations, derived
727 data, data version, software version, software configurations, and analysis parameters.
728 Provenance in the genomic data lifecycle can be maintained when introducing any data series.
729 Data integrity protections can include assurances that data are correct and that the chain of
730 provenance remains intact. Maintaining genomic data integrity throughout the data lifecycle
731 requires hardware and software security, effective data storage and analysis, as well as secure
732 dissemination and sharing of data sets through interconnected systems. Sharing genomic data is
733 uniquely important in this process because it becomes increasingly difficult to preserve original
734 source rights and privacy rights over time as data is shared with third parties. Integrating data
735 integrity assurances early in the data lifecycle, such as during research study design, also
736 improves security outcomes.

737 **Rationale:** Data provenance and integrity were identified as the highest priority because of their
738 impact on all Mission Objectives. If the data cannot be trusted, then the research, investigations,
739 and consumer services will be inherently flawed.

5.2. Objective 2: Preserve privacy of relatives

The commonality of genomic data among deceased, living, and future biological relatives can reveal health conditions, disease histories, unknown relations, and permit discrimination of identifiable populations. The sensitivity of information that can be revealed regarding donor relatives warrants careful management and control of genomic data. Organizations can identify where privacy risks to relatives may arise due to an organization's role in the genomic data processing ecosystem as well as in their internal operations. Information about relatives can be safeguarded from potential privacy harms such as genetic association (for example, social, economic, and psychological) or the non-consensual usage of their genomic information. These harms to relatives can be considered throughout the data processing lifecycle (for example, determining how data sources interact and what can be shared, implementing reasonable retention policies, and instituting processes for addressing privacy risks to relatives).

Rationale: Relatives' privacy was rated highly because of the number of people impacted and the fact that relatives are not involved in the process. Relatives may not be aware of the impact and do not have the opportunity to provide consent for the use of or inferences that may come from donor's genomic data. As described in Sec. 2.3, some aspects of privacy rely on cybersecurity, such as controlling access to information about relatives that may be included when processing genomic data. The stakeholders wanted to highlight the privacy impact on relatives because it can potentially be overlooked and may change with advances in technology.

5.3. Objective 3: Identify, model, and address security and privacy risks to genomic data

Genomic information is subject to a variety of evolving security threats, from hardware and software vulnerabilities to misuse of information, and privacy problems, such as dignity loss, discrimination, loss of trust, or loss of autonomy as a result of unanticipated revelation of health conditions or progeny. Addressing risks to genomic data protects bioeconomy interests from malicious outcomes such as discrimination, exploitation, and abuse. The genomics community can use security and privacy standards and risk models (such as the NIST Cybersecurity and Privacy Frameworks) for processing genomic information to address known security threats and privacy problems. Improved understanding of risks can help organizations select appropriate practices; reviewing and updating them to ensure they address emerging capabilities that introduce new risks, such as quantum computing.

Rationale: This Mission Objective was rated highly because the selection and effectiveness of cybersecurity and privacy capabilities depends on the ability to identify relevant cybersecurity threats and vulnerabilities and potential privacy problems as well as their potential impact.

5.4. Objective 4: Manage informed consent throughout the genomic data lifecycle

Organizations institute policies and practices for obtaining and maintaining meaningful informed consent prior to collecting or processing human donor information and to ensure that consent requirements travel with genomic data when it is shared. At a minimum, meaningful informed consent includes providing these donors information about the organization's data processing practices (sometimes referred to as a privacy notice), including operational activities and privacy

and security protections, donor rights, and privacy points of contact in a way that clarifies the terms of consent. Organizations can ensure that their operational practices conform to the agreements they make with donors through the consent process. Procedures to review consent as needed are established to ensure the operational environment and donor consent remain in sync over time, such as when technologies enable new processing capabilities or when genomic data is shared with new partners. Special care needs to be taken regarding the unconsented use of secondary data subjects (relatives), which may require improvements in consent models that ensure consent is meaningful for all parties.

Rationale: While much of consent relies on privacy processes, cybersecurity plays a role in ensuring data processing activities are consistent with consent through appropriate access controls and data protection mechanisms. Donors will be hesitant to share their genomic data if organizations do not require their consent, manage the data according to that agreement, and communicate the benefits of participation. Prioritization of this Mission Objective is impacted by the fact that it applies only to human genomic data.

5.5. Objective 5: Preserve privacy of donors

Processing human genomic data presents some unique privacy challenges. Privacy risks can occur throughout the data processing lifecycle. Examples include determining how data sources interact and what can be shared, implementing reasonable retention policies, and instituting processes for addressing privacy risks to relatives. Organizations can review these recommendations and consider applying this guidance in the context of their role in the genomic ecosystem, taking into consideration both the needs and expectations of genetic donors and their relatives, as well as the safeguards and limitations of individual informed consent. In addition, appropriate security safeguards help protect against loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of genomic data.

Rationale: Donors will be hesitant to provide their genomic data unless they trust that organizations will follow appropriate privacy practices. As described in Sec. 2.3, some aspects of privacy rely on cybersecurity, such as protecting information about donors when processing genomic data. By managing risks to the donor's privacy, organizations maintain the donor's trust and are better able to comply with local, national, and international laws and regulations. Prioritization of this Mission Objective is impacted by the fact that it applies only to human genomic data.

5.6. Objective 6: Manage authorized data access

Without certain precautions, genomic data can be accessed and exploited by unauthorized users. Organizations can establish appropriate data access controls in controlled environments that manage access authorization to genomic data and prevent unauthorized usage. Establishing controls with appropriate levels of access enables authorized usage, providing information containment without impacting necessary activities such as data analysis. Data access can be granted solely from a managed authority. These controls manage who can access data, who has authority to grant access, and what permissions can be granted. These permissions can be modified or revoked aligned with consent agreements. This type of dynamic consent

management translates directly to authority management to both prevent unauthorized access and manage authorized access.

Rationale: This Mission Objective's capability to grant access to authorized users and prevent unauthorized usage enables other mission objectives.

5.7. Objective 7: Maintain trust and manage reputational risk

Organizations manage reputational risks to maintain credibility and a positive public perception. This trust relationship helps donors feel comfortable participating in genomic data activities and ensures that the public may continue deriving value from those activities. Trust also impacts an organization's ability to collaborate effectively with other organizations and throughout the genomics community. It is vital that reputational risk management and trust building activities be tailored to reflect the needs of different subgroups with genetic commonalities (for example, different racial and ethnic subgroups, those with similar conditions or diseases) and to address privacy problems. Organizations can build and maintain the trust of donors through responsible and effective genomic data management, privacy, and security practices along with the legal and regulatory compliance described in other Mission Objectives.

Rationale: Individuals need to trust organizations before they will participate in genomic data activities. Failure to maintain trust and manage reputational risk could put other Mission Objectives at risk when organizations or individuals decide not to collaborate or work with an organization.

5.8. Objective 8: Facilitate research and education to advance science and technology

Investments in genomic research and education that will train the next generation of geneticists and biologists can help unlock new scientific and technological breakthroughs. Ways to facilitate genomic research and education include providing hands-on guidance and best practices; supporting collaborative genetic research; and supporting the safe use of genetic information to improve the health of our populations and environment (for example, "One Health"[14]). Ensuring clear communication and understanding between scientific and cybersecurity professionals for safe storage and management of genomic data can prevent potential data loss and disruptions to research. Maintaining the integrity and availability of the research environment can also help ensure the reproducibility of a study.

Rationale: Organizations focused on research and education prioritized this Mission Objective higher than others. Research and education unlock the full potential and usage of genomic data. This Mission Objective overlaps with other Mission Objectives (1, 3, 6, 12) that support authorized data sharing, data quality, and comprehensive data sets.

5.9. Objective 9: Maintain compliance to laws and regulations

Organizations processing genomic data are required to comply with national and international laws and regulations. Organizations can make risk-based determinations regarding which

[14] https://www.cdc.gov/onehealth/index.html

858 countries to maintain operations in that best align their business priorities with the constraints of
859 applicable laws and regulations. Organizations can ensure their activities support Good Practices
860 (GxP) and other standards of practice. International privacy rights may impose unique challenges
861 that require stricter compliance with laws and regulations.

862 **Rationale:** Compliance with laws and regulations represents the foundation for processing and
863 protecting genomic data. While complying with laws and regulations is mandatory to conduct
864 business and manage reputational risk, it was ranked lower due to the increased focus on Mission
865 Objectives that address issues beyond compliance.

866 5.10. Objective 10: Protect intellectual property

867 Safeguarding intellectual property is a core function of many organizations. Organizations
868 working with genomic data and developing intellectual property, such as trade secrets or
869 patentable information, protect these assets and associated business interests. Some
870 organizational operations require indefinitely sequestering genomic information and associated
871 analyses until they can be shared or disclosed. Securing intellectual property also helps establish
872 and/or trace ownership.

873 **Rationale:** This Mission Objective broadly represents an inherent component of business
874 operations. Organizations will continue to own and protect their inventions and investments, and
875 the priority of this Mission Objective will reflect each organization's specific requirements for
876 their own intellectual property.

877 5.11. Objective 11: Enable and preserve sample diversity

878 Human genomic data sets have historically lacked population diversity and under-protected
879 vulnerable groups. Through sample diversity, organizations can access genetic variants that
880 allow for a more comprehensive and inclusive understanding of diverse populations, improved
881 research and health outcomes, and reduced privacy risk. Sample diversity supports fairness and
882 protects vulnerable groups.

883 **Rationale:** This Mission Objective rated lower because the activities required to conduct this
884 Mission Objective involve processes that happen prior to the genomic data collection.
885 Additionally, this Mission Objective applies to all other Mission Objectives processing human
886 genomic data.

887 5.12. Objective 12: Promote the use of secure platforms for the controlled
888 sharing of genomic data

889 Many organizations prefer to bring the people to the data rather than sharing the data across
890 multiple environments. This type of secure platform can facilitate uploading, analysis,
891 collaboration, and help control downloading genomic data. The benefits of this approach include
892 the ability to enforce consistent security practices that manage provenance, ensure data integrity,
893 restrict access to authorized entities, and enhance incident/breach response while enabling safe
894 and controlled use of the genomic data. Such platforms can also support the implementation of
895 emerging technologies and international standards for transfer of clinical and administrative data
896 between software applications used by various healthcare providers.

Rationale: While the potential to increase the effective, controlled sharing of genomic data was considered a high priority for stakeholders, provisioning potential platforms was considered less important because not all organizations play a direct role in providing these platforms. Since there are other mechanisms for data access and confinement, it received a lower priority ranking compared to the rest of the Mission Objectives.

6. Priority Subcategories by Mission Objective

Following the methodology outlined in Sec. 4, NCCoE working sessions led the stakeholders through a process to score what they considered the most important CSF Categories for implementing each Mission Objective. This section presents the results of analyzing the stakeholders' Category prioritization and related discussions to prioritize the selection of the 108 CSF Subcategories for each Mission Objective.

Table 3 through **Table 48** summarize the information, presenting one table for each of the 23 CSF Categories. Each Subcategory was assigned High, Moderate, or Other priority, along with a rationale to help an organization understand the relative importance of a Subcategory to a Mission Objective.

The Subcategories' priority importance is indicated in each Table by:

- Three dots (●●●) for High Priority: These represent the most critical Subcategories for enabling a Mission Objective that should be addressed most immediately given available resources.
- Two dots (●●) for Moderate Priority: These Subcategories should be the next priority after implementing High Priority Subcategories and may become higher priority in certain contexts or environments to implement a given Mission Objective.
- One dot (●) for Other Priority: Subcategories that are important to the overall cybersecurity of a Mission Objective but may not require the same level of urgency as higher priority Subcategories. Note that "Other Priority" does not equate to low priority. All CSF Subcategories should receive consideration.

Although organizations should develop cybersecurity strategies that address all CSF Subcategories, the prioritization provides adaptable guidance that suggests cybersecurity capabilities that will provide the greatest impact toward meeting Mission Objectives for organizations in the genomics community.

Table 3 through **Table 48** present the detailed results of this Subcategory analysis. As shown in **Fig. 5**, each table starts with the description of the CSF Category along with comments collected from the stakeholders during the working session. The numbers 1 to 12 along with the keyword in the table align to the 12 Mission Objectives from Sec. 5 (**Table 2**). Each row identifies the priority of the Subcategory for every Mission Objective using the dots.

Each table includes columns for General Rationale and Mission Objective Specific Considerations. The General Rationale column provides organizations with Mission Objective-agnostic content that may inform an organization's prioritization of a Subcategory. The Mission Objective Specific Considerations column provides organizations with context specific to a given Mission Objective for why a Subcategory was elevated in priority. The Tables use the acronym MO for Mission Objective for brevity.

Some cybersecurity activities can introduce privacy risks that must be considered when implementing cybersecurity Subcategories. Also, the Mission Objectives in this Profile are supported by privacy activities and outcomes, in addition to cybersecurity Subcategories. Cybersecurity and privacy practitioners should coordinate when determining how to best apply this Profile within their organization. Additionally, reviewing NIST Privacy Framework Subcategories and identifying those that support these Mission Objectives, as well as other organization-specific Mission Objectives that may warrant privacy considerations, will enhance an organization's cybersecurity and privacy posture.

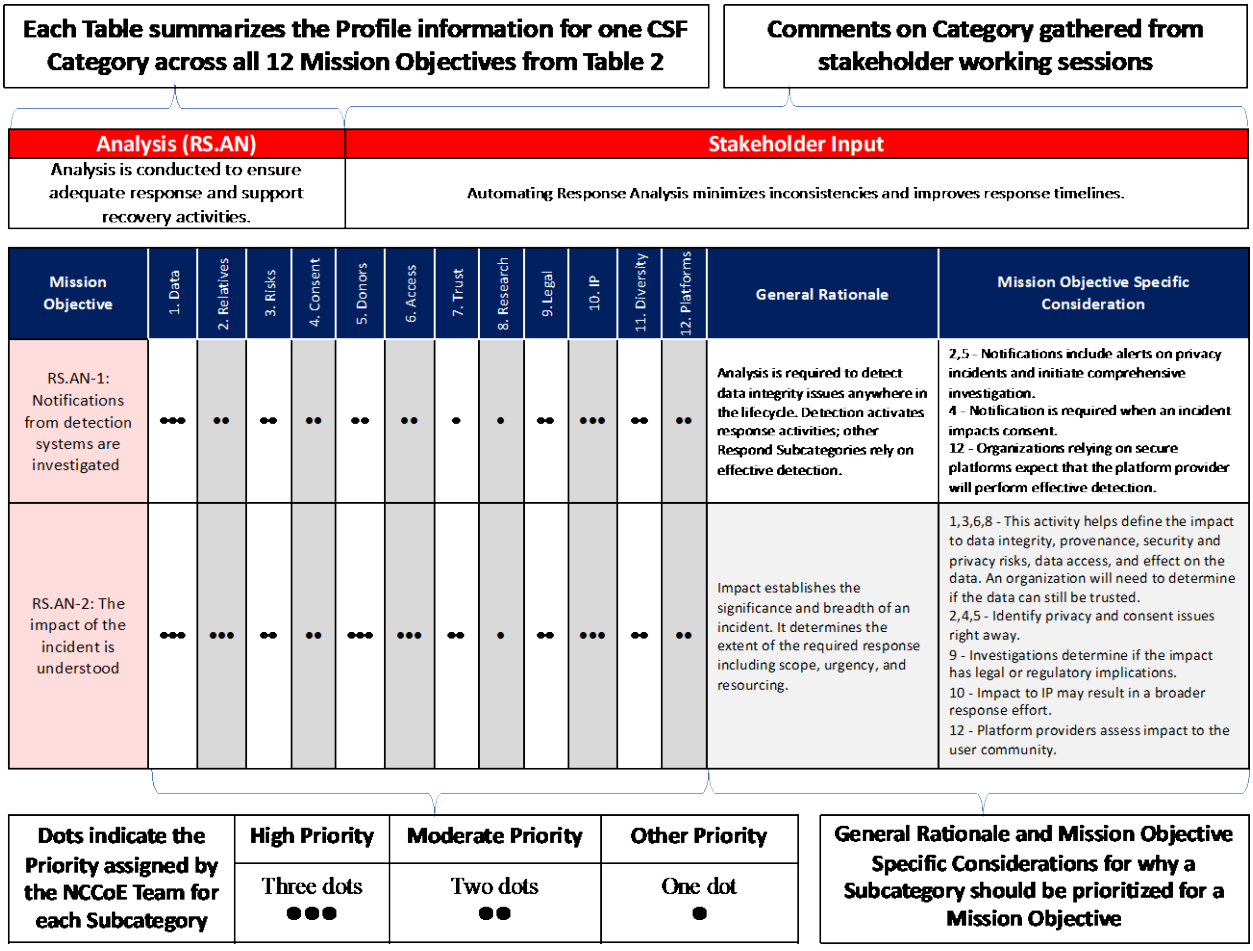

Fig. 5. Sample Subcategory Table with Descriptions.

947 **Table 3.** IDENTIFY: Asset Management Category and Stakeholder Input.

Asset Management (ID.AM)	Stakeholder Input
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	*An accurate inventory supports categorizing assets, controlling access and accounts, the processes to identify IP and other sensitive data, and the ability to manage data as an asset. Management includes knowing where the data was used but may not include where the data came from (provenance).*

948 **Table 4.** IDENTIFY: Asset Management Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.AM-1: Physical devices and systems within the organization are inventoried	●●	●●	●●	●●	●●	●●●	●	●●	●●	●●●	●●	●●●	Manage physical assets to secure data stored, identify risks, and secure the analysis pipeline. Physical device asset management is rated a lower priority than managing virtual or software assets because it is generally considered a less likely attack vector.	6,10,12 - Physical access was considered higher priority for managing unauthorized access to data, protecting IP, and securing data analysis pipelines. 11 - Physical location may affect sample diversity; point of collection may vary from data processing location.
ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●●●	●●●	●●●	●●●	●	●●●	●●	●●●	●●	●●●	Software is considered a more likely attack vector and thus a higher priority than hardware to manage access, identify risks, and protect intellectual property. Software asset management helps identify potential risks to data integrity, provenance, IP protections, and platforms.	1 - Software inventory supports managing data integrity and provenance. 2,4,5 - Software Asset Management provides useful inputs for privacy risk management and requirements including managing consent. 10 - Software may be IP. 11 - Need to identify any software bias that impacts sample diversity.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.AM-3: Organizational communication and data flows are mapped	●●●	●●●	●●	●●●	●●●	●●●	●	●●●	●●	●●●	●●	●●	Managing data flows helps determine where and how to manage security and privacy risks and requirements throughout the genomic data lifecycle.	1,3,6,12 - Communications and data flows are key components for identifying and managing risks to genomic data integrity, provenance, access, and platforms throughout the genomic data lifecycle. 4 - Understanding communications and data flows facilitates management of informed consent, which travels with the data wherever it flows. 11 - Data flows may indicate data sources (provenance) and influence sample diversity.
ID.AM-4: External information systems are catalogued	●●●	●●	●●	●●	●●	●●●	●	●●●	●●	●●●	●●	●●●	Organizations need to identify external systems that handle genomic data to include them in asset management processes. Most genomic organizations rely on and exchange data with external systems to perform some set of analysis functions during a data processing workflow.	1,3,6,12 - Manage where data is shared with external systems to identify risks to genomic data integrity, provenance, access, and platforms throughout the lifecycle. 4 - Understanding external systems that are part of data processing facilitates management of security capabilities that support informed consent, which travels with incoming and outgoing data.
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	●●●	●●	●●●	●●	●●	●●●	●●	●●	●●	●●●	●●	●●	Prioritize resources based on risks to genomic data, privacy, consent, unauthorized access, research outcomes, IP, and ability to process (e.g., on a platform).	2,4,5 - For human genomic data, prioritize privacy-related assets and requirements. 9 - Know potential risks to legal/regulatory compliance and prioritize assets accordingly. 11 - Enabling sample diversity requires prioritization of how organizations collect data.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	●●	●●	●●●	●	●●	●●	●●	●●	●●	●●●	●●	●●●	Defining roles and responsibilities helps inform practices for access controls, training, and other areas. Those interacting with genomic data need to understand their responsibilities in securing the data, including communication with third-party stakeholders.	2,4,5 - Understand how cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders support privacy objectives. 9 - Laws and regulations may stipulate specific cybersecurity and privacy roles and responsibilities.

949

950 **Table 5.** IDENTIFY: Business Environment Category and Stakeholder Input.

Business Environment (ID.BE)	Stakeholder Input
The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	*ID.BE sets the context for an organization's use of genomic data along with legal and regulatory compliance, and associated security and privacy requirements.*

951 **Table 6.** IDENTIFY: Business Environment Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.BE-1: The organization's role in the supply chain is identified and communicated	●●●	●●●	●●●	●●●	●●●	●●●	●●	●●●	●●●	●●●	●●●	●●●	ID.BE-1 directly links to the supply chain Category. The organization's role in the genomics supply chain can define priorities, expected outcomes, and potential risks to genomic data integrity, provenance, or privacy.	1,12 - Supply chain considerations apply across the lifecycle (MO1) and may be best addressed through using a secure platform (MO12). 2,4,5 - The organization's role in the genomics supply chain helps identify privacy-supporting cybersecurity requirements. 3 - Threat modeling should include supply chain considerations. 10 - The organization's role in supply chain may help identify risks to IP.
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	●●	●●●	●●●	●●●	●●●	●●	●●	●●	●●	●	●	●	Genomic data is not closely tied to critical infrastructure but should be factored in through sector-specific risk analysis. Organizations consider their role in the industry sector and genomic data processing ecosystem when evaluating risk.	3,5,9 - Organizations in the healthcare sector consider applicable healthcare laws, such as Health Insurance Portability and Accountability Act (HIPAA), as well as other related laws and regulations as part of their risk management approach. 6 - The impact of unauthorized data access may be defined by an organization's role in the genomic sector and genomic data lifecycle. 12 - In some sectors, use of a secure platform may help build in security and privacy requirements.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	●●	●●	●●	●●	●	●●	●●	●●●	●●●	●●●	●●●	●●	Understanding organizational objectives and priorities helps prioritize appropriate MOs and related CSF Subcategories.	2,4,5 - Privacy requirements that rely on cybersecurity activities should be identified, prioritized, and communicated. 10 - If IP exists, protection of IP will be prioritized. 11 - If sample diversity is prioritized, then it will impact other activities.
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	●●	●	●●●	●	●	●●	●●	●●●	●●	●●	●	●●	Genomic data is not typically tied to delivery of critical services. However, some services such as those that are critical from healthcare organizations may depend on genomic data (for example, genomic sequencing for patients in critical care units). In such situations, dependencies and criticality factor into Subcategory prioritization.	1,3 - The data lifecycle is dependent on data quality to support essential services. The impact of these dependencies should be incorporated into risk management. 12 - Platform providers should understand criticality of their services.
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	●	●	●●	●	●	●	●	●●	●●	●	●	●	Resilience and availability are typically not the highest priority cybersecurity capabilities for genomic users. Exceptions may include healthcare, platform providers, and business applications.	3,9,10 - Resilience may factor into security risks, legal and regulatory compliance, and/or protection of IP. 8,12 - Resilience may be a high priority for organizations providing a service that other organizations are highly dependent on, such as research organizations, healthcare, and secure platform providers.

952 **Table 7.** IDENTIFY: Governance Category and Stakeholder Input.

Governance (ID.GV)	Stakeholder Input
The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	*Governance ranked high overall compared to other Identify Subcategories. It aligns the organization's priorities to meet legal, regulatory, and policy expectations for security and privacy including HIPAA, General Data Protection Regulation (GDPR), Federal Information Security Modernization Act (FISMA), etc.*

953 **Table 8.** IDENTIFY: Governance Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.GV-1: organizational information cybersecurity policy is established and communicated	●●●	●●●	●●●	●●●	●●●	●●	●●●	●●●	●●●	●●●	●●●	●●●	Policy establishes organizational expectations, processes, responsibilities, and priorities. Policies embed legal, regulatory, security, and privacy requirements.	1 - Policy includes data integrity and provenance requirements. 2,4,5 - Policy addresses privacy and consent requirements including protecting relatives' privacy. 3,6,10 - Policy includes security protections. 11 - Policies could help enable and preserve sample diversity.
ID.GV-2: Cybersecurity roles & responsibilities are coordinated and aligned with internal roles and external partners	●●●	●●	●●●	●●●	●●	●●	●●●	●●●	●●●	●●●	●	●●●	Roles and responsibilities establish accountability for internal and external partners interacting with genomic data. Privacy requires close coordination between cybersecurity and privacy roles.	Each MO will have unique roles and responsibilities associated with cybersecurity activities.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	●●●	●●●	●●●	●●●	●●●	●●	●●	●●●	●●●	●●	●●	●●●	Laws and regulations should be implemented through organizational policy, processes, and procedures. Security and privacy requirements, including civil liberties, should be prioritized across all MOs to meet legal requirements.	2,4,5 - Failure to comply with cybersecurity or privacy laws and regulations could deter donors from participating. 7 - Reputation and trust will be damaged if laws and regulations are not followed. 9 - This Subcategory directly supports achievement of this MO. 11 - Sample diversity may need to be legislated.
ID.GV-4: Governance and risk management processes address cybersecurity risks	●●●	●●●	●●●	●●●	●●●	●●	●●	●●●	●●●	●●●	●●●	●●●	Risk management processes help integrate cybersecurity and privacy activities into each MO.	1 - Risk management should be built into the data lifecycle. 2,4,5 - Privacy risk management is also included, with care to address relatives' privacy. 7 - Risk Management processes incorporate trust and reputation management. 10 - Risk management processes help identify and prioritize appropriate IP protections. 12 - Secure platforms integrate appropriate cybersecurity and privacy risk management.

954

955 **Table 9.** IDENTIFY: Risk Assessment Category and Stakeholder Input.

Risk Assessment (ID.RA)	Stakeholder Input
The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	*Risk assessment helps organizations connect trust to operations and demonstrates compliance. External vendors submit security plans and obtain authority to operate prior to using federal systems. Identify important potential risks including managing supply chain risks. Risk modeling incorporates requirements from regulations, laws, contracts, and dependencies. Risks may be introduced not only from data provenance, but also when organizations use a processing environment for their analysis.*

956 **Table 10.** IDENTIFY: Risk Assessment Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.RA-1: Asset vulnerabilities are identified and documented	●●	●	●●●	●	●	●●	●●	●●●	●●	●●●	●●	●●	Asset vulnerability management is a basic cyber-hygiene practice that should be expected in any environment. Asset vulnerabilities may expose genomic data to cybersecurity and privacy risks.	1 - Asset vulnerabilities threaten data integrity. 3,6,10,12 - Asset vulnerabilities help identify risks to data processing environments. 11 - Identifying vulnerabilities that threaten data integrity may help preserve sample diversity.
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	●	●	●●●	●	●	●	●	●●	●●	●●	●	●●	This Subcategory was not as highly prioritized as other Identify Subcategories because there are not many sources for genomic threat intelligence outside of the BIO-ISAC (Bioeconomy Information Sharing and Analysis Center). As attacks on genomic data increase, organizations should monitor threat intelligence sources. Threat intelligence informs those processing genomic data of specific threat actors and attack vectors to help target protections and cyber investments.	1,3,7,8,10 - Organizations should identify specific threats and active attacks on the types of data processed to focus cyber investments on the most likely attacks. 12 - Platform providers have an additional responsibility to understand threats and protect their environments appropriately.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.RA-3: Threats, both internal and external, are identified and documented	●●●	●●	●●●	●	●●	●●	●●	●●●	●●	●●●	●	●●	Threats should be identified through ID.RA-2, but in the absence of threat intelligence, organizations should perform threat modeling to prioritize protections most likely to be effective.	1,6,10 - Organizations should understand the threats specific to the data they manage to prioritize their cyber protections. 2,4,5 - Impacts to privacy should also be factored into threat identification. 3,8,12 - Threats should be used to calculate risks to processing environments.
ID.RA-4: Potential business impacts and likelihoods are identified	●●	●●●	●●●	●●	●●	●●	●●	●●●	●●	●●●	●●	●●●	Business impact is a primary factor to calculating risks and varies by organization and mission. Understanding the impact of a cybersecurity or privacy incident can help organizations prepare for and prioritize their protection and response capabilities.	1,6,10 - Business impact to data integrity issues should be understood. 2,4,5,6 - Business impacts from unauthorized data access or other risks that impact privacy should be factored in. 3,7,9,10,12 - Business impact to operating environments and the role in their supply chain should be understood.
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	●●●	●●●	●●●	●●	●●●	●●	●●	●●●	●●	●●●	●●	●●●	Risk is calculated from the likelihood of a threat (ID.RA-3), the existence of a vulnerability (ID.RA-1), and the potential business impact (ID.RA-4).	2,4,5 - Organizations determine the impact of cybersecurity risks on privacy. 1,3,6 - Risks to data integrity, provenance, and lifecycle should be determined. 8,10,12 - Risks to operating environments should be determined.
ID.RA-6: Risk responses are identified and prioritized	●●	●●	●●●	●●	●●	●●	●●●	●●●	●●	●●●	●	●●	Risk responses define the actions that the organization will take to mitigate, transfer, accept, or otherwise address risks identified through this assessment. ID.RA-6 informs Response Function activities.	1,8,11,12 - Response communications across organizations participating in the genomic data lifecycle should be coordinated. 2,4,5 - Privacy considerations are factored into risk responses. 7 - Reputational response activities should be included. 9 - Risk responses consider legally required response activities.

957 **Table 11.** IDENTIFY: Risk Management Strategy Category and Stakeholder Input.

Risk Management Strategy (ID.RM)	Stakeholder Input
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	*Risk management strategy may be prioritized lower than performing the risk assessment because of the more practical benefits resulting from an assessment.*

958 **Table 12.** IDENTIFY: Risk Management Strategy Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	●●	●●	●●●	●●	●●	●●●	●●●	●●	●●●	●●●	●	●●	Risk management processes help integrate cybersecurity and privacy activities for each MO.	1,3 - Risk management processes should be integrated into the data processing lifecycle and systems development lifecycle. 2,4,5 - Privacy risk management should be included. 7 - Processes for managing reputational risk should be included. 9 - Legal and regulatory requirements should be included. 12 - Users of a secure platform should be aware of and/or agree to the platform's risk management processes.
ID.RM-2: organizational risk tolerance is determined and clearly expressed	●●	●●	●●	●●	●●	●●	●●●	●	●●	●●●	●●	●●	Risk tolerance helps define triggers and priorities for risk response activities.	1,6,7,10 - Risk tolerance should help define provenance, data integrity, who can access the data, and what might cause reputational harm. 2,4,5 - Risk tolerance should factor in privacy risks. 3 - Risk tolerance can help define when a risk is realized. 9 - Laws and regulations may help define organizational risk tolerance or thresholds.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	●●●	●●	●●	●●	●●	●●	●●●	●	●●●	●●	●●	●●	Any organization with an important role in the sector should understand the potential impact of a sector-specific risk to their business as well as their impacts on others in the sector. Genomics is not closely tied to critical infrastructure, but as an industry sector, there are sector-specific risks that are related to processing genomic data that should be considered in this analysis. Risk tolerance is sometimes considered a more mature capability, and further definition based on sector-specific risk analysis may require even greater maturity.	1,3,6,8,9,10,11,12 - Any organization sharing genomic data throughout the data processing lifecycle should evaluate how their work impacts data integrity and provenance that might be used by the entire genome sector, and the impact of others in the sector to the organization. 9 - Where there are legal requirements regulating the sector, there should be risk thresholds and response activities defined.

960 **Table 13.** IDENTIFY: Supply Chain Risk Management Category and Stakeholder Input.

Supply Chain Risk Management (ID.SC)	Stakeholder Input
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	*Each ID.SC Subcategory describes a process for managing genomic data through its supply chain, which consists of many parties.*

961 **Table 14.** IDENTIFY: Supply Chain Risk Management Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	●●●	●●	●●●	●●	●●	●●	●●	●●	●●	●	●●	●●●	Managing the genomic data lifecycle includes understanding data provenance risks and aligning priorities for all who are interacting with data.	2,5 - Any organization in the genomic data supply chain should preserve privacy. Privacy risk may arise even when processing data that has been aggregated or de-identified (including anonymized data). 4 - Consent follows the data throughout the lifecycle. 6 - Data access requirements apply to each organization in the supply chain. 7 - Reputation and trust are managed across all organizations processing the data. 8 - Research relies on data quality maintained in the supply chain. 9 - Legal requirements apply throughout the supply chain. 11 - Sample diversity should be preserved throughout the supply chain. 12 - Secure platforms manage how they acquire and then share data and analysis.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	●●●	●●●	●●●	●●	●●●	●●	●●	●●	●●	●	●●	●●	Suppliers should be included in risk processes. Genomic data lifecycles include interconnections between different types of third parties, which introduce risk. Organizations develop cyber supply chain risk assessment processes tailored to meet privacy, data integrity, provenance, and data access requirements. Priority for this Subcategory may be similar to ID.SC-1 but is applied to the suppliers and third-party partners, not just the organization.	1,3,8,12 - Managing the data lifecycle includes understanding data provenance risks and aligning priorities for all who interact with the data. 2,4,5 - Systems and organizations interacting with data should participate in the supply chain risk assessment to assess privacy requirements.
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	●●●	●●●	●●	●●●	●●●	●●	●●	●●	●●	●●	●●	●●	Contracts define and enforce cybersecurity, privacy, and supply chain requirements. The genomic lifecycle should use contracts to define data processing requirements between parties.	1 - Data integrity and provenance requirements should be included in contracts. 2,4,5 - Contracts include privacy requirements. 3,6,7,8,9,12 - Contracts address data sharing requirements including risk management, data access, response coordination, legal/regulatory requirements, and expectations to protect IP and research results. 11 - Sample diversity should be addressed contractually, when applicable.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	●●	●●	●●	●●	●	●●	●●	●	●●	●	●●	●●●	Auditing suppliers and third parties was considered a more mature capability that will help determine if contractual agreements are being upheld. Audits ensure organizations are doing what they agreed to, but these assessments require higher levels of effort and resources. This might not be possible for all organizations if resources are not available.	2 - Because consent cannot be given by relatives, this Subcategory may be even more important for protecting relatives' privacy than donor's privacy. 9 - Laws may require auditing as part of due diligence. 12 - Users of the platform may rely on audit results to verify that protections are in place.
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	●●	●	●●	●	●	●●	●	●	●●	●●	●	●●	Including all parties in these activities was considered a more mature capability that may not be possible for all organizations. Categories under Respond and Recover were ranked as higher priorities by stakeholders rather than response and recovery planning specific to suppliers.	1 - Provenance and data integrity should be maintained when sharing data with other organizations, even during response and recovery operations. 2,4,5 - Privacy requirements should be maintained during response and recovery operations, including ensuring suppliers and third-party providers know what their responsibilities are in supporting the organization with privacy-related response and recovery activities. 6,10 - Data access and IP protections should be maintained during response and recovery operations. 9 - When legally required, response and recovery planning should include all parties involved in processing genomic data. 12 - Organizations using a secure platform should coordinate response and recovery with the provider.

962 **Table 15.** PROTECT: Identity Management, Authentication and Access Control Category and Stakeholder Input.

Access Control (PR.AC)	Stakeholder Input
Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	*Managing access to the data is one of the critical components to managing risks and compliance. Access control applies and cascades down through other controls. Data sharing environments control who has what access with fine granularity while managing authorization for using data according to consent. Access controls can support both confidentiality and integrity of privacy-related data.*

963 **Table 16.** PROTECT: Identity Management, Authentication and Access Control Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	●●●	●●●	●●●	●●●	●●●	●●●	●	●●	●●●	●●●	●●	●●●	Using access control techniques of identity and credential management is a baseline priority for protection of genomic data and typically the first line of defense for system security.	1,3,6,9,10,12 - Organizations need a robust identity and credential management program as an effective defense for protecting organizational information throughout the data processing lifecycle. 2,4,5 - Privacy protections require the ability to manage who accesses data and what they do with the data. 8,12 - Shared environments control data access to manage data integrity and provenance.
PR.AC-2: Physical access to assets is managed and protected	●	●	●●	●●	●	●●	●	●	●●	●●	●	●●	Physical access is a less likely attack vector for genomic data compared with virtual access.	3,6 - Physical access risks are included in risk models along with protections applying to physical environments. 8,12 - Organizations operating data sharing environments may prioritize managing physical access higher.
PR.AC-3: Remote access is managed	●●●	●●●	●●●	●●●	●●●	●●●	●	●●	●●	●●●	●●	●●●	Remote access is a primary attack vector and should be highly prioritized and managed by all organizations. Many genomic teams use cloud environments.	3 - Risks of using cloud environments and others where remote access is prevalent should be incorporated into models. 8,12 - Researchers and shared platforms prioritize the controls around remote access.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	●●●	●●●	●●●	●●●	●●●	●●●	●	●●	●●	●●●	●	●●●	Policies and procedures involved in the management of data and platform access (such as least privilege, role-based access, and separation of duties) were generally prioritized higher, as they provide protections against unauthorized or unwarranted access.	1,3,6,8,10,12 - Least privilege and separation of duties help enforce data access controls in shared environments. 2,4,5 - Privacy protections rely on appropriate management of access through least privilege, separation of duties, and role-based access control (or other more restrictive means).
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	●●	●●	●●●	●●	●●	●●●	●	●●	●●	●●●	●	●●	Protecting infrastructure and the data flows at the network level secures genomic data processed on the organization's network, including when systems share genomic data internally and externally. Network segregation and segmentation enhance other access controls in this Category.	3 - Network integrity controls are important tools for managing security risks. 8,12 - Network integrity controls should be in place in any data sharing environment. 10 - IP should be protected through network integrity controls.
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	●	●	●●	●	●	●●	●	●	●	●●●	●	●●	Identity proofing rated lower across most MOs, since it is a more granular level of access management that may not be applicable in all environments. As organizations implement a zero-trust architecture, they will want to assert authentication for high-risk data interactions.	2,4,5,10 - Wherever highly sensitive data is identified, these capabilities should be prioritized to improve data protections and aligned with efforts to implement other requirements related to a zero-trust architecture.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	●	●●	●●	●	●●	●●	●	●●	●●	●●●	●	●●●	Risk-based authentication of users and devices is generally viewed as a more mature and advanced capability for most organizations, but scored high in situations where a zero-trust architecture is expected to be implemented.	2,4,5,10 - Wherever highly sensitive data is identified, these capabilities should be prioritized to improve data protections and aligned with efforts to implement other requirements related to a zero-trust architecture.

964

965 **Table 17.** PROTECT: Awareness and Training Category and Stakeholder Input.

Awareness and Training (PR.AT)	Stakeholder Input
The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	*Training informs users (privileged and not) how data should be protected and why protection processes are important. People contributing data need to understand what consent means. There is also an awareness aspect to inform potential data users of how to use the technology with the data, protect the data, and not share the data unnecessarily.*

966 **Table 18.** PROTECT: Awareness and Training Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.AT-1: All users are informed and trained	●●●	●●●	●●●	●●●	●●●	●	●●●	●●●	●●●	●●●	●●●	●●	Instructing users how to actively participate in cybersecurity and privacy protections through training maximizes the impact of other security and privacy activities.	2,4,5 - Training should cover privacy-related topics. 7 - Organizations should train users on how to manage reputational risks. 8,12 - Users in data sharing environments should be trained to understand their roles and responsibilities. 10 - Organizations with IP should ensure those with access to IP understand how to protect it.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.AT-2: Privileged users understand roles and responsibilities	●●	●●	●●●	●●●	●●	●●●	●●	●●●	●●●	●●●	●	●●	Organizations should prioritize training for privileged users such as system administrators with elevated privileges who oversee data management permissions, conduct backups, and implement integrity checking mechanisms. System administrators are not typically interacting with the data in the way that system users do (i.e., not directly processing the data), but they do play an important role in ensuring that data protections are managed appropriately.	2,4,5,9,10 - Privileged users should understand what types of sensitive data are on their systems and what legal, regulatory, or compliance constraints apply. 8,12 - Privileged users with access to shared data environments have a higher responsibility to protect the data and the environment.
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	●●	●●●	●●	●●●	●●	●	●●●	●●●	●●●	●●●	●●●	●●	In general, third parties require the same types of training as other users since genomic data protections apply throughout the lifecycle in every processing environment. Contracts do not supersede legal, regulatory, or compliance requirements.	2,4,5 - Organizations should ensure privacy requirements are traveling with the data. Training contractors is often a privacy requirement. This may be a lower priority compared to training all users and privileged users. 6 - Enforce the same data access requirements across all parties. 11 - Third parties who provide samples need to understand requirements for sample diversity.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.AT-4: Senior executives understand roles and responsibilities	●●	●●	●	●●	●●	●	●●	●●●	●●●	●●●	●●	●●	Senior executives need to understand the importance of cybersecurity and privacy as well as how both areas relate to the organization's risk posture, so that they can make informed decisions about how to enable and support the organization's capabilities, provide the resources to support cybersecurity and privacy capabilities, and set the culture for the organization.	2,4,5 - Senior executives should understand their organizational privacy requirements. 7 - Senior executives should be aware of organization risks to reputation and trust. 9 - Senior executives bear legal and regulatory responsibilities. 10 - Senior executives are responsible for preventing IP loss.
PR.AT-5: Physical and information security personnel understand roles and responsibilities	●●	●●	●●●	●●●	●●	●●	●●	●●●	●●●	●●●	●●	●●	Physical and security personnel should be aware of the organization's processing of genomic data and the associated risks to effectively administer cybersecurity and privacy capabilities.	8,12 - In shared processing environments, these roles may be primary in ensuring appropriate protections are implemented, including personnel screening.

967

968 **Table 19.** PROTECT: Data Security Category and Stakeholder Input.

Data Security (PR.DS)	Stakeholder Input
Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. *NOTE: Privacy Framework maps generally to these Subcategories.*	*Data security protects against data loss and corruption as well as managing data integrity and access including privacy protections. Data sharing environments should implement comprehensive data security controls including encryption and controls on who can access, analyze, change, upload, and share data along with auditing all actions.*

969 **Table 20.** PROTECT: Data Security Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.DS-1: Data-at-rest is protected	●●●	●●●	●●●	●●	●●●	●●●	●	●	●●	●●●	●●	●●●	Encryption is a primary method for protecting data at rest and should be implemented whenever sensitive data is involved. Additional measures may be required to protect genomic data.	2,4,5,6,10 - Encryption prevents unauthorized access to sensitive data. 8,12 - Encryption supports data protections in data sharing environments.
PR.DS-2: Data-in-transit is protected	●●●	●●●	●●●	●●	●●●	●●●	●	●	●●	●●●	●●	●●●	Encryption is a primary method for protecting data in transit and should be implemented whenever sensitive data is involved. Additional measures may be required to protect genomic data.	2,4,5,6,10 - Encryption prevents unauthorized access to sensitive data. 8,12 - Encryption supports data protections in data sharing environments.
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	●●●	●●	●●	●	●●	●●	●	●	●●	●●●	●●	●●	Asset removal may not be the most probable attack vector, but prevention remains a best practice particularly in data sharing environments. Data disposition should be carefully managed as part of privacy practices and asset disposition. Organizations should consider implementing this Subcategory as part of organization's insider threat program.	2,4,5 - Managing data on assets, particularly through the disposition process, supports implementation of privacy requirements, which often include data retention and disposition constraints. 8,12 - Data sharing environments should have tight controls around asset removal, transfer, and disposal.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.DS-4: Adequate capacity to ensure availability is maintained	●	●	●	●	●	●	●	●	●	●●	●	●●	Capacity and availability were not prioritized as high as other Protect Subcategories for genomic data. However, organizations with higher availability requirements manage capacity to ensure they can meet those requirements.	8,10 - Capacity and availability will be higher priority in data sharing environments particularly if they are for time-sensitive applications such as healthcare.
PR.DS-5: Protections against data leaks are implemented	●●●	●●●	●●●	●●●	●	●●	●●	●●	●●●	●●●	●	●●●	Data exfiltration or leaks are a primary attack vector and should be carefully monitored on any genomic data processing environment.	2,4,5 - Preventing data leaks is a priority for preventing privacy breaches. 7 - Data leaks threaten trust and reputation. 10 - Protect IP against data leaks.
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	●●●	●●●	●●	●●	●●●	●●	●●	●●	●●	●●●	●●	●●	Integrity checking mechanisms help manage data and software integrity issues throughout the genomic lifecycle. These mechanisms can help identify compromises to the data or software and verify the integrity of data analysis environments.	1,3,6 - Integrity checking supports genomic data lifecycle management, identifying data inconsistencies and any unauthorized access that may impact the data. 2,4,5 - Privacy requirements inform data integrity requirements. Data integrity needs and characteristics can vary depending on the context of data processing. 7,10 - Lack of data integrity threatens reputation and IP. 8,12 - Integrity checks help maintain shared data processing environments including verifying software (e.g., open source), firmware, and data.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.DS-7: The development and testing environment(s) are separate from the production environment	●●	●●	●●	●●	●●	●●	●	●	●●	●●●	●	●●	Non-production environments typically do not have the same cybersecurity and privacy protections in place and should not be permitted to process sensitive data. This practice ensures that data is not exposed or altered in non-production environments. The primary data store should not reside in development and testing environments.	8,12 - In a collaborative data sharing environment, organizations operating those environments should ensure that data is not exposed or altered through unauthorized access in a non-production environment.
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	●●	●	●	●	●	●●	●	●	●●	●●	●	●	Hardware integrity was not considered as high of a priority as software integrity. It will be important for managing any type of operational technology and genomic-specific hardware (e.g., genomic sequencers).	8,12 - Data processing environments that include significant proprietary hardware (e.g., sequencers) should implement effective configuration management including integrity checking.

970

971 **Table 21.** PROTECT: Information Protection Processes and Procedures Category and Stakeholder Input.

Information Protection Processes and Procedures (PR.IP)	Stakeholder Input
Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	*Genomic Data sharing environments manage processes and procedures for configuration control, vulnerability management, backups, and planning for response and recovery. In addition to their security benefits, these processes and procedures support privacy objectives, including maintaining operational activities that are compatible with consent (e.g., responding to requests for deletion of data, ensuring data is only processed according to consent, any changes that impact previous consent are communicated and the opportunity to update consent is provided when necessary).*

972 **Table 22.** PROTECT: Information Protection Processes and Procedures Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	●●●	●●	●●	●●	●●	●●	•	•	●●	●●●	●●	●●	Establishing a baseline configuration can help manage risks from IT, operational technology, or industrial control systems, including genomic sequencers. Minimizing interaction with data to only what is needed can help ensure data integrity and provenance. Baselines can help implement security and privacy related capabilities and identify anomalies.	1,3,6,10,12 - Baseline configurations facilitate the ability to build systems that are secure up front and then can detect anomalous behavior in response to threats or incidents. 2,4,5 - Helps implement privacy-related cybersecurity capabilities and identify anomalies.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.IP-2: A System Development Life Cycle to manage systems is implemented	●●●	●●	●●	●●	●●	●●	●	●	●●	●●●	●	●	A System Development Life Cycle provides a framework to manage system and data security through development and operations.	1,8,10,12 - System Development Lifecycle principles should be used to implement and manage controls for systems throughout the genomic data lifecycle. 2,3,4,5,6,9 - The System Development Lifecycle includes processes and activities that address the risks associated with processing genomic data (e.g., privacy engineering practices, IP handling).
PR.IP-3: Configuration change control processes are in place	●●●	●●	●●	●●	●●	●●	●	●	●●	●●●	●	●●	Configuration change control is a fundamental capability expected in every system. It facilitates implementation of secure configurations, managing changes (e.g., patching), and detecting authorized and unauthorized changes. It helps manage data integrity, privacy protections, data access, and IP protections.	1,6,10 - Configuration change control is a primary mechanism to manage data integrity throughout the lifecycle, manage data access, and protect IP. 2,4,5 - Change control processes ensure systems and environments maintain their intended privacy risk posture as changes occur over time. 8,12 - Data sharing environments implement effective change control to protect data, analysis, and results.
PR.IP-4: Backups of information are conducted, maintained, and tested	●●●	●●	●●	●●	●●	●	●	●	●●	●●●	●●	●●	Managing backups is a basic function that can prevent data loss and protect against ransomware. Access to backups should be restricted to prevent loss of sensitive data including IP.	1,10 - Backups enable recovery from an incident involving data integrity issues or loss of sensitive data, including IP. This practice helps ensure provenance and manage integrity by providing a state to restore to. 2,4,5,9,10 - Backups provide benefits but may also be an attack vector for sensitive data. Enterprise and system management plans consider both the roles and risks of backup management.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	●●	●●	●●	●●●	●●	●●●	●	●	●●●	●●	●●	●●	This practice links the Governance areas of policy and compliance to the physical operational environment to ensure that appropriate cybersecurity and privacy protections are in place. These include managing provenance and data integrity. Policies and regulations prescribe cybersecurity and privacy requirements for managing genomic data, especially in cases where data is stored locally. Policies specific to the physical operating environment may be secondary to others specific to virtual or logical environments.	1,2,4,5 - Ensures local data management practices are considered as well as requirements for international data transfers. 8,10,11,12 - Shared data processing environments should incorporate protections for locally stored data and meet legal requirements (e.g., Clinical Laboratory Improvement Amendments).
PR.IP-6: Data is destroyed according to policy	●●●	●●●	●●	●●●	●●●	●●●	●	●●	●●●	●●●	●●	●●●	Organizations follow privacy, IP, research, and data usage agreements that stipulate data destruction requirements. Genomic data includes specific approved uses and should not be shared otherwise without permission. This practice helps manage provenance--when data is expected to be destroyed it needs to be properly destroyed. Unnecessarily stored data increases data security risks. Additionally, as costs decrease the need to retain some datasets may decline as well.	1,3 - Proper destruction of data at the end of the information lifecycle reduces the risk of unauthorized access. 2,4,5 - Data destruction supports specific privacy protections including minimization, consent to use data, and the "right to be forgotten" under certain laws. 11 - Improper data deletion can adversely impact sample diversity while deleting data according to policy may encourage participation in data collection.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.IP-7: Protection processes are improved	●●	●●	●●●	●●	●●	●●●	●●	●●	●●	●●	●	●	Processes in place to capture and implement ongoing changes and enhancements are important to incorporate lessons-learned and provide continuous improvements. Adapting to lessons learned will improve the protection of information systems and foster trust.	3,6 - Process improvement helps address the dynamic nature of threats, such as the rapidly changing landscape in emerging privacy risks and adapting to challenges for remote access.
PR.IP-8: Effectiveness of protection technologies is shared	●●	●	●●	●	●	●●	●	●	●	●	●	●	Sharing the effectiveness of protection technologies provides an industry platform for participants to learn from sector-wide threats and mitigations; however, this was not as highly prioritized compared to other Protect Subcategories. Organizations should participate in groups like the BIO-ISAC for sharing cyber threat intelligence.	1,3 - Information sharing may help partner organizations in the supply chain or genomic data lifecycle coordinate mitigation efforts to ensure data integrity. 2,4,5 - Effectiveness of certain cybersecurity technologies impact privacy risk. Sharing that information may help speed mitigation and meet legal reporting requirements. 3,6,8,12 - Sharing information regarding issues with protection technologies facilitates mitigation across the community.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	●●●	●●●	●●●	●●	●●●	●●	●●	●●	●●	●●●	●	●●●	Creating response and recovery plans ensures that organizations are prepared to act when a cybersecurity incident happens. Without this step, there are no defined activities for the Respond and Recover functions. Plans should articulate actions for analysis, containment, mitigation, communication, recovery, and capturing lessons learned.	Review response and recovery plans to incorporate these MO-specific requirements: 1,3,6 - Protections for data integrity, provenance, data access, and other identified security and privacy risks. 2,4,5 - Some cybersecurity incidents impact privacy. Cybersecurity and privacy functions coordinate response and recovery plans to help their organization and its partners identify and address privacy issues and meet their obligations for handling privacy breaches. 7 - Activities required to manage trust and reputation. 8 - Coordinate with members of the research community. 9 - Compliance with legal and regulatory requirements. 10 - Protection and recovery of IP. 12 - Coordination with users of the secure platform.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.IP-10: Response and recovery plans are tested	●●	●●	●●	●	●●	●	●●	●	●●	●●●	●	●●	Testing response and recovery plans should involve all responsible parties and verify the ability to meet response and recovery objectives identified in the plans.	Plan testing should verify the effectiveness of: 1,3,6 - Protections for data integrity, provenance, data access, and other identified cybersecurity and privacy risks. 2,4,5 - Privacy protections consistent with the operational environment and links to other processes, including notification for privacy breaches. 7 - Activities required to manage trust and reputation. 8 - Coordinate with members of the research community. 9 - This Subcategory directly supports achievement of this MO. 10 - Protection and recovery of IP. 12 - Coordination with users of the secure platform.
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	●	●	●●●	●	●	●●●	●	●●	●●	●●●	●●	●●	Human resource planning for cybersecurity takes into consideration important vectors, including insider threats and other personnel-related risks. It should be integrated with access control policies such as deprovisioning.	3,6,10 - These MOs require higher prioritization of personnel screening and management due to insider threat risks including unauthorized access or IP loss. 8,9,11,12 - Organizations operating shared data environments or managing data stores should implement HR policies to address personnel cybersecurity risks.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.IP-12: A vulnerability management plan is developed and implemented	●●●	●●●	●●●	●●	●●●	●●●	●	●	●●	●●●	●	●●	Organizations are responsible for comprehensive management of vulnerabilities in their environment including scanning, remediation, disclosure, and countermeasures to protect sensitive data such as data that impacts privacy and IP.	1 - Vulnerability management plans should help manage vulnerabilities that may threaten data integrity or provenance such as securing data stores and analysis environments. 2,4,5 - Some vulnerabilities may introduce privacy risks that lead to problems for individuals (e.g., discrimination, loss of autonomy, loss of trust) and related risks for the organizations (e.g., compliance, reputation). 8,12 - Data sharing environments are responsible for managing vulnerabilities to the data and environment. 9 - Federal organizations follow legal and regulatory requirements for their vulnerability management programs including time to mitigate high or critical vulnerabilities (Binding Operational Directive 22-01 [14]).

973

974 **Table 23.** PROTECT: Maintenance Category and Stakeholder Input.

Maintenance (PR.MA)	Stakeholder Input
Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	*The stakeholders did not identify specific comments on this Category.*

975 **Table 24.** PROTECT: Maintenance Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	●●	●	●●	●	●	●	●	●	●●	●●	●	●●	Proper maintenance, including patching, helps to address vulnerabilities that could impact the security of genomic data or data processing environments or the privacy of individuals. Logging facilitates accountability in the event of unauthorized or malicious activity.	1,8,10 - Environments processing sensitive information require a higher degree of maintenance due to the sensitivity and critical nature of the information and the dependencies across the data lifecycle. Maintained environments provide confidence that system vulnerabilities are mitigated. 9 - Laws or guidance may stipulate patching outdated software and even migration away from unsupported hardware and software.
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	●●	●	●●	●	●	●●	●	●	●●	●●	●	●●	Remote system maintenance has become more common as systems move to the cloud. At the same time, remote access is a common attack vector. Organizations implement protections to approve, log, and monitor remote maintenance to prevent unauthorized data access, data integrity issues, provenance issues, and loss of sensitive data including data that may impact privacy or IP.	6,8,12 - Organizations with remote maintenance of shared and cloud environments will need to take extra precautions to implement effective access controls such as multifactor authentication, event correlation to detect malicious behavior, and infrastructure as code to improve configuration compliance. 9 - Federal organizations follow federal requirements for managing remote access (e.g., Federal Risk and Authorization Management Program [FedRAMP], NIST).

976 **Table 25.** PROTECT: Protective Technology Category and Stakeholder Input.

Protective Technology (PR.PT)	Stakeholder Input
Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	*Most of these Subcategories align to the safe storage and management of genomic data. Protective Technology assumes IP has been identified then layered security and related technologies protect it. Protective technologies can be used to further secure and monitor sharing platforms.*

977 **Table 26.** PROTECT: Protective Technology Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	●●●	●●	●●●	●●	●●	●●	●	●●	●●●	●●●	●	●●	Logging records changes to data and the environment that along with audit review may help identify or indicate issues with data integrity, provenance, or unauthorized access. This practice can help identify misuse, determine what happened, and who is responsible.	1,3,6,8,10,12 - Logging can help manage data integrity, provenance, and unauthorized data access and supports incident response investigations. 2,4,5 - Logging may help detect and understand privacy incidents related to unauthorized access or disclosure. 9 - Audit records verify compliance and can identify noncompliance.
PR.PT-2: Removable media is protected and its use restricted according to policy	●	●	●	●	●	●	●	●●	●●	●●●	●	●	Removable media, such as flash drives or removable hard disks, was determined to be less likely of an attack vector compared with network attacks.	8,10 - In cases where there is opportunity to use removable media, there is a substantial risk for stealing sensitive information such as IP or provide unauthorized access to research results. 9 - Laws or regulations may prohibit the use of removable or portable data storage devices.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	●●	●●	●●●	●●	●●	●●●	●	●	●●	●●●	●	●●	Least functionality restricts users from making unauthorized changes to the platform or performing unauthorized operations such as unauthorized access or impacting the quality and integrity of data.	1,3,6,8,9,10,12 - Manages risks by significantly reducing the likelihood and impact of unauthorized access or making unauthorized changes to the data or environment. 2,4,5 - Least functionality supports privacy protections related to minimization and preventing unauthorized access or unauthorized changes to the data.
PR.PT-4: Communications and control networks are protected	●●	●●	●●	●●	●●	●●	●	●●	●●	●●●	●	●●	Organizations protect their network traffic from potentially malicious attacks using technologies such as boundary protections, segmentation, firewalls, or remote access controls. These barriers limit unwarranted access of sensitive genomic data. Reducing the flow of information to only what is necessary using network protections reduces risks of data loss and compromise.	10 - Safeguarding sensitive information such as IP using network protections is strengthened by effective network and boundary controls.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	•	•	•	•	•	•	•	•	•	•	•	••	Protections to maintain resiliency were not prioritized as high compared to other protective technologies. This Subcategory will be a higher priority for operations requiring a high degree of availability, uptime, or business process continuity.	1,3,8 - Availability, as ensured by resilience mechanisms, was identified as more important for MOs where information or research is being shared across a supply chain. 9 - Certain sectors may have laws or regulations that stipulate uptime requirements that would require resilience mechanisms. 10 - Organizations protecting IP may prioritize resilience higher, potentially in cases where use of the IP is tied to outcomes that may be potentially impacted by outages (e.g., healthcare).

978

979 **Table 27.** DETECT: Anomalies and Events Category and Stakeholder Input.

Anomalies and Events (DE.AE)	Stakeholder Input
Anomalous activity is detected in a timely manner and the potential impact of events is understood.	*Stakeholders found significant overlap in the three Detect Categories but tended to prioritize security continuous monitoring. They recognized the need to validate access controls to verify they work as intended, use machine learning to automate detection, and address both insider threat and failure to adhere to policy. Data sharing environments and those hosting sensitive data will prioritize detection capabilities higher. For research environments, if data is compromised, then research is devalued.*

980 **Table 28.** DETECT: Anomalies and Events Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	●●●	●	●●	●●●	●●	●●●	●	●●●	●●	●●●	●	●●●	Managing the baseline helps identify authorized vs. unauthorized network activity that may threaten data integrity and privacy.	1,3,6 - Baseline may help identify unauthorized data access. 10 - Unexpected data flows may indicate threats to IP.
DE.AE-2: Detected events are analyzed to understand attack targets and methods	●●●	●	●●	●	●●	●●●	●	●●●	●●	●●●	●	●●	Respond Subcategories rely on effective detection. Analysis is required to determine the appropriate response activities.	1 - Analysis may detect an attack that involves data integrity or provenance. 2,4,5 - Analysis may detect an attack that involves privacy or consent issues. 6,10 - The analysis may determine if the attack exposes sensitive data including unauthorized access or threats to IP.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	●●	●	●	●	●	●●	●	●●	●	●●	●	●●	Correlation helps provide a broader understanding of the potential attacks across the entire organization and identify similar attacks across different systems. These activities require additional resources and expertise and are sometimes considered a more mature activity.	1,3,6,8,10 - Correlation facilitates the ability to hunt for similar attacks across the network that may impact data integrity, provenance, or the data lifecycle. 2,4,5 - Correlation can help to coordinate response to attacks that result in privacy impacts.
DE.AE-4: Impact of events is determined	●●●	●	●●	●●	●●	●●●	●●	●●●	●●	●●●	●	●●	Impact analysis will help determine if assets or data involved in a response effort includes privacy breach, consent issues, data integrity, provenance, or IP.	Subcategory may be prioritized as needed to determine: 1 - Did the attack cause data integrity or provenance issues? 2,4,5 - Does the impact include privacy or consent issues? 6,10 - Did the attack expose sensitive data? 8,12 - What is the impact on shared data services?
DE.AE-5: Incident alert thresholds are established	●●	●	●●	●●	●●	●●	●	●●●	●●	●●●	●	●●	Incident alerts activate related response teams including communications, forensics, and privacy incident teams.	2,4,5 - Thresholds may indicate the need to activate the privacy incident response team. 7 - Thresholds may indicate the need to involve public relations teams if there is a risk to reputation.

981

982 **Table 29.** DETECT: Security Continuous Monitoring Category and Stakeholder Input.

Security Continuous Monitoring (DE.CM)	Stakeholder Input
The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	*Monitoring helps make sure technology is performing as intended with network monitoring and detection of incidents. It can support an improved understanding of risks and emerging threats and capabilities.*

983 **Table 30.** DETECT: Security Continuous Monitoring Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
DE.CM-1: The network is monitored to detect potential cybersecurity events	●●●	●	●●●	●●	●●●	●●●	●●	●●●	●●●	●●●	●●	●●●	Network monitoring is considered an essential detection capability and will be prioritized by most organizations. Organizations need to monitor emerging threats and the risks they introduce, along with remote access and interconnections between organizations. Network is the virtual edge of systems and responsibility.	7 - Network monitoring is considered basic security due diligence; failure to monitor may erode trust. 8,12 - Data processing environments should maintain robust network monitoring capabilities.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	●●	●	●	●	●	●●	●	●●	●●	●●	●	●●	Physical access is a less likely attack vector for genomic data compared with virtual access, so physical monitoring is rated a lower priority.	1,3,6,8,10,12 - Shared data analysis environments may have physical components that require monitoring. Research environments and those with IP may prioritize this Subcategory higher.
DE.CM-3: Personnel activity is monitored to detect potential	●●●	●	●●	●●	●●	●●●	●	●●●	●●	●●●	●●	●●●	Personnel monitoring should be a high priority to enforce access controls and prevent insider threat.	1,3,6,8,10,12 - Shared data analysis environments will warrant enhanced personnel monitoring. Providers, research environments, and those with IP may prioritize this Subcategory even higher.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
cybersecurity events														
DE.CM-4: Malicious code is detected	●●	●	●●	●	●	●●●	●●	●●●	●●	●●●	●●	●●●	Malicious code can compromise data integrity and access to sensitive data. This Subcategory should be prioritized due to the high impact and prevalence of ransomware and the use of malicious code as an attack technique.	1,2,4,5 - Malicious code may be a primary attack vector impacting data integrity or privacy. 3,6,8,10,12 - Shared data analysis environments will want enhanced malicious code monitoring. Providers, research environments, and those with IP may prioritize this Subcategory even higher.
DE.CM-5: Unauthorized mobile code is detected	●●	●	●●	●	●	●●	●	●●	●	●●	●●	●●●	Mobile code can compromise data integrity and access to sensitive data when not carefully managed.	1,2,4,5 - Mobile code may be a primary attack vector impacting data integrity or privacy. 3,6,8,10,12 - Shared data analysis environments will want enhanced mobile code monitoring. Providers, research environments, and those with IP may prioritize this Subcategory even higher.
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	●●●	●	●●	●●	●●	●●●	●	●●●	●●	●●●	●●	●●●	External service providers broaden the attack surface of an organization's data. Monitor external service providers carefully to ensure data protections are in place and requirements are met.	1,3,6,8,12 - All parties in data sharing environments should consistently address data integrity protections throughout the lifecycle; monitoring should be consistent across external service providers. 2,4,5,10 - Protections for sensitive data (privacy, IP, etc.) should be consistent internally and with external providers. Monitoring helps ensure that privacy requirements travel with data and are enforced wherever data is shared.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	●●●	●	●●	●●	●●	●●●	●●	●●●	●●	●●●	●●	●●●	In addition to network and personnel monitoring, organizations should be able to detect unauthorized users, connections, devices, or software. Organizations should use allow-lists and deny-lists to inform cybersecurity tools that log and audit system activity to detect suspicious events.	1,3,6,8,10,12 - Shared data analysis environments will want enhanced detection capabilities that should include event aggregation, correlation, and analysis. Providers, research environments, and those with IP may prioritize this Subcategory even higher.
DE.CM-8: Vulnerability scans are performed	●●●	●	●●●	●	●●	●●●	●●	●●●	●●●	●●●	●	●●●	Scanning is considered a high priority because it proactively identifies and evaluates vulnerabilities that may introduce cybersecurity risks and helps organizations mitigate known threats by identifying potential attack vectors. Federal agencies will prioritize scanning as part of their required vulnerability management programs.	3,8,10,12 - Vulnerability scans should be conducted as part of routine maintenance, but organizations should consider the timing of vulnerability scans to avoid disrupting operations. 7 - Vulnerability scanning is considered basic security due diligence; failure to monitor would erode trust.

984

985 **Table 31.** DETECT: Detection Processes Category and Stakeholder Input.

Detection Processes (DE.DP)	Stakeholder Input
Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	*Stakeholders prioritized Detection Processes for MO1 and MO3. Most important to have the detection processes in place and an understanding of requirements. The other Categories support other aspects of Detect.*

986 **Table 32.** DETECT: Detection Processes Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	●●	●	●●	●●	●●	●●	●	●	●●	●●●	●	●	Well defined roles and responsibilities help coordinate detection activities and manage chain of custody of sensitive information.	1,6 - Procedures should be clearly defined to escalate detected data integrity or unauthorized access issues to responsible parties. 2,4,5 - Clearly defining privacy incident detection roles and responsibilities supports the ability to quickly report and respond when required. 10 - Ensure those handling IP are aware of their responsibilities.
DE.DP-2: Detection activities comply with all applicable requirements	●●●	●	●●	●●	●●●	●●●	●●	●●	●●●	●●●	●	●●	Detection activities should be implemented to comply with organizational policies defined under Governance along with any legal and regulatory requirements. Well defined organization-specific requirements ensure detection activities align with MOs. Non-compliance with minimum requirements (such as laws, regulations, or policies) will negatively affect trust and reputation and may prevent or halt operations.	Subcategory may be prioritized to address requirements from: 1,3,6 - Security and privacy risk management including data integrity, provenance, and unauthorized data access. 2,4,5 - Privacy and consent (e.g., reporting, notification, mitigation). 9 - Applicable laws and regulations.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
DE.DP-3: Detection processes are tested	●●	●	●●	●	●●	●●	●	●	●●	●●●	●	●●	Testing detection processes ensures they are effective and properly informs response activities. Higher priority is placed on development and implementation of detection processes.	4,5,6,10,12 - Organizations processing sensitive data such as data with privacy impacts or IP may prioritize detection process testing higher.
DE.DP-4: Event detection information is communicated	●●	●	●●	●●	●●	●	●	●	●●	●●●	●	●●	Initial communication of event detection triggers response activities and informs appropriate parties of potential unauthorized access, privacy breaches, and compromised IP so they can determine whether and how to respond.	4,5,6,10,12 - Organizations processing sensitive data such as data that impacts privacy and IP will prioritize detection communication processes higher.
DE.DP-5: Detection processes are continuously improved	●●	●	●●●	●	●●	●●	●●	●●	●●	●●●	●	●●	Process improvement can proactively reduce the likelihood of new incidents and prevent repeat incidents.	4,5,6,10,12 - Organizations processing sensitive data such as data that impacts privacy and IP prioritize improving processes higher to keep up with the dynamic nature of threats and changing environments. 7 - Updating detection processes demonstrates that organizations concerned about trust and reputation are taking measures to foster trust, maintain a good reputation, and avoid negligent practices.

987 **Table 33.** RESPOND: Response Planning Category and Stakeholder Input.

Response Planning (RS.RP)	Stakeholder Input
Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	*Response planning was deemed highly important, but detection comes before response. It is important to think in advance and in depth about how to respond and recover when there is an incident. Incidents are more likely due to the increasing complexity and sophistication of adversaries. Many breaches are caused by an internal failure to adhere to policy.* *2 - Response, specifically through notification, is not the same with relatives as it would be with donors. Respond and Recover happen after preservation of relatives privacy has failed, emphasis should be on improving prevention and detection processes to prevent future issues.* *6,12 - Response plan should consider inevitable changes where access that was authorized in the past is no longer authorized.* *7 - Poor responses can cause loss of trust and reputation for companies that do not respond well to breaches.* *12 - Response planning takes into account the data sensitivity and confidentiality of the platforms to ensure these attributes are maintained during the response to a security incident.*

988 **Table 34.** RESPOND: Response Planning Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RS.RP-1: Response plan is executed during or after an event	●●●	●●●	●●●	●●	●●●	●●●	●●●	●●●	●●●	●●●	●	●●●	Organizations that process genomic data, even organizations that are not the original source of collection, should be prepared to respond immediately and effectively to assess and limit incident impacts. Response may include reporting and notification stipulated by laws and regulations, especially as related to privacy. Response plans should consider how to maintain data integrity during response. A feedback loop helps ensure all problems are addressed. The Response Plan should establish all response coordination activities.	2,4,5,9 - Organizations that are the original point of collection may have additional responsibilities for interacting with donors and other individuals affected by an incident for information they process, including information shared with an organization that experiences an incident. If there is a privacy incident, the plan drives communication that needs to occur with other organizations, such as sharing partners, and the affected donors and relatives. Laws and regulations typically define the circumstances under which an incident is considered a breach and specific notification requirements. Breach plans account for the complexities around incidents to determine whether, how, and when notification is required. 4 - Manage impacts related to achieving consent requirements in coordination with privacy leadership and in accordance with the plan. 12 - Response plan execution is particularly important for platform providers as users are dependent on service providers to communicate with them so that they can address and mitigate the impact on their organization or project.

989

990 **Table 35.** RESPOND: Communications Category and Stakeholder Input.

Communications (RS.CO)	Stakeholder Input
Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	*This Category focuses on providing clear and effective Response Communication, internally to coordinate response and externally to inform authorities, across customers, collaborators, donors, and relatives.* *Reporting and timing of the reporting may be stipulated in laws and regulations.* *4,12 - Communication should include notification of any changes impacting consent.* *7,8 - Effective communication and messaging helps maintain reputation and avoid damage after an incident.*

991 **Table 36.** RESPOND: Communications Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RS.CO-1: Personnel know their roles and order of operations when a response is needed	●●	●●	●●	●●	●●	●●	●●●	●●	●●●	●●●	●	●●	Well-defined roles help expedite response activation, improve effectiveness, and maintain legal and regulatory compliance while coordinating response activities.	9 - Especially important to maintain legal and regulatory compliance.
RS.CO-2: Incidents are reported consistent with established criteria	●●	●●	●●	●●	●●	●●	●●	●●	●●●	●●	●	●●	Appropriate incident reporting helps organizations meet policy and legal response requirements (e.g., privacy) and maintain trust.	4 - Incident reporting should meet consent requirements. 7 - Failure to report could tarnish reputation and trust. 9 - Reporting is required to maintain legal and regulatory compliance.
RS.CO-3: Information is shared consistent with response plans	●●	●●	●●	●●	●●	●●	●●	●●	●●	●●	●	●●	Consistent reporting ensures the appropriate personnel and organizations are notified and activated to respond to the incident, protect data integrity, contain the damage, and report privacy breaches.	9 - Legal and regulatory reporting requirements should be built into the information sharing aspects of Respond activities.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	●●●	●●●	●●	●●	●●	●●	●●	●●	●●	●●	●●	●●	Genomic data is shared across multiple organizations and any response should notify and involve these parties appropriately to manage the impact to the data, research, and analysis.	1,3,6,7,8,11,12 - Coordination includes the appropriate organizations involved in the data lifecycle to manage any issues with data integrity, provenance, data access, and impact to data sharing agreements. 2,4,5,9 - Privacy breaches can require specialized coordination beyond what is required for responding to cybersecurity incidents.
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	●	●	●	●	●	●	●	●	●	●	●	●	Voluntary sharing was not considered a high priority for organizations. Sharing helps maximize the benefits of lessons learned from an incident. Because of the collaborative nature of genomic data usage, voluntary sharing may help others improve their cybersecurity and privacy protections, benefiting the broader community. As information sharing capabilities increase in the genomics community, organizations will need to prepare to receive and react to shared information.	No additional considerations identified.

992

993 **Table 37.** RESPOND: Analysis Category and Stakeholder Input.

Analysis (RS.AN)	Stakeholder Input
Analysis is conducted to ensure adequate response and support recovery activities.	*Automating Response Analysis minimizes inconsistencies and improves response timelines.*

994 **Table 38.** RESPOND: Analysis Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RS.AN-1: Notifications from detection systems are investigated	●●●	●●	●●	●●	●●	●●	●	●	●●	●●●	●●	●●	Analysis is required to detect data integrity issues anywhere in the lifecycle. Detection activates response activities; other Respond Subcategories rely on effective detection.	2,5 - Notifications include alerts on privacy incidents and initiate comprehensive investigation. 4 - Notification is required when an incident impacts consent. 12 - Organizations relying on secure platforms expect that the platform provider will perform effective detection.
RS.AN-2: The impact of the incident is understood	●●●	●●●	●●	●●	●●●	●●●	●●	●	●●	●●●	●●	●●	Impact establishes the significance and breadth of an incident. It determines the extent of the required response including scope, urgency, and resourcing.	1,3,6,8 - This activity helps define the impact to data integrity, provenance, security and privacy risks, data access, and effect on the data. An organization will need to determine if the data can still be trusted. 2,4,5 - Ensure criteria are in place to identify incidents that may result in privacy and consent issues. 9 - Investigations determine if the impact has legal or regulatory implications. 10 - Impact to IP may result in a broader response effort. 12 - Platform providers assess impact to the user community.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RS.AN-3: Forensics are performed	●●	●●	●●	●●	●●	●●●	●	●	●●	●●	●●	●●	Forensics help clarify the extent of the impact—whether and how data was accessed by whom and when, and whether data was changed. Results of the forensics analysis help determine the scope and magnitude of impact to the organization and affected individuals, which in turn informs response requirements.	1,3,8,12 - Forensics may be necessary to determine data integrity issues that may impact data usage throughout the lifecycle. 9 - Forensics may be stipulated by laws or regulations. 10 - Forensics can verify access to IP and may identify who accessed the data. 11 - May identify changes to the data impacting ability to preserve sample diversity.
RS.AN-4: Incidents are categorized consistent with response plans	●●●	●●●	●●	●●	●●●	●●●	●●	●	●●	●●	●●	●	Correctly categorizing incidents ensures appropriate resources are mobilized.	2,4,5 - Identify and categorize privacy incidents correctly. 7 - Identify incidents that may damage reputation. 9 - Categorize incidents as required to comply with laws and regulations.
RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources	●●	●●	●●	●	●●	●	●	●	●	●●●	●●	●●	Identifying and addressing new vulnerabilities reduces the likelihood of some risks.	12 - Platform providers have a responsibility to track known vulnerabilities and mitigate them appropriately to maintain the security posture of their environment.

995 **Table 39.** RESPOND: Mitigation Category and Stakeholder Input.

Mitigation (RS.MI)	Stakeholder Input
Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	*Response Mitigation activities were prioritized highly, after Planning.*

996 **Table 40.** RESPOND: Mitigation Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RS.MI-1: Incidents are contained	●●●	●●●	●●	●●	●●●	●●●	●	●	●●	●●●	●	●●●	Containment reduces additional impact from an incident and should be a high priority for Respond.	1 - Containment helps manage data integrity and ensures compromised data is not propagated to others interacting with data. 2,4,5 - Containment minimizes the privacy impact an incident may have on individuals. 6 - Containment restricts additional unauthorized access. 8 - Containment minimizes effects on others using the research data. 10 - Containment can minimize the impact to IP. 12 - Containment can manage the impact to the secure platform to control effect on users.
RS.MI-2: Incidents are mitigated	●●●	●●●	●●	●●	●●●	●●●	●	●	●●	●●●	●	●●	Mitigation helps resolve whatever caused the incident and prevents additional issues, including data leaks or unauthorized access.	2,4,5 - Mitigation addresses incidents that impact privacy. 7,8,12 - Effective mitigation fosters trust.
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	●●	●●	●●●	●	●●	●●	●	●	●●	●●●	●	●●	Organizations are increasingly expected to be proactive and dynamic in addressing newly identified vulnerabilities. Identifying new vulnerabilities was considered a secondary priority compared to containing	10 - This practice helps provide dynamic protection for IP.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
													and mitigating known risks and incidents.	

997

998 **Table 41.** RESPOND: Improvements Category and Stakeholder Input.

Improvements (RS.IM)	Stakeholder Input
Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	*Improvements in response strategies and plans help organizations address the dynamic aspect of cybersecurity.*

999

1000 **Table 42.** RESPOND: Improvements Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RS.IM-1: Response plans incorporate lessons learned	●●	●●	●●●	●●	●●	●●	●●	●●	●●	●●	●	●	Improves response outcomes and minimizes likelihood of repeating a past mistake. Updating the response plan was prioritized over updating the response strategy.	7 - Repeating a prior mistake and not implementing response improvements present a serious risk to maintaining trust and organizational reputation. 2,4,5,9 - There may be negligence if organizations fail to incorporate lessons learned and have the same issue more than once.
RS.IM-2: Response strategies are updated	●	●	●●	●	●	●●	●	●●	●●	●●	●	●	Threats and technologies are dynamic. Response strategies need periodic updating to improve future outcomes.	9 - Organizations need to periodically check response strategies to incorporate any changes based on legal and regulatory requirements.

1001

1002 **Table 43.** RECOVER: Recovery Planning Category and Stakeholder Input.

Recovery Planning (RC.RP)	Stakeholder Input
Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	*Recovery planning might be lower priority compared to response planning; however, recovery plans help return operations to a prior uncompromised state following an incident. Having a plan can enable continuation of operational activities and protect assets. Recovery plans can help manage reputation risks following an incident by establishing requirements for communication of privacy related incidents and restorative processes.* *1 - Recovery with respect to genomic data helps verify the integrity of the data prior to resuming normal operations and can be complex.* *3 - Recover was considered important but not prioritized as high as Respond by stakeholders.* *7 - Trust in organizations and their genomic data impacts willingness to participate in research, use data as a source for research, trust the results of the research. Sometimes there is no opportunity to recover data so other activities were prioritized higher.* *10 - The ratings help provide understanding of priorities for protecting IP since not every activity can be resourced.* *11 - Recover does not have the same meaning as recovery. Organizations should be able to protect assets in the future.* *12 - Secure platform providers put a recovery plan in place. Recovery steps maintain safeguards on sensitive/confidential data/systems.*

1003 **Table 44.** RECOVER: Recovery Planning Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RC.RP-1: Recovery plan is executed during or after cybersecurity incident.	●●●	●●	●●	●●	●●	●●	●●●	●●	●●	●●●	●●	●●	Recovery plans help restore data access and integrity to an acceptable operational state. Having a plan can help to manage high-risk operations, impacts to IP and privacy, and applicable requirements from laws, policies, consents, and regulations.	1,8,11,12 - The recovery plan establishes the activities required to restore operations and data integrity to a trusted, uncompromised state. 2,4,5,9 - Prioritize recovery planning to address legal, policy, regulation, privacy, and consent requirements. 3,10 - Recovery plan manages high-risk recovery operations and impacts to IP. Risk modeling and tolerances may help determine the scope and resourcing required to manage recovery operations. 6 - Recovery plan incorporates and enforces data access protection requirements, including access controls for backups. 7 - Recovery plan addresses restoration of data access and integrity as well as communication required to maintain and restore trust in the organization.

1004 **Table 45.** RECOVER: Improvements Category and Stakeholder Input.

Improvements (RC.IM)	Stakeholder Input
Recovery planning and processes are improved by incorporating lessons learned into future activities.	*Recovery plan should incorporate lessons learned to update strategies, continuously improving and adjusting practices based on the dynamic threat and operating environments. Response and recovery happen after an incident; emphasis should be on improvement to avoid future incidents. Recovery without improvement is not progress.* *2,4,5,9 - Plans should be updated to reflect changes in laws, regulations, privacy, and consent requirements.* *8,12 - Data sharing environments have an obligation to continuously improve their ability to recover from data and ransomware attacks to maintain the trust of users.*

1005 **Table 46.** RECOVER: Improvements Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RC.IM-1: Recovery plans incorporate lessons learned.	●●	●●	●●	●	●●	●●	●●	●●	●	●●●	●	●●	Recovery plans should be updated to incorporate lessons learned and address emerging threats that could compromise recovery activities.	1 - Data integrity recovery helps restore trust in data. 2 - Improvements may be needed to identify and address issues with notifying relatives. 3 - Risk models and actions may need to be revised. 7,8,9,12 - Implementing improvements demonstrates due diligence rather than repeating mistakes, maintain the trust of users, researchers, and the genomics community.
RC.IM-2: Recovery strategies are updated.	●	●	●	●	●	●	●	●●	●	●●	●	●	Updating recovery strategies to address known issues and lessons learned is important, but secondary to updating recovery plans. Updating recovery strategies is a longer-term activity that may also inform changes to other cybersecurity and privacy capabilities. However, if governance requires, the priority for updating recovery strategies would be elevated.	1,2,5,8,10,12 - Threats to data, privacy, and processing environments are dynamic. Recovery strategies need to evolve to maintain the trust of donors, researchers, and users. 3,6,7 - Though considered secondary to having an effective plan, strategies help organizations adjust cybersecurity capabilities to maintain their effectiveness. 9 - Priority should be consistent with governance requirements.

1006 **Table 47.** RECOVER: Communications Category and Stakeholder Input.

Communications (RC.CO)	Stakeholder Input
Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	*Communications with stakeholders, donors and the public are important for maintaining trust and ensuring long-term organizational priorities in the genomics ecosystem. Communications can also be part of statutory requirements, particularly where privacy is related.* *7 - Communication leads to trust in relationships; it is a key dependency. Dependencies on service providers should be maintained and there are additional responsibilities. What is trusted is just as important as who one trusts.* *8 - Communication is important to manage the relationships within the research community and ensure continued collaboration. Communications help to regain trust in an organization's research and results.*

1007 **Table 48.** RECOVER: Communications Subcategory Prioritization and Notes.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RC.CO-1: Public relations are managed.	•	••	••	••	••	•	•••	••	•	•	••	•	Managing public relations is important for maintaining trust in the genomic data ecosystem to ensure future trust of donors, relatives, organizations using genomic data, the public, and the genomic community.	2 - Public relations may be the primary way relatives interact with genomic data. Poor public relations can impact trust and whether individuals will trust the organization in the future. Good public relations can rebuild and extend trust. 4,5 - Public perception could limit future donors if they do not trust the organization to manage privacy or consent. 8 - Researchers manage public perception to promote trust in research participation and results.

Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
RC.CO-2: Reputation after an event is repaired.	●●	●●	●	●●	●	●	●●●	●●	●	●	●●	●	Repairing reputation helps to limit impact of negative public relations and maintain trust.	1 - Reputation helps to secure the organization's place in the genomic data ecosystem and maintain trust of others working with a compromised organization's data after it has recovered from an incident. 4,5 - Negative reputation due to an incident could limit the participation of future donors if they do not trust organizations to manage privacy or consent. 8 - Researchers manage reputation to promote trust in research participation and results.
RC.CO-3: Recovery activities are communicated to internal and external stakeholders and executive and management teams.	●●●	●●●	●●	●●●	●●●	●●	●●●	●●	●●	●●	●●	●●	Communications help manage trust for those working with genomic data, processing environments, and other organizations involved. Communications also ensure all parties are informed and able to carry out their roles and responsibilities appropriately and improve future outcomes. Executives take primary responsibility for managing risk, resources, compliance with laws, reputation/trust activities, and assess impact to IP and rely on appropriate communications to both stay well informed and convey necessary information to stakeholders.	1 - Communication throughout the genomic data lifecycle helps organizations maintain trust in data integrity and improve future outcomes. 2,4,5,9 - Applicable laws and regulations often include communication requirements regarding privacy and consent. While it may be particularly difficult to contact relatives, organizations should determine what processes need to be developed to communicate with or contact relatives of donors. 8 - Recovery communications help researchers repair their reputation to retain access to their data sources.

1008

References

[1] National Cybersecurity Center of Excellence, "NCCoE Virtual Workshop on the Cybersecurity of Genomic Data," 26 January 2022. [Online]. Available: https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-virtual-workshop-cybersecurity-genomic-data.

[2] National Cybersecurity Center of Excellence, "NCCoE Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data," 18 May 2022. [Online]. Available: https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-virtual-workshop-exploring-solutions-cybersecurity-genomic-data.

[3] National Institute of Standards and Technology (2023) The Cybersecurity of Genomic Data. (Department of Commerce, Washington, D.C.), NIST Internal Report (NIST IR) 8432, Initial Public Draft. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8432.ipd.pdf.

[4] M. Naveed and et.al., "Privacy in the Genomic Era," ACM Computer Survey, vol. 48, no. 1, 1228 pp. 1-49, September 2015.

[5] M. Naveed and et.al., "Privacy in the Genomic Era," ACM Computer Survey, vol. 48, no. 1, 1228 pp. 1-49, September 2015.

[6] Y. Erlich and A. Narayanan, "Routes for breaching and protecting genetic privacy," Nature 1230 Reviews, vol. 15, pp. 409-421, June 2014.

[7] Y. Erhlich and et.al., "Identity Inference of Genomic Data Using Long-Range Familial 1232 Searches," Science, vol. 362, pp. 690-694, 2018.

[8] A. Schwab and et.al., "Genomic Privacy," Clinical Chemistry, vol. 64, no. 12, pp. 1696-1282 1703, 2018.

[9] M. Gianfrancesco and et.al., "Potential Biases in Machine Learning Algorithms Using 1284 Electronic Health Record Data," JAMA Internal Medicine, vol. 11, no. 178, pp. 1544-1547, 1285 2018. 1286

[10] Y. Joly and et.al., "Establishing the International Genetic Discrimination Observatory," 1287 Nature Genetics, vol. 52, pp. 466-468, 2020. 1288

[11] R. Parikh and et.al., "Addressing Bias in Artificial Intelligence in Health Care," JAMA, vol. 1289 24, no. 322, pp. 2377-2378, 2019.

[12] National Counterintelligence and Security Center (NCSC), "China's Collection of Genomic 1265 and Other Healthcare Data From America: Risks to Privacy and U.S. Economic and 1266 National Security," pp. 1-5, February 2021.

[13] "Cybersecurity and Privacy Reference Tool," 2023. [Online]. Available: https://csrc.nist.gov/Projects/cprt.

[14] Cybersecurity & Infrastructure Security Agency (2021) "Binding Operational Directive 22-01," 03 November 2021. [Online]. Available: https://www.cisa.gov/news-events/directives/binding-operational-directive-22-01.

[15] National Institute of Standards and Technology (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (Department of Commerce, Washington, D.C.), NIST Internal Report (NIST IR) 8286. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

[16] National Institute of Standards and Technology (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (Department of Commerce, Washington, D.C.), NIST Special Publication (NIST SP) 800-160, vol. 2, revision 1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

[17] National Institute of Standards and Technology (2020) Recommendation for Cryptographic Key Generation. (Department of Commerce, Washington, D.C.), NIST Special Publication (NIST SP) 800-133, revision 2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf.

[18] "NHGRI Talking Glossary of Genomic and Genetic Terms," 2023. [Online]. Available: https://www.genome.gov/genetics-glossary.

[19] National Institute of Standards and Technology (2021) Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-71. (Department of Commerce, Washington, D.C.), NIST Special Publication (NIST SP) 800-172. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf.

[20] National Institute of Standards and Technology (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (Department of Commerce, Washington, D.C.), NIST Special Publication (NIST SP) 800-161, revision 1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

[21] National Institute of Standards and Technology (1992) Foundations of a Security Policy for Use of the National Research and Educational Network. (Department of Commerce, Washington, D.C.), NIST Internal Report (NIST IR) 4734. https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4734.pdf.

[22] National Institute of Standards and Technology (2010) Contingency Planning Guide for Federal Information Systems. (Department of Commerce, Washington, D.C.), NIST Special Publication (NIST SP) 800-34, revision 1. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

Appendix A. List of Symbols, Abbreviations, and Acronyms

The following acronyms are used in this publication.

AC
Access Control

AE
Anomalies and Events

AM
Asset Management

AN
Analysis

AT
Awareness and Training

BE
Business Environment

BIO-ISAC
Bioeconomy Information Sharing and Analysis Center

CM
Security Continuous Monitoring

CO
Communications

CSF
Cybersecurity Framework

DbGaP
Database of Genotypes and Phenotypes

DE
Detect

DNA
Deoxyribonucleic acid

DP
Detection Processes

DS
Data Security

EO
Executive Order

FedRAMP
Federal Risk and Authorization Management Program

FISMA
Federal Information Security Modernization Act (2014)

GDPR
General Data Protection Regulation

GxP
Good Practices

GV
Governance

HIPAA
Health Insurance Portability and Accountability Act (1996)

ID
Identify

IM
Improvements

IP
Information Protection Processes and Procedures

IP
Intellectual Property

ITL
Information Technology Laboratory

MA
Maintenance

MI
Mitigation

MO
Mission Objective (only used in the Tables)

NCBC
National Centers for Biomedical Computing

NCBI
National Center for Biotechnology Information

NCCoE
NIST National Cybersecurity Center of Excellence

NIST
National Institute of Standards and Technology

NIST IR
NIST Internal Report

PHI
Protected Health Information

PR
Protect

PT
Protective Technology

RA
Risk Assessment

RC
Recover

RM
Risk Management Strategy

RP
Recovery Planning

RP
Response Planning

RS
Respond

SC
Supply Chain Risk Management

SRA
Sequence Read Archive

Appendix B. Glossary

Asset
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes [15].

Cybersecurity Event
A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation) [16].

Data Integrity
A property possessed by data items that have not been altered in an unauthorized manner since they were created, transmitted, or stored [17].

Genome
The entire set of DNA instructions found in a cell. In humans, the genome consists of 23 pairs of chromosomes located in the cell's nucleus, as well as a small chromosome in the cell's mitochondria. A genome contains all the information needed for an individual to develop and function [18].

Network
A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices [19].

Provenance
The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data [20].

Sensitive Data
A descriptor of information whose loss, misuse, or unauthorized access or modification could adversely affect security [21].

System
A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [22].