To: Nathan Ford, President of SITS Sophie Deveraux, General Counsel for SITS

From: Drew Helgerson, tah568

Date: May 4, 2025

Subject: Proposed Course of Action Regarding the PaSCaQL Lab Issues

Dear President Ford and General Counsel Deveraux,

I am writing to provide recommendations for addressing the recent cybersecurity issues in the Pan-Sterling Cybersecurity and Quantum Lab (PaSCaQL) at SITS. The attached memorandum outlines the key issues, the legal and ethical implications, and a proposed course of action to ensure compliance with federal regulations, protect sensitive data, and maintain the reputation of the institution.

I. INTRODUCTION

The Sierra Institute of Technology and Science (SITS) has faced a series of cybersecurity violations, including failure to implement required security protocols, misrepresentation of compliance status, and the exposure of sensitive data through inadequate security measures. This memorandum aims to identify the key issues, analyze the legal and ethical implications, and propose a course of action to address these concerns.

II. QUESTION PRESENTED

Has SITS and its researchers violated federal cybersecurity regulations by failing to implement necessary security measures, misrepresenting compliance status, and allowing insecure access to classified information, leading to potential data breaches and legal consequences?

III. BRIEF ANSWER

Yes, SITS has violated federal cybersecurity regulations by failing to implement a System Security Plan (SSP), inadequate cybersecurity infrastructure, misrepresentation of compliance status, failure to conduct security assessments, and insecure research tools, all of which have exposed sensitive data and compromised national security. Action must be taken to avoid heavy fines or the closure of the facility.

IV. DISCUSSION

1. SITS must immediately develop and implement an SSP to meet federal requirements.

The federal government mandates a certain amount of effort be taken to allow prevent cybersecurity issues and allow court-ruled investigation. Kansas v Frontier Telecommunications Company (789 F.7d 747 (10th Cir. 2021)). This case emphasizes the mechanisms federal law mandates be in place for such fields. SITS currently lacks an SSP,

exposing their systems to vulnerabilities. While developing an SSP is resource-intensive, the cost of non-compliance is higher, including (non-)potential data breaches and legal penalties. SSP implementation is mandatory and essential for safeguarding sensitive information.

2. SITS must upgrade its cybersecurity infrastructure to include antivirus software and secure access controls. Hefty fines will be awarded to those who fail to implement reasonable security. California v SecureSmart Systems (984 F. Supp. 2d 1123 (C.D. Cal. 2024)); FTC v ByteTech Services (982 F. Supp. 2d 257 (D. Vt. 2024)). This case concretizes the consequences for failure to abide by such mandates. PaSCaQL systems lack antivirus software and secure access, increasing vulnerability. While upgrading infrastructure requires resources, the risk of non-compliance is greater. Immediate upgrades are necessary to protect against future cyber threats and avoid a possible negative ruling.

3. SITS must ensure accurate compliance reporting to federal authorities. Serious fines and legal troubles will be due upon those who falsify compliance reports. United States v East Winifred University (No. 5:24-cv-0168, 2024 WL 61323481 (W.D. Okla. Sept. 12, 2024); United States v Guidehouse Solutions and RanchoDelta Systems (No. 1:22-cv-335 (S.D. Nev. Jun. 14, 2022)); Vittori v CustomerEase, Inc. (No. 1:24-cv-552 (Wy. 2024)). These cases highlight the legal consequences of misrepresenting compliance with federal regulations. SITS submitted misleading compliance scores and ignored internal warnings. Misrepresentation may stem from a lack of understanding of regulations, but intent matters. Transparent and accurate compliance reporting is mandatory and must be prioritized.

4. SITS must conduct mandatory security assessments using DoD tools. Failure to comply with mandatory security assessments can result in heavy fines and other legal issues. United States v East Winifred University (No. 5:24-cv-0168, 2024 WL 61323481 (W.D. Okla. Sept. 12, 2024). These cases exemplify the consequences of failing to comply with existing assessment requirements. PaSCaQL has failed to conduct required security assessments, leaving vulnerabilities. Assessments may be resource-intensive, but they are critical for

compliance. Regular and thorough security assessments must be prioritized to identify and mitigate risks.

5. SITS must ensure all research tools and devices meet federal security standards. Failure to properly handle sensitive data can be met with serious fines and legal trouble. United States v Musk (194 S. Ct. 612 (2022)). This case emphasizes the importance of securing tools used for sensitive research and the danger of mishandling sensitive data. Prototypes and devices lacked basic security features. Secure tools may require additional resources, but the cost of non-compliance is higher. Secure all research tools to prevent data exposure.

6. SITS must enhance cybersecurity measures to prevent and mitigate future cyber-attacks. Failure to uphold adequate security measures and blatant disregard can have serious legal consequences. Digital Horizons LLC v PhantomTech Entertainment (759 F. Supp. 3d 874 (N.D. Cal. 2010); United States v Guidehouse Solutions and RanchoDelta Systems (No. 1:22-cv-335 (S.D. Nev. Jun. 14, 2022)). These cases illustrate the courts tendency to weigh the damage done in its verdict. A cyberattack has already exposed classified data, underscoring vulnerabilities. Addressing cyber-threats requires ongoing efforts and resources. Implementing robust cybersecurity measures is essential to prevent future breaches.

V. CONCLUSION

The cybersecurity violations at SITS pose a significant risk to national security and federal compliance. The failure to implement required security measures, misrepresent compliance status, and allow insecure access has exposed sensitive data and compromised trust in SITS's operations. Immediate and decisive action is necessary to address these issues and mitigate further risks.

Key Recommendations include: Develop and implement a comprehensive System Security Plan (SSP) to align with federal requirements, Upgrade cybersecurity infrastructure to include antivirus software, secure access controls, and multi-factor authentication (MFA), Ensure accurate and transparent compliance reporting to federal authorities, Conduct mandatory security assessments using DoD-prescribed tools to identify and address

vulnerabilities, Secure all research tools and devices to meet federal standards and prevent data exposure, Enhance cybersecurity measures to prevent and mitigate cyberattacks. By taking these steps, SITS can restore its compliance posture, avoid penalties, and protect sensitive data. Proactive measures are no longer optional but are vital to preventing future breaches and safeguarding national security. Collaboration between SITS leadership, the Office of General Counsel (OGC), and federal authorities is essential to navigate this complex situation and ensure the continued success of its research programs.

Immediate action is required to address these issues and avoid further legal and financial repercussions.

Respectfully,

Drew Helgerson – tah568