2022 CASC Top Priority Areas: Improve Cybersecurity and Compliance

Summary Statement

Research Computing and Data (RCD) institutions, including CASC members, should create a structured approach to cybersecurity and compliance, optionally including the use of security enclaves, and audit their programs in these areas regularly. Research sponsors at the federal level should include academic RCD representation on relevant advisory bodies to ensure adequate input and take steps to provide consistent guidance on topics in these areas to federal program officers. State governments should work to minimize extra regulatory layers and customize requirements only when necessary. CASC should establish a standing cybersecurity and compliance working group to advise members on these topics.

Why it Matters

Cybersecurity and compliance with regulatory requirements have become increasingly important to academic institutions with RCD centers. In 2015, the Federal Acquisition Rules (FAR) outlined that all data needs to be classified in a consistent way as specified by 2009 Executive Order 13526 [Federal Register vol 75 no. 2, Jan 2010]. Previously the Federal Information Security and Management Act [FISMA 2002; Public Law 107-347] required similar security compliance for data managed by federal agencies, but it was found that many data breaches occurred with contractors, hence this suggested enhancement of the FAR was introduced.

The 2015 FAR language was adopted for defense contracts through the Defense Federal Acquisition Rules Supplement (DFARS). Enforcement began in Dec 2017, with an increasing number of Department of Defense (DoD) academic hosted research awards subsequently requiring compliance. The program often relied on self-assessment, and unfortunately, many organizations lacked the expertise to adequately assess their security practices and controls. These concerns led to a renewed effort by the DoD called the Cybersecurity Maturity Model Certification (CMMC) beginning in 2019. The implementation of this program was pursued and extensively debated, with version 2.0 announced in November 2021.

Multiple federal requirements related to privacy also exist and continue to be updated. Documenting compliance with such requirements is increasingly crucial for data sets commonly utilized in the social and medical sciences. Specifically, federal privacy regulations protect personally identifiable information (PII) such as social security numbers [Federal Privacy Act of 1974; Public Law 93-579; 5 U.S.C. 552a] and individual student records [Federal Family Educational Rights and Privacy Act [FERPA 1974; 20 U.S.C. § 1232g; 34 CFR Part 99]. Personal Health Information (PHI) privacy is federally regulated by the Health Insurance Portability and Accountability Act [HIPAA 1996; Public Law 104-191]. Institutions have legal and ethical obligations to protect such research data in compliance with all the, often overlapping, privacy and cybersecurity regulations.

Beyond the legally binding compliance obligations, RCD centers also must defend our institutions and users from malicious intellectual property (IP) theft, denial of service/resource (DoS) attacks, use of the computational power for offensive cyberattacks (botnets), and institutional ransom (ransomware). In 2021, numerous academic and private organizations were the targets of successful ransomware attacks. As a result, several federal agencies have followed DoD's practices of including security requirements in their contracts with universities, and state governments have often added further contractual requirements and restrictions.

To protect the research, academic, and business operations of universities from attacks, universities must commit to achieving increased cybersecurity awareness and implement appropriate controls. We can break these considerations into categories of risks and benefits.

Risks

- Grants and contracts sometimes include mandates for regulatory compliance, such as the example given above of compliance with DFARS for DoD. Other federal agencies like NASA, USDA, NIH, and various state agencies are also increasingly putting forth compliance requirements.
- A consequence of the increase in ransomware attacks beginning in 2021 is that cybersecurity insurance policies have become significantly more expensive and some institutions with no cybersecurity program or immature programs cannot get cybersecurity insurance at all.
- Individual faculty members and their lab group participants can no longer rely on informal practices to ensure compliance and protect their research methods using ad-hoc methods. A systematic university-wide program that utilizes state-of-the art tools, resources, and talent is necessary to ensure conformance with current cybersecurity and compliance best practices.

Benefits

- A well-organized compliance program ensures that the university is well-prepared to support all types of research data including its supporting infrastructure and methods.
- The primary goal of the federal Controlled Unclassified Information (CUI) data protection program is to protect export-controlled information. Implementing these practices, also help protect other forms of university intellectual property in the form of research products such as data, papers, software, dissertations, and theses. These practices help ensure appropriate attribution via publication and reduce the risk of important discoveries being claimed in an unwanted way by external entities.
- A mature cybersecurity program enhances the reputation of the university, attracts new faculty, and opens up new paths to funding and collaborations.
- Effective cybersecurity, once considered only as a cost, is now viewed as a strategic investment. Much like wired and wireless network infrastructure, it enables new capabilities and helps generate revenue for universities.

Current Challenges

The primary challenges designing a cybersecurity program include technical controls, training of stakeholders, staffing, and procedures to execute the processes as designed. In meeting these challenges, the goal should be to produce an ecosystem of controls that enhance and facilitate the security of research operations and protect the interests of all parties without interfering unduly with research productivity. The designers of cybersecurity and compliance programs also face the challenge to keep in mind the research goals of the systems being secured so that they can effectively serve both the mission of the institution and the reporting and functional needs of these programs.

While technical controls are sometimes considered to be straightforward to implement by RCD experts, it is important to note that the Executive Order[1] 14028 of May 2021 calls for use of Zero Trust principles that require architecture and design and cannot be addressed by merely purchasing software or add-on tools. That means that implementation of these principles requires, in addition to funds for specialized equipment and software, time and

[1] Executive Order 14028 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

effort from system administrators and network engineers to design and configure the systems based on zero-trust principles.

All stakeholders require training to familiarize themselves with the structure and processes of the cybersecurity program. The organization's leaders need to realize why cybersecurity is important and what resources must be committed to the program. The engineers operating the systems need adequate background knowledge and experience specific to this area. The researchers (and data stewards) who handle the restricted data often require training explicitly mandated by the compliance framework. Recruiting and retaining expert staff can be difficult in areas of cybersecurity and compliance due to the very high demand for this specific skill set.

Institutional commitment is needed to execute the cybersecurity program, to follow the procedures, and to execute the processes as designed, documented, and taught. Accountable personnel must continuously monitor the systems and act on alerts in a timely manner. The complexity of cybersecurity and its inherently hands-on nature, opens up the possibility that an organization will not follow through consistently on its designed cybersecurity program. Such a condition immediately reduces the effectiveness of the program and the value of all investments, in hardware, software, time, and effort, made in cybersecurity.

Compliance programs should be developed in-step with cybersecurity programs. A strong compliance program ensures that the organization enforces documentation and processes that monitor the application of cybersecurity measures.

Specific challenges and corresponding possible solutions exist in the following areas.

Organizational Structure

Academic institutions typically have distributed authority and accountability structures that include such elements as the offices of the Provost/Chancellor, President, Board of Trustees, Information Technology (Chief Information Officer and Chief Information Security Officer), Research, Compliance/Privacy, Internal Audit, General Counsel. Each of these has specific university functions. For example, the Office of Research is often the fiduciary agency that signs a contract and therefore they can be the owner or the primary customer dictating the requirements of the service. General Counsel, Privacy, and Internal Audit offices can provide important external advisors to ensure the quality of the cybersecurity program. A faculty governance committee can also provide important input to the operation of the program and to the service owners.

Successfully implementing compliance programs requires getting the right people to agree on the structure, responsibilities, and governance of a cybersecurity and compliance program. For example, Information Technology or Research Computing departments or divisions might be good choices to operate a given service, but the Information Security Office and the CISO will also need to be involved as a partner to retain independence in assessing and auditing the service. Each institution faces such challenges routinely in defining and implementing its research programs to ensure that the right parties are involved at the right levels.

Scoping the System Security Boundary

An effective cybersecurity program must carefully consider where to impose the technical controls, and how to design the processes and procedures so as not to jeopardize the mission of the institution. For example, making all campus information and operations compliant with NIST 800-171 is neither practical nor advised.

Sustainability and Cost Models

Cybersecurity and regulatory compliance are sometimes considered only as costly intrusions that researchers or their institutions would like to minimize. The challenge in these areas is to implement measures to achieve these goals in ways that produce documented benefits that are obvious to all participants. A properly funded cybersecurity program is a strategic necessity for an institution. Saying "our organization does not handle regulated data compliance" is no longer a viable option to retain the range of data handling capabilities expected of a modern RCD organization. Instead, the focus should be on putting programs into place that increase the range of research possible at an institution due to protections that are in place and protecting and preserving the research data and processes of the institution.

Cost models for cybersecurity and compliance need to be built into institutional plans and included directly in funded research programs to achieve sustainability. To achieve this condition will require alignment of funding agency programs, community goals, and institutional practices along the lines discussed earlier in this document.

Auditing Compliance

Self-assessment is allowed in many compliance requirements but carrying out a valid assessment requires expertise and experience that is not always available among staff at institutions. External audits do incur extra cost and also require effort and expertise by the staff to avoid the very expensive audits where the external party is contracted to do all the work.

A solid compliance program should have credible, preferably external, audit and assessment reports against at least one chosen compliance framework. Organizations currently must map many frameworks to the one (or subset) that their institution uses and negotiate with contractors to have that report be provided in an acceptable format. Higher education operates differently from companies for which the compliance frameworks were developed; as a result, some recommended controls implementations may have severe impacts on the research activities of academic institutions.

Multiple federal agencies, states, and companies all introduce their own requirements. The institution may need to negotiate to have the available report accepted in place of custom reports and requirements requested by the various federal agencies, states, and companies. If standardization can be achieved, this would save the institution considerable cost and effort.

Impact on Research Projects

Clarifying what projects and data need to be covered by compliance (systems and processes) at the contract stage is often a challenge, as contract managers at federal and state governments and at companies prefer to leave themselves the freedom to avoid such details and instead put the burden of determination on the university. Security professionals, such as the CISO, tend to impose requirements too strictly or in terms that are too broad, jeopardizing what researchers perceive to be the mission of the university by not incorporating the unique characteristics of research computing that differ from enterprise computing characteristics.

Researchers are sensitive to the burdening impacts that compliance processes can place on their workflow. It is therefore sometimes a challenge to get their buy-in. To deal with this challenge, buy-in from researchers can be facilitated by making them partners in the governance. In this way, cooperation can be achieved once they realize that the service is responsive to their needs, the compliance effort and benefits are not negligible, and their institutional partner is taking care of them properly.

Vision of Success

Successful cybersecurity and compliance programs will have the following characteristics:

Institutional buy-in: Institutional administration agrees that such programs are strategic to the institution's success and may require investment from the institution, as opposed to considering them just as cost centers that should be minimized or eliminated.

Clear policies exist, backed up by procedures, guidance, and training, for students, faculty, and staff to follow when confronted with the need to deal with data and objects covered by laws, regulations, or contractual obligations.

A sustainable business model is in place that ensures that all stakeholders have skin in the game. The university pays for some things, and the researchers contribute from grants and contracts. Free access to resources often leads to biased estimates for need, which jeopardizes long-term planning. Long-term planning in the cybersecurity and compliance world is crucial since one cannot arbitrarily drop the service once the contract is signed.

Research productivity: The researchers can achieve their goals while protecting the integrity of their data and methods with efficient and well-documented procedures. Compliance and security controls are well integrated into research processes that enhance rather than interfere with routine data processing and handling and preserve opportunities for appropriate sharing and scientific discovery.

Recommendations and Next Steps

Best Practices for Member Institution Implementation:

1. **Create a Structured Approach to Cybersecurity and Compliance.** Establishing compliance with at least one of several cybersecurity frameworks is a necessary first step to address the threat of cyberattacks. The associated compliance program will institutionalize a list of processes that allow the organization to minimize the risk of cybersecurity events becoming devastating and impacting the mission of the organization. A compliance program requires institutional buy-in, funding, a balance of mission vs. risk, a commitment of the stakeholders, and training, awareness, and communication activities. It also involves putting technical staffing and controls in place.

2. **Consider Use of Security Enclaves.** Separate security enclaves, operated using on-premises or commercial cloud services or through network isolation, can sometimes be used. Such enclaves, if used, must have the ability to support coherent inter-related infrastructures, such as data in labs where instruments are housed that are subject to compliance requirements and need to exchange data with each other but be isolated from other interactions. The architecture of each system should allow for a coherent overall approach with relatively little extra effort required to add a lab that becomes in scope with some new contract. The staff expertise, documentation, policies, training, and guidance can all be leveraged to save cost and make the cybersecurity program nimble.

3. **Audit Cybersecurity and Compliance Programs on a Regular Basis.** One important part of the compliance program is the process of auditing the compliance on a regular basis. The organization can define who will audit, what will be audited, and how often; it is crucial that some auditing happens, and that institutional leadership sees the audit reports. Most academic institutions have an Office of Internal Audit that is considered sufficiently independent to provide acceptable and credible audit reports to state

and federal agencies about processes and practices of the institution. Such an office can provide audit reports on the compliance of the institution's cybersecurity program with its chosen cybersecurity framework. Partial audits can also be carried out at defined intervals. For example, FedRAMP recommends[2] that ⅓ of all controls are reviewed annually which effectively completes a full audit every 3 years. The resulting attestations from internal or external auditors can enhance contract negotiations with sponsoring agencies and other related parties regarding the institution's ability to safeguard RCD systems and their operation.

Positions to Research Sponsors

To the Federal Government:

1. **Have explicit academic RCD representation on relevant advisory bodies.** Representation will help ensure that considerations related to advanced academic RCD needs will be taken into account in developing and implementing cybersecurity and regulatory compliance guidelines.

2. **Provide Guidance on RCD Cybersecurity and Compliance Topics to Federal Program Officers.** CASC should develop positions that provide guidance to federal program managers to help delineate data classification considerations such as that between open science and CUI.

To the State Government:

1. **Minimize extra regulatory layers.** Adding or mixing additional duplicative or conflicting compliance requirements beyond the often suitably comprehensive governing federal regulations greatly diminishes the ability of research organizations to help your state while adding minimal security benefit.

2. **Customize Requirements Only When Necessary.** Follow federal regulations with any deviations or additions clearly specified in relation to those controls already required in the federal regulation.

Proposed CASC Action Items

- **Establish a CASC Cybersecurity Working Group**
    - The group should review recommended RCD best practices annually and explore topics as input to CASC positions for sharing with external agencies and make periodic reports at CASC meetings or through email communications with members.
    - It is important to rotate membership in this group to promote growth of expertise in our community and to provide opportunities for new perspectives, input, and insights.

Conclusions

In the report above, CASC presents recommendations for actions to be taken by its member institutions and by the organization as a whole to pursue improvements in cybersecurity and compliance issues, based on priorities that emerged from focus group discussions and surveys of the CASC membership. CASC anticipates making further recommendations on top priority areas in the future. In the meantime, implementing the recommendations in this document will produce material benefits to CASC institutions, individual researchers and partners, and the overall program of RCD-related research.

[2] FedRAMP Annual Assessment Guidance, Version 2, Nov 24, 2017, https://www.fedramp.gov/assets/resources/documents/CSP_Annual_Assessment_Guidance.pdf