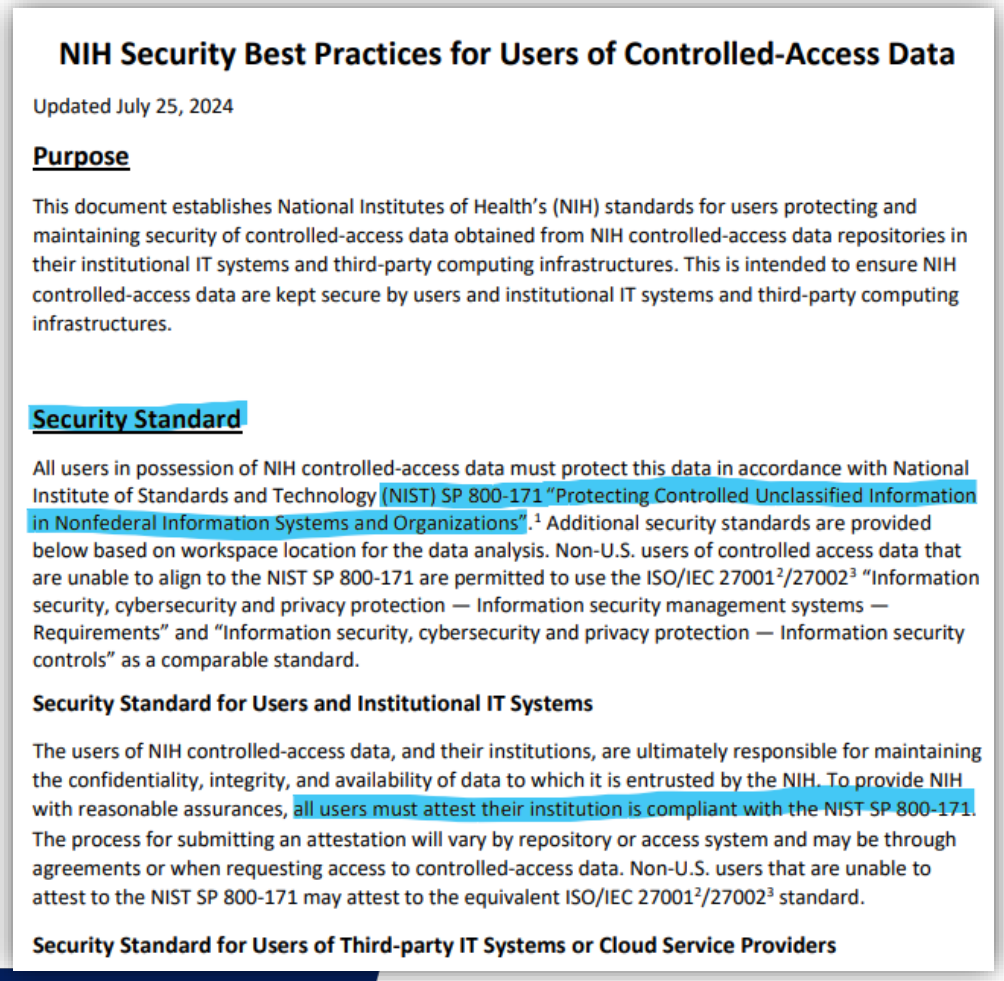
Export Control Office Updates

- New Requirements for Securing NIH Controlled- Access Genomic Data
- Use of Visual Compliance to conduct Restricted Party Screening

March 11, 2025

NIH Genomic Data Sharing (GDS) policy

- Effective January 25, 2025, researchers working with controlled-access genomic data from NIH repositories must comply with updated data management and storage requirements.
- "Approved Users" of NIH controlled-access data will attest institutional systems used to access or store covered data are compliant with NIST SP 800-171
  - Attestation may be part of NIH data use agreements



NIH Security Best Practices for Users of Controlled-Access Data

Updated July 25, 2024

Purpose

This document establishes National Institutes of Health's (NIH) standards for users protecting and maintaining security of controlled-access data obtained from NIH controlled-access data repositories in their institutional IT systems and third-party computing infrastructures. This is intended to ensure NIH controlled-access data are kept secure by users and institutional IT systems and third-party computing infrastructures.

Security Standard

All users in possession of NIH controlled-access data must protect this data in accordance with National Institute of Standards and Technology (NIST) SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations".[1] Additional security standards are provided below based on workspace location for the data analysis. Non-U.S. users of controlled access data that are unable to align to the NIST SP 800-171 are permitted to use the ISO/IEC 27001[2]/27002[3] "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" and "Information security, cybersecurity and privacy protection — Information security controls" as a comparable standard.

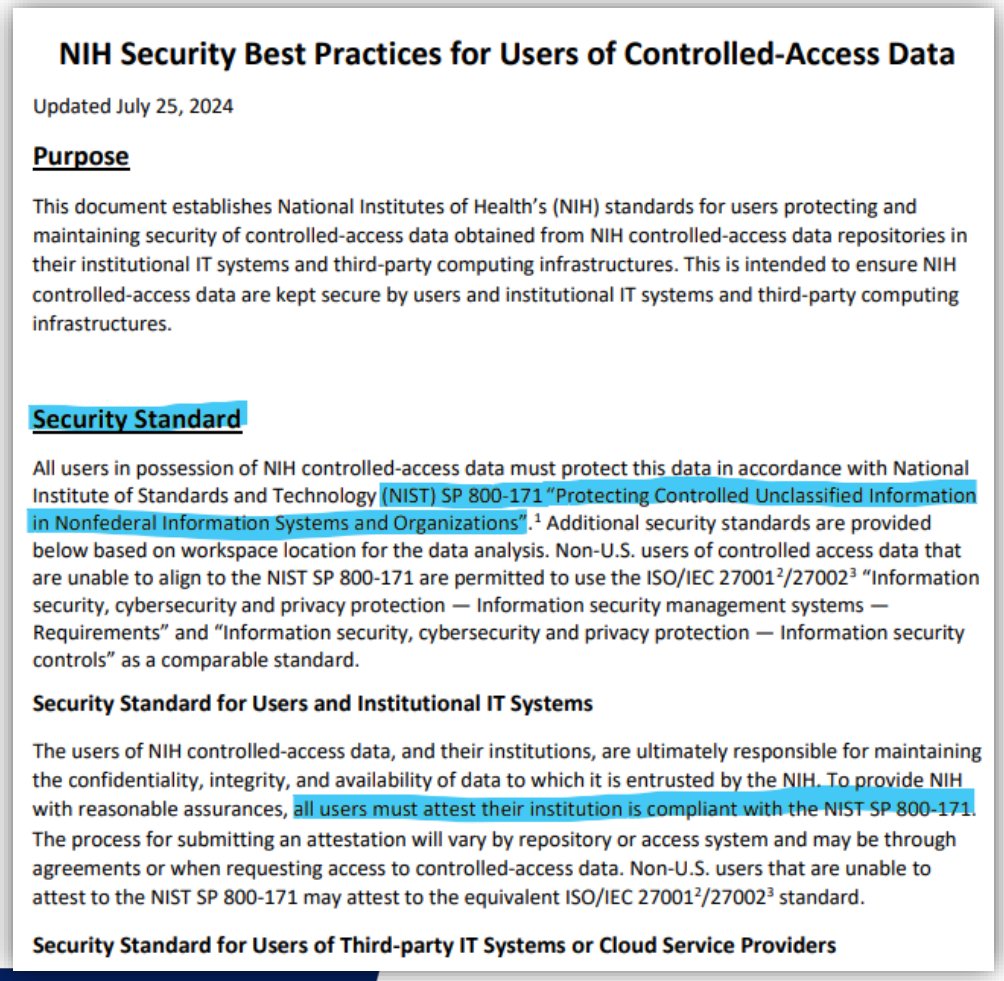
Security Standard for Users and Institutional IT Systems

The users of NIH controlled-access data, and their institutions, are ultimately responsible for maintaining the confidentiality, integrity, and availability of data to which it is entrusted by the NIH. To provide NIH with reasonable assurances, all users must attest their institution is compliant with the NIST SP 800-171. The process for submitting an attestation will vary by repository or access system and may be through agreements or when requesting access to controlled-access data. Non-U.S. users that are unable to attest to the NIST SP 800-171 may attest to the equivalent ISO/IEC 27001[2]/27002[3] standard.

Security Standard for Users of Third-party IT Systems or Cloud Service Providers

NIH Genomic Data Sharing (GDS) policy

- Third Party Systems: "Approved Users" choosing a third-party IT system and/or Cloud Service Provider (CSP) for data analysis and/or storage will provide NIH with an attestation affirming that the third-party system is compliant with NIST SP 800-171
- Applies to new or renewed genomic data use agreements



NIH Security Best Practices for Users of Controlled-Access Data

Updated July 25, 2024

Purpose

This document establishes National Institutes of Health's (NIH) standards for users protecting and maintaining security of controlled-access data obtained from NIH controlled-access data repositories in their institutional IT systems and third-party computing infrastructures. This is intended to ensure NIH controlled-access data are kept secure by users and institutional IT systems and third-party computing infrastructures.

Security Standard

All users in possession of NIH controlled-access data must protect this data in accordance with National Institute of Standards and Technology (NIST) SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations".[1] Additional security standards are provided below based on workspace location for the data analysis. Non-U.S. users of controlled access data that are unable to align to the NIST SP 800-171 are permitted to use the ISO/IEC 27001[2]/27002[3] "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" and "Information security, cybersecurity and privacy protection — Information security controls" as a comparable standard.

Security Standard for Users and Institutional IT Systems

The users of NIH controlled-access data, and their institutions, are ultimately responsible for maintaining the confidentiality, integrity, and availability of data to which it is entrusted by the NIH. To provide NIH with reasonable assurances, all users must attest their institution is compliant with the NIST SP 800-171. The process for submitting an attestation will vary by repository or access system and may be through agreements or when requesting access to controlled-access data. Non-U.S. users that are unable to attest to the NIST SP 800-171 may attest to the equivalent ISO/IEC 27001[2]/27002[3] standard.

Security Standard for Users of Third-party IT Systems or Cloud Service Providers

NIH Genomic Data Sharing (GDS) policy

- Scope: 20 NIH controlled-access data repositories (https://sharing.nih.gov/accessing-data/NIH-security-best-practices)
- If your repository is not currently listed, the new requirements are not applicable.
- Costs of using a secure environment should be an allowable cost and part of a proposal budget when known at the proposal stage. Work with RCRA, Emory Digital, and OSP to ensure these data management costs are included as necessary for the project.

Controlled-access repositories implementing NIH Security Best Practices

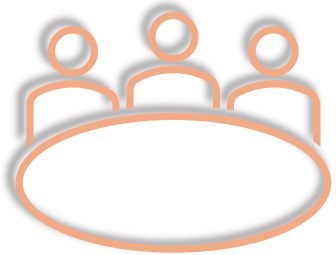
Repository	Access System	URL
Database of Genotypes and Phenotypes (dbGaP)	dbGaP Access System	https://www.ncbi.nlm.nih.gov/gap/
BioData Catalyst	dbGaP Access System	https://biodatacatalyst.nhlbi.nih.gov/
The NHGRI Genomic Data Science Analysis, Visualization, and Informatics Lab-Space (AnVIL)	dbGaP Access System	https://anvilproject.org/
National Cancer Institute (NCI) Genomic Data Commons	dbGaP Access System	https://gdc.cancer.gov/
Cancer Data Service (CDS)-Trusted Partner	dbGaP Access System	https://dataservice.datacommons.cancer.gov/#/home
Kids First Data Resource	dbGaP Access System	https://kidsfirstdrc.org/resources/
INvestigation of Co-occurring conditions across the Lifespan to Understand Down syndromE (INCLUDE) Data Hub	dbGaP Access System	https://portal.includedcc.org/login?redirect_path=/dashboard
Restricted Portion of Sequence Read Archive (SRA)	dbGaP Access System	https://www.ncbi.nlm.nih.gov/sra
National Institute of Mental Health Data Archive (NDA)	NDA Access System	https://nda.nih.gov/
NDA: National Institute on Alcohol Abuse and Alcoholism Data Archive (NIAAADA)	NDA Access System	https://nda.nih.gov/niaaa/

Restricted or Prohibited Parties

- In general, the term refers to **individuals** and **entities**
  - **Excluded** from receiving federal **contracts**, certain **subcontracts**, and certain types of federal **financial and non-financial assistance** and benefits.
  - Against whom certain **restrictions,** or **prohibitions** are applied by the U.S. federal agencies, international organizations, or foreign governments.
- U.S. federal gov lists are maintained by different agencies and are publicly available.

Restricted or Prohibited Parties' Screening

- **Due diligence** process to determine whether any parties involved in a transaction are listed on watch lists maintained by multiple U.S. government and international agencies.
- **Ensures** that we are not doing business with a party of concern.
- Conducted by different offices/business units across Emory



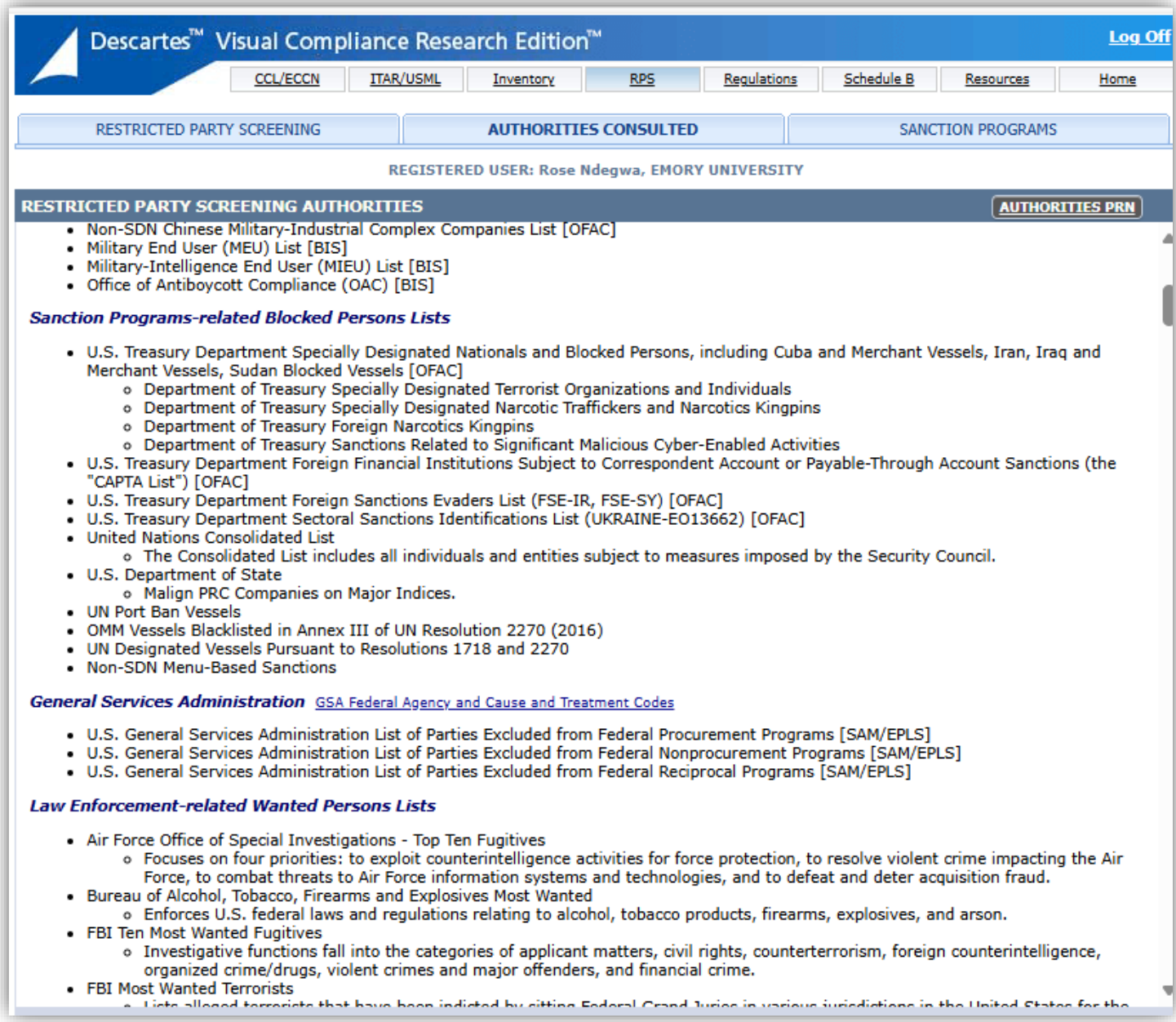
Emory Departments/Offices

Over 80 Active Users

ADVANCEMENT AND ALUMNI ENGAGEMENT	OSP	HUMAN RESOURCES	GLOBAL ENGAGEMENT	RCRA
IRB	OTT	WISC/OCR	PROCUREMENT	FINANCE OPERATIONS
	SOM	SOM/ BME Admin	EGHI/IANPHI	

Restricted or Prohibited Parties' Screening

- Emory uses Descartes Visual Compliance
- Consolidates over 80 lists
- Contact Export Control Office for help with
  - Access to Visual Compliance
  - Evaluating screening results
  - Training in use of software



EMORY UNIVERSITY | Research Compliance and Regulatory Affairs