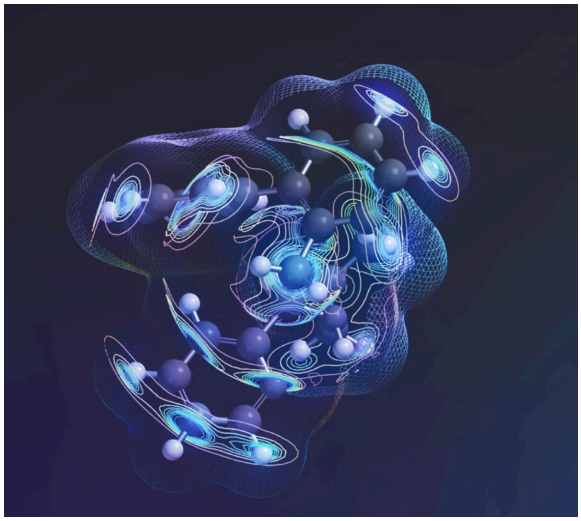
CASC | Coalition for Academic Scientific Computation

NIST SP 800-171 – Guidance for Research Computing and Data Centers



Background

Twenty years ago, the U.S. federal government introduced a set of cybersecurity standards under the National Institute for Standards and Technology Special Publication 800-53 (NIST SP 800-53) to protect federal information as required by the Federal Information Security Management (FISMA) Act of 2003. In 2010, Executive Order 13526 introduced Controlled Unclassified Information (CUI) [1]. A subset of 800-53, called NIST SP 800-171, was developed and documented to guide non-governmental entities, such as universities and businesses, on how to safeguard CUI that they receive, store, process, or transmit on behalf of federal agencies [2]. For these organizations, compliance with standards is often mandated through contractual clauses or data use agreements as a prerequisite for accessing federally controlled data.

Until recently, NIST SP 800-171 (hereafter referred to as 800-171) primarily applied to universities with Department of Defense (DoD) and NASA contracts, where compliance has been mandatory since 2018. This landscape shifted significantly when the National Institutes of Health (NIH) released the notice "Implementation Update for Data Management and Access Practices Under the Genomic Data Sharing Policy" (NOT-OD-24-157). Effective January 1, 2025, this notice requires computing systems that store NIH controlled-access

data—such as the Genotype and Phenotypes database (dbGaP)—to meet the cybersecurity standards outlined in 800-171.

This new requirement means research computing and data (RCD) centers that support genomic analysis must develop strategies to secure high performance computing (HPC) systems. Institutions responsible for data governed by HIPAA or FERPA must also assess how 800-171 requirements align with their existing control environments. The unique resource and architectural needs of genomics and other data-intensive scientific workflows in HPC environments often present new challenges, even for early adopters. As a result, many RCD centers are now actively seeking information and implementation guidance.

This paper aims to highlight pressing issues and describe potential solutions for leaders and managers of RCD center infrastructure and support organizations who are faced with understanding and implementing 800-171 compliance. It will serve as a resource for stakeholders at research-intensive institutions – including members of the Coalition for Academic Scientific Computation (CASC), Chief Information Officers (CIOs), Vice Presidents for Research (VPRs), Chief Information Security Officers (CISOs), and Research Integrity and Compliance Officers.

The introduction of 800-171 requirements reinforces the need for researchers to understand that, while their institution holds ultimate responsibility for compliance, they also have individual responsibilities to operate within the compliance framework. Moreover, 800-171 compliance cannot be addressed solely through technical or architectural configurations. Achieving compliance often requires a culture shift among RCD center staff, faculty, and the broader institution. Recognizing that cultural change can be challenging in large organizations, this paper outlines several interconnected challenges institutions face in implementing and sustaining compliant environments for regulated research. Some challenges are technical, but many are organizational, requiring cross-functional collaboration and strategic alignment among leadership, IT, information security and privacy offices, legal counsel, research administration, and faculty stakeholders.

Challenges

Institutional Buy-in and Executive Responsibility. Successful implementation of an 800-171 compliance program is a shared institutional responsibility and requires coordination among a wide array of stakeholders. Information Security Officers and RCD center staff play key roles in decision making and implementation of technical components of any compliance effort; however, other units and personnel who should be involved include institutional compliance officers, information technology leadership, and the leadership in the institution's Office of General Counsel and Institutional Review Board. Historically, these offices use different terminologies,

frameworks, and reporting lines, posing more challenges to aligning around a complex technical and regulatory framework like 800-171.

Effective Governance. Governance must foster regular communication, facilitate shared decision making, and clearly define roles and responsibilities for compliance oversight, system implementation, user support, and incident response. 800-171 compliance must include robust mechanisms for continuous evaluation and adaptation. This includes defining key performance indicators (KPIs) and metrics for compliance readiness, platform adoption, user satisfaction, and incident response efficacy. Regular audits, self-assessments, and dashboard reporting should be integrated into the governance framework to provide transparency and guide iterative improvements. For examples of governance structure, including CUI governance structure, see Appendix A.

Communication/Education. Cross-unit training initiatives can bridge gaps in understanding – especially around technical controls and risk management concepts – ensuring that all parties have a consistent grasp of their responsibilities. Communication strategies should focus on demystifying the technical elements of 800-171 while empowering stakeholders to make informed decisions aligned with institutional risk tolerance.

Faculty Engagement. Faculty RCD users must be engaged in developing compliance efforts to ensure their research is conducted efficiently, effectively, and safely. Programs designed to meet 800-171 requirements must be user-friendly, support mixed workflows, and minimize disruptions to research activities. Reducing administrative friction and “time to science” is critical for maintaining research productivity while ensuring data security and regulatory compliance.

Sustainability. Compliance with 800-171 is a dynamic, continuous process that demands persistent maintenance, periodic reassessment, and regular updates to technical infrastructure and policy. A successful sustainability model includes dedicated funding streams and staffing plans to support compliance efforts over time, avoiding the trap of one-time grant-based solutions that lack continuity.

Different Agency Requirements. While the 800-171 framework provides a common set of controls to be leveraged for security compliance, different federal funding agencies (and at times different programs within a funding agency) require different applications of the standard. For example, the recently updated NIH requirements for sharing genomic data sets require compliance with 800-171 r3, [3] while CUI and the current Cybersecurity Maturity Model Certification (CMMC) 2.0 L2 standards designate following 800-171 r2. [4]. Beyond the different versions of 800-171, funding agencies have their own standards of compliance, such as HIPAA, which secures protected health information (PHI), and the International Traffic in Arms Regulations (ITAR), which regulate how national defense data and technologies can be shared. NASA has historically had its own custom security requirements, though it seems to be moving towards leveraging

the 800-171 (and perhaps CMMC) standards.

Finally, 800-171 compliance should never operate in isolation; it must be seamlessly integrated into broader data governance and digital strategy efforts. Institutions should look for alignment with enterprise-wide data classification policies, data lifecycle management plans, and cloud governance models. Integration will ensure consistency in data handling and avoid duplication of effort while strengthening the overall institutional posture on data stewardship.

Understanding Requirements

The 800-171 controls are organized into "families" covering Access Control, Incident Response, System and Communications Protection, Configuration Management, and Security Assessment. Each family includes requirements for different aspects of system security, such as user access management, encryption, security monitoring, and vulnerability management. 800-171r2 includes 14 control families and 110 specific CUI controls. Revision 3, released in May 2024, introduced 17 control families and reduced the number of CUI controls to 97. In most organizations, no one person or single unit can manage all the control families or specific controls. The scope in which controls are applied – for example, within a secure enclave for handling sensitive data, an RCD center environment, or an enterprise IT infrastructure – directly influences the complexity and the specificity of associated policies and procedures. In turn, that determines which units are responsible for drafting, implementing, and periodically reviewing controls. Understanding controls and control families is critical, since noncompliance requires a Plan of Action and Milestones (POAM) to address deficiencies, detailing the corrective actions and timelines for compliance [5]. In general, 800-171 compliance requires a central cross-unit team that will:

- Identify the system boundary for all components that transmit, store, and process CUI.
- Use the NIST assessment guide [6] to review each control and document how the control is being met.

Appendix B shows a possible version of an organizational responsibility matrix.

Compliance: Assessment, Audit and Risk

To comply with standards, keep data secure, and avoid the risks of noncompliance, organizations must ask themselves a series of questions, which will inform their actions.

WHAT to Assess? Identify the scope of the systems to assess. For CUI, all elements within the system that transmit, store, or process data must meet compliance requirements. Most institutions establish a well-defined, separate environment for CUI compliance. An inventory of all in-scope assets, including people, facilities, and technologies, will be needed.

HOW to Assess? Identify which revision of 800-171 is required for your situation. Some agencies, such as DoD, require 800-171-r2, while others, such as NIH, require 800-171-r3, although NIH has stated that compliance with r2 is acceptable. For each of the 320-r2 assessment objectives or 390-r3 objectives, organizations must document either: (a) how they are meeting the requirement or (b) a plan of action for how and when they will meet the requirement. The controls used will define a combination of technical implementation, policies, and documented procedures. This documentation will result in a System Security Plan (SSP) and/or a Plan of Action and Milestones (POAM) for addressing controls not yet met. A helpful guide for securing HPC systems is the NIST publication "High-Performance Computing Security: Architecture, Threat Analysis, and Security Posture."[7]

WHO Does the Assessing? Assessment is a team process. After system administrators configure the systems, security staff weigh in on whether the configuration meets the required standard, and research compliance officers attest that the organization complies with grant and contract requirements. Local IT support staff might also participate in the process. An established governance system provides the framework for this work.

WHEN to Assess? An 800-171 compliance program is a continuous process; the SSP is not a "one and done" document. POAMs will have defined goals and deadlines. Implementations will need discussion, review, and agreement. The status of all controls should be reviewed regularly, allowing your organization to incorporate any updates to the 800-171 standard.

HOW to Determine Compliance? Different agencies interpret compliance with different degrees of rigor. For example, NIH has stated that creating SSPs and POAMs that include dates for when unmet controls will be in place is currently adequate for storing and processing NIH controlled-access data. The DoD requires institutions to self-assert a compliance score in the federal Supplier Risk Performance System (SPRS). CUI in DoD contracts requires CMMC, which, beginning in 2026, will require an external audit to certify compliance and the validity of SPRS scores. A written audit by an external party – whether required or not – can be a valuable tool for communicating the condition of your system and confidence in

its compliance. However, such an audit can be expensive (think six figures), so make sure you are ready for this step.

What's the RISK in Failing to Comply? NIH requires genomics data sets to be compliant with 800-171 for researchers to have access to those data sets. For DoD contracts, entering an inaccurate SPRS score could make your institution vulnerable to lawsuits under the False Claims Act, with significant financial penalties as well as loss of reputation.

Scoping

Once you have institutional support to develop a protected 800-171 compliant environment, how should you proceed? How do you determine what is within scope, and how do you balance completeness and cost? While there is no single path that is the best, your compliance program should consider: (1) your use case and implementation needs; (2) the time frame for deployment; and (3) cost. Expenses to consider include: personnel (compliance staff, training needs, auditors); technology and infrastructure (monitoring tools, software and licensing, secure cloud or on-premise systems); and regulatory requirements (incident response, legal and compliance considerations, certifications, and possibly evaluation of an existing insurance policy).

On-site or in the cloud? On-site deployments of 800-171 compliant architectures require long lead times. From the initial planning and design to the acquisition of equipment and the implementation of cybersecurity controls, to creating standardized processes and designing onboarding and marketing materials, this undertaking will take at least a year to complete. Cloud providers often offer building blocks for organizations to compose protected environments along with some management tools as a service (aaS). The aaS framework can provide an easy on-ramp for 800-171 compliance, deploying a protected environment quickly. Cloud providers also have templates and orchestration tools to deploy infrastructure to meet specific cybersecurity requirements. Keep in mind that successful cloud deployments still require governance and coordination at the institution; cloud providers only provide the infrastructure with some attestation that a subset of the controls are implemented as required.

Cloud computing can be costly and includes costs for using compute resources, storage capacity, and network bandwidth. A cloud environment also includes costs for licensing of common software to meet the security needs of vendors such as Amazon Web Services, AWSGovCloud, or Microsoft 365 Government Community Cloud High. Costs should directly correspond to the uses of a

protected environment. For example, if users share documents, the cost for securing digital intellectual property (IP) in the cloud should be manageable. If users require HPC infrastructure, such as high performance CPU nodes with large core counts, high-end GPUs for generative AI, or high-bandwidth and high IOPS storage for data-intensive computing, costs can quickly strain the budget. Several studies comparing the cost of on-site HPC systems to cloud computing deployments estimated the cloud to be three to eight times more costly compared to on-premise operations [8].

Retrofitting as a middle-ground solution. Retrofitting an existing protected environment to comply with new requirements or upgrading to a higher security level takes time and planning, but less than deploying a new system, and costs may be less daunting than cloud solutions. In the effort to comply with updated cybersecurity requirements for NIH grants, more than half of CASC member institutions have taken the path of retrofitting an existing HIPAA environment to meet the 800-171 standards (called self-attestation). These are typically R1 institutions with substantial HPC workloads in "omics" and generative AI. Some member institutions have taken the cloud computing path. In some cases, an institution may subscribe to another institution's mature on-premise protected environment as a service.

The path to compliance with the 800-171 requirements will depend on how your resources are used, the timeline for full deployment, and costs. Determining what elements are within your scope depends on where you are in the journey. While CMMC might be considered the gold standard for compliance, it is not the end goal for RCD centers. For these centers, a protected environment is simply a step toward enabling new scientific discoveries. Various resources can help RCD center managers and administrators figure out costs and requirements. These include the Council on Government Relations (COGR) [9], the document Federal Acquisition Regulation: Controlled Unclassified Information [10], and a Federal Register document on the federal CMMC program [11].

Determining Cost. The costs of compliance vary widely, but several organizations have examined them:

A COGR survey found that members with R&D expenditures of less than $100 million spent $12,500 in IT costs and another $7,400 on preparation and training for compliance. Larger centers reported spending about $147,000 for IT and another $65,555 for preparation and training [12].

The Federal Register CMMC program estimates the cost of self-assessment for 800-171 compliance to meet NIH genomic data guidelines at $37,196 for a three-year assessment at a smaller center, while a third-party assessment increases that cost to $104,670. For larger centers, those numbers increase to $48,827 and $117,768, respectively [13].

These costs do not consider upgrades and new implementations of HPC hardware and software. Also, centers that require fully isolated systems for CMMC need to include costs of hardware, networking, storage, identity management, any cloud services, and staffing. Those sustained costs could be in the millions annually. RCD centers in higher education can recoup at least some costs through different service models. [14]

Recommendations and Actions

For those at RCD centers that handle CUI or sensitive NIH data, the course of action is clear: make your center 800-171 compliant in the most efficient and effective manner possible. Compliance involves different specifics for different organizations, but awareness of the following factors should make compliance easier.

Get your governance right. Compliance with 800-171 requires continuous evaluation, and that means clearly defining key performance indicators, metrics for measuring success, setting up transparent reporting systems, and more. A clear governance plan that delineates who is involved in compliance, what responsibilities they have, who they report to, and who makes the final decisions will make compliance less stressful and more likely to succeed.

Understand your data. Not all data needs special protection, and CUIs connected to different projects will require different levels of protection. Likewise, different federal agencies have their own compliance and assessment requirements, meaning that working with the NIH data, for example, won't be the same as working with DoD data. If you know your data, you will understand the capabilities needed to handle it and comply with 800-171.

Be aware of different details around compliance requirements. For example, NIH-controlled access data repositories require organizations to complete System Security Plans (SSPs) and POAMs to process, store, and transmit that data. CMMCv2 compliance will require certification by an external assessor every three years.

Have a clear picture of costs and risks. As costs rise, organizations must work to keep their compliance plans within scope. They must know the limitations of their computational and data resources, whether they can leverage technologies and people within the organization, and what risks they run by being noncompliant. Those risks include the possibility of losing government contracts, financial penalties, legal consequences, and reputational loss.

Community Action: A Call for Harmonized Compliance

Multiple regulations for different agencies and an alphabet soup of acronyms are not the most effective way to manage sensitive data that needs to be protected. Heterogeneous regulations make compliance more difficult, especially for smaller organizations that can't afford a large number of specialized staff. T*he CASC community, the HPC community, and the larger community of nationwide research data centers must begin dialogues with federal agency representatives to advocate for harmonized compliance requirements between agencies.* Developing one compliance system will save time, dollars, and physical resources for RCD centers and others that must comply with 800-171. It will streamline government agency compliance activities, simplify using CUI data without sacrificing data security, and make research easier and more productive.

Most research to date on 800-171 compliance involves business organizations, rather than RCD centers that are usually located on university campuses and often part of the larger campus IT infrastructure. More research into the costs and implementation issues in higher education settings will help RCD centers better understand compliance issues relevant to their organizations. *CASC will work with the RCD community to gain a clear picture of costs, benefits, and risks surrounding 800-171 for RCD centers in higher education.*

Key Takeaways

- RCD centers that handle Controlled Unclassified Information (CUI) must comply with NIST SP 800-171 requirements, including centers with grants from the National Institutes of Health under its new Genomic Data Sharing policy. RCD center professionals must understand these policies, how they might impact their centers, and consider the resources and architectural needs for compliance.
- Understanding 800-171 controls and control families is critical to achieving and maintaining compliance. When organizations are not in full compliance, they must develop a Plan of Action and Milestones (POAM) to document deficiencies, outline corrective actions, and establish timelines for resolution.
- While some funding agencies, such as NIH, allow for self-attestation to show compliance, others, such as

the DoD, require CMMC to show compliance – a system that will require an external audit beginning next year. Whether required or not, a written audit by an external third party can be valuable for communicating the condition of your system and confidence in its security.

- If the timeframe to compliance is short, RCD centers might choose to deploy a protected system in the cloud. However, cloud environments can be costly and include the price of using compute resources, storage capacity, and network bandwidth, as well as costs for licensing common software that meets vendors' security needs.
- Deploying new RCD resources that meet compliance requirements is often too costly and can take years to deploy. Retrofitting an existing system is another option that requires less time and fewer expenses than a cloud solution. The path to compliance will depend on how your resources are used, the timeline for full deployment, and costs.
- The road to compliance will be different for different RCD centers, but in general, it will involve setting up a clear governance plan, understanding your data and what needs to be protected, awareness of different compliance standards, and a clear picture of costs and risks.

Authors: *Karen Green; Jill Gemmill, Clemson University; Kim Wong, University of Pittsburgh; Carolyn Ellis, Arizona State University; Jeremy Frumkin, University of Arizona; H. Birali Runesha, University of Chicago; Katia Bulekova, Boston University; Deepa Phanish, Georgia Institute of Technology; Jason Christopher, University of California Berkeley, Alex Pacheco, New Jersey Institute of Technology; Brian Christian, Case Western Reserve University; Tabitha Samuel, University of Tennessee, Knoxville; Erik Deumens, University of Florida; Subhashani Sivagnanam, San Diego San Diego Supercomputer Center; Carolyn Casler, CASC; Kathryn Kelley, CASC*

About CASC

The Coalition for Academic Scientific Computation is an educational nonprofit 501(c)(3) organization with 105+ member institutions representing many of the nation's most forward-thinking universities and computing centers. CASC is dedicated to advocating for the use of the most advanced computing technology to accelerate scientific discovery for national competitiveness, global security, and economic success, as well as develop a diverse and well-prepared 21st century workforce. Learn more at http://casc.org.

References

[1] Controlled Unclassified Information (CUI) Registry. National Archives. https://www.archives.gov/cui/registry/category-list

[2] Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. & Guissanie G. (2020). NIST SP 800-171r2. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." https://doi.org/10.6028/NIST.SP.800-171r2.

[3] Ross R. & Pillitteri V. (2024). NIST SP 800-171 Rev. 3 (2024). "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." https://doi.org/10.6028/NIST.SP.800-171r3.

[4] Cybersecurity Maturity Model Certification (CMMC) Model Overview, Version 2 (2021). U.S. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

[5] Thepsiri, T. (2024). "What Is A NIST 800-171 POAM (Plan Of Action & Milestones) & Key Steps." Kelser Corporation. https://www.kelsercorp.com/blog/what-is-a-nist-800-171-poam-plan-of-action-milestones.

[6] NIST Special Publication 800-30 Revision 1 (2012). "Guide for Conducting Risk Assessments."] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

[7] Guo, Y., et. al. (2024). "High-Performance Computing Security Architecture, Threat Analysis, and Security Posture." Special Publication (NIST SP) https://doi.org/10.6028/NIST.SP.800-223

[8] Rajamohan, S. and Settlage, R. (2020). "Informing the On/Off-prem Cloud Discussion in Higher Education." Presented at PEARC '20: Practice and Experience in Advanced Research Computing. https://doi.org/10.1145/3311790.3396627.

[9] Council on Government Relations (COGR). https://www.cogr.edu/

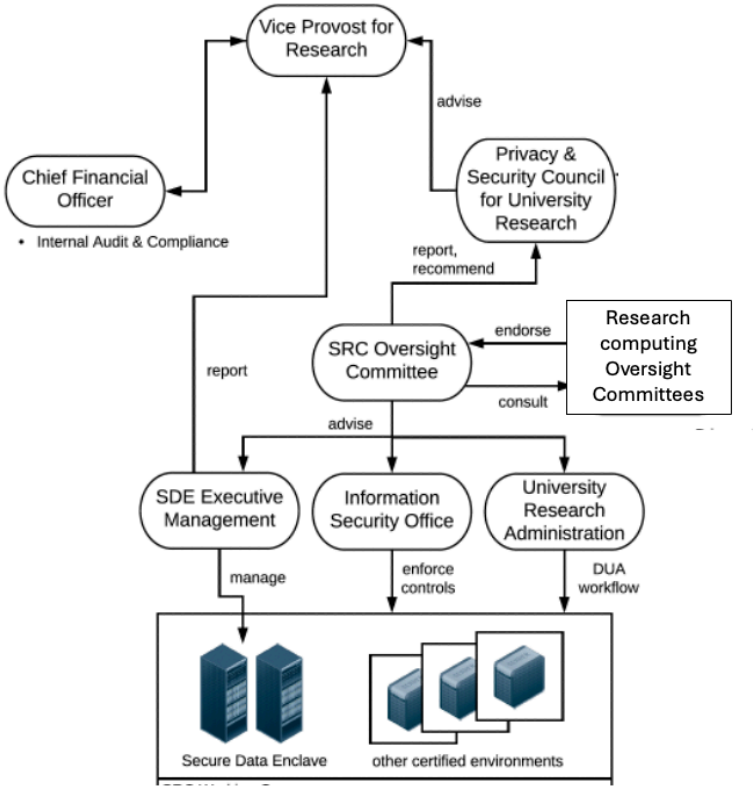
[10] Federal Register, The Daily Journal of the United States Government (2025). Federal Register/Vol. 90, No. 9/Wednesday, Jan. 15, 2025/Proposed Rules. https://www.govinfo.gov/content/pkg/FR-2025-01-15/pdf/2024-30437.pdf

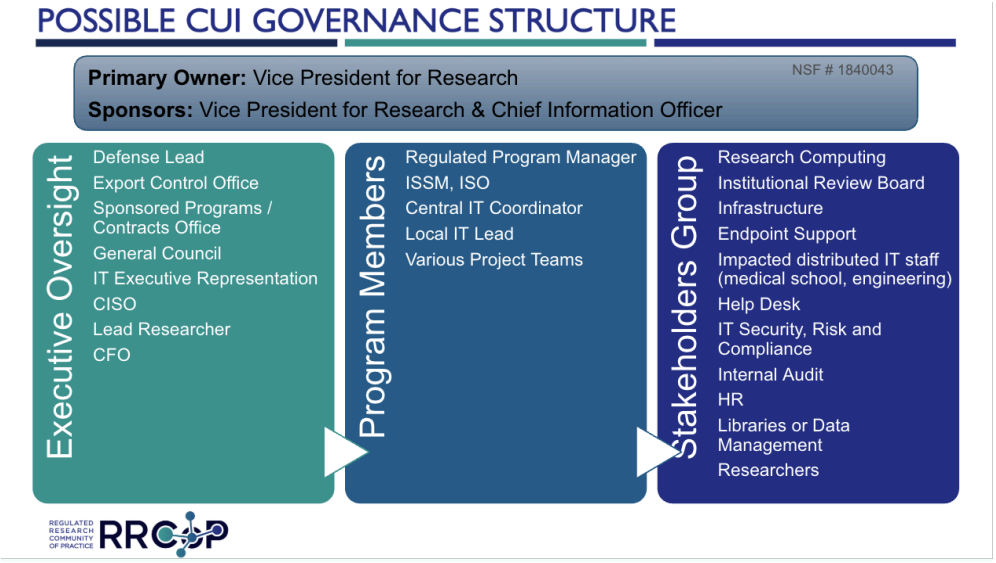
[11] Federal Register, The Daily Journal of the United States Government (2024). Federal Register/Vol. 89, No. 199/Tuesday, Oct. 15, 2024/Rules and Regulations. https://www.govinfo.gov/content/pkg/FR-2024-10-15/pdf/2024-22905.pdf.

[12] Council on Government Relations (2025). "Summary of Recent Significant Updates to the NIH Genomic Data Sharing Policy." https://www.cogr.edu/sites/default/files/Summary%20of%20Recent%20Updates%20to%20the%20NIH%20Genomic%20Data%20Sharing%20Policy%20Update%20Jan%203%202025_1.pdf

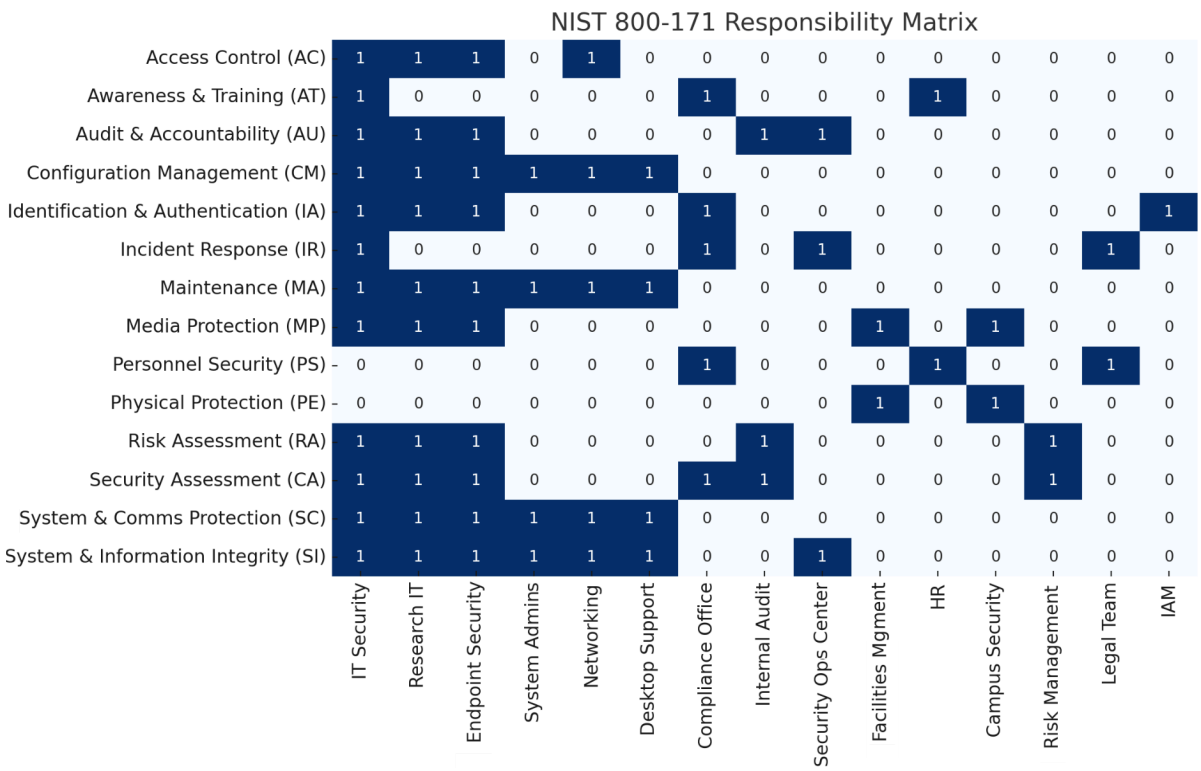
[13] Federal Register, The Daily Journal of the United States Government (2025). Federal Register/Vol. 90, No. 9/Wednesday, Jan. 15, 2025/Proposed Rules. https://www.govinfo.gov/content/pkg/FR-2025-01-15/pdf/2024-30437.pdf
[14] EDUCAUSE (2023). Cloud Computing Contract Advisory. https://library.educause.edu/resources/2023/5/cloud-computing-contract-advisory

Appendix A




POSSIBLE CUI GOVERNANCE STRUCTURE
NSF # 1840043
Primary Owner: Vice President for Research
Sponsors: Vice President for Research & Chief Information Officer
Executive Oversight
Defense Lead
Export Control Office
Sponsored Programs / Contracts Office
General Council
IT Executive Representation
CISO
Lead Researcher
CFO
Program Members
Regulated Program Manager
ISSM, ISO
Central IT Coordinator
Local IT Lead
Various Project Teams
Stakeholders Group
Research Computing
Institutional Review Board
Infrastructure
Endpoint Support
Impacted distributed IT staff (medical school, engineering)
Help Desk
IT Security, Risk and Compliance
Internal Audit
HR
Libraries or Data Management
Researchers
REGULATED RESEARCH COMMUNITY OF PRACTICE
RRCoP

Appendix B


NIST 800-171 Responsibility Matrix
Access Control (AC) 1 1 1 0 1 0 0 0 0 0 0 0 0 0 0
Awareness & Training (AT) 1 0 0 0 0 0 1 0 0 0 1 0 0 0 0
Audit & Accountability (AU) 1 1 1 0 0 0 0 1 1 0 0 0 0 0 0
Configuration Management (CM) 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0
Identification & Authentication (IA) 1 1 1 0 0 0 1 0 0 0 0 0 0 0 1
Incident Response (IR) 1 0 0 0 0 0 1 0 1 0 0 0 0 1 0
Maintenance (MA) 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0
Media Protection (MP) 1 1 1 0 0 0 0 0 0 1 0 1 0 0 0
Personnel Security (PS) 0 0 0 0 0 0 1 0 0 0 1 0 0 1 0
Physical Protection (PE) 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0
Risk Assessment (RA) 1 1 1 0 0 0 0 1 0 0 0 0 1 0 0
Security Assessment (CA) 1 1 1 0 0 0 1 1 0 0 0 0 1 0 0
System & Comms Protection (SC) 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0
System & Information Integrity (SI) 1 1 1 1 1 1 0 0 1 0 0 0 0 0 0
IT Security
Research IT
Endpoint Security
System Admins
Networking
Desktop Support
Compliance Office
Internal Audit
Security Ops Center
Facilities Mgment
HR
Campus Security
Risk Management
Legal Team
IAM