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

From: Drew Helgerson, tah568

Date: May 4, 2025

Proposed Course of Action Regarding the PaSCaQL Lab Issues

## I. CAPTION

The Sierra Institute of Technology and Science (SITS) has been implicated in several cybersecurity violations, including failure to implement required security protocols, misrepresentation of compliance status, and exposure of sensitive data through inadequate security measures. This report outlines the key issues and provides actionable recommendations to address them.

## 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 in order to avoid heavy fines and possible closure.

## IV. FACTS

**1. Failure to Develop and Implement an SSP:** SITS did not develop an SSP, a mandated requirement for handling CUI and classified information, leaving their security posture vulnerable.

**2. Inadequate Cybersecurity Infrastructure:** PaSCaQL systems lack antivirus software, and researchers use unsecured devices, increasing the risk of data breaches.

**3. Misrepresentation of Compliance Status:** SITS submitted misleading compliance scores to secure funding, violating federal regulations and ignoring internal warnings.

**4. Lack of Security Assessments:** Mandatory security assessments using DoD tools were not conducted, leaving vulnerabilities exposed.

**5. Insecure Research Tools:** Prototypes and devices lacked basic security features, such as secure passwords and encryption, posing easy targets for hackers.

**6. Cyberattack by Conflict-Incognito:** A cyberattack exposed classified data, highlighting the consequences of inadequate security measures.

## V. DISCUSSION

Our situation underscores the critical importance of adhering to federal cybersecurity regulations to protect sensitive data, avoid heavy fines and legal action, and maintain national security. The failure to implement necessary security measures, misrepresent compliance status, and allow insecure access has not only exposed sensitive information but also compromised the trust and continuity of SITS’s research programs. This analysis will examine the key issues, using relevant legal cases to provide a framework for analysis.

### Identified Subissues with CRRACC Analysis

1. **Failure to Develop and Implement an SSP**
   * **C (Conclusion):** SITS must immediately develop and implement an SSP to meet federal requirements.
   * **R (Relevant Cases):** Kansas v. Frontier Telecommunications Company (789 F.7d 747 (10th Cir. 2021)).
   * **R (Explanation):** These cases emphasize the mechanisms federal law mandates be in place.
   * **A (Applicable Facts):** SITS lacks an SSP, exposing their systems to vulnerabilities.
   * **C (Counterarguments):** While developing an SSP is resource-intensive, the cost of non-compliance is higher, including (non-)potential data breaches and legal penalties.
   * **C (Resolution):** SSP implementation is mandatory and essential for safeguarding sensitive information.
2. **Inadequate Cybersecurity Infrastructure**
   * **C (Conclusion):** SITS must upgrade its cybersecurity infrastructure to include antivirus software and secure access controls.
   * **R (Relevant Cases):** 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))
   * **R (Explanation):** These cases establish the legal requirements for securing sensitive information, and the consequences for failure.
   * **A (Applicable Facts):** PaSCaQL systems lack antivirus software and secure access, increasing vulnerability.
   * **C (Counterarguments):** Upgrading infrastructure requires resources, but the risk of non-compliance is greater.
   * **C (Resolution):** Immediate upgrades are necessary to protect against cyber threats.
3. **Misrepresentation of Compliance Status**
   * **C (Conclusion):** SITS must ensure accurate compliance reporting to federal authorities.
   * **R (Relevant Cases):** 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)).
   * **R (Explanation):** These cases highlight the legal consequences of misrepresenting compliance with federal regulations.
   * **A (Applicable Facts):** SITS submitted misleading compliance scores and ignored internal warnings.
   * **C (Counterarguments):** Misrepresentation may stem from a lack of understanding of regulations, but intent matters.
   * **C (Resolution):** Transparent and accurate compliance reporting is mandatory and must be prioritized.
4. **Failure to Conduct Security Assessments**
   * **C (Conclusion):** SITS must conduct mandatory security assessments using DoD tools.
   * **R (Relevant Cases):** United States v East Winifred University (No. 5:24-cv-0168, 2024 WL 61323481 (W.D. Okla. Sept. 12, 2024).
   * **R (Explanation):** These cases exemplify the consequences of failing to comply with existing assessment requirements.
   * **A (Applicable Facts):** PaSCaQL failed to conduct required security assessments, leaving vulnerabilities.
   * **C (Counterarguments):** Assessments may be resource-intensive, but they are critical for compliance.
   * **C (Resolution):** Regular and thorough security assessments must be prioritized to identify and mitigate risks.
5. **Insecure Research Tools**
   * **C (Conclusion):** SITS must ensure all research tools and devices meet federal security standards.
   * **R (Relevant Cases):** United States v Musk (194 S. Ct. 612 (2022)).
   * **R (Explanation):** These cases emphasize the importance of securing tools used for sensitive research and the danger of mishandling sensitive data.
   * **A (Applicable Facts):** Prototypes and devices lacked basic security features.
   * **C (Counterarguments):** Secure tools may require additional resources, but the cost of non-compliance is higher.
   * **C (Resolution):** Secure all research tools to prevent data exposure.
6. **Cyberattack by Conflict-Incognito**
   * **C (Conclusion):** SITS must enhance cybersecurity measures to prevent and mitigate cyberattacks.
   * **R (Relevant Cases):** 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)).
   * **R (Explanation):** These cases illustrate the courts tendency to weigh the damage done in its verdict.
   * **A (Applicable Facts):** A cyberattack exposed classified data, underscoring vulnerabilities.
   * **C (Counterarguments):** Addressing cyber threats requires ongoing efforts and resources.
   * **C (Resolution):** Implementing robust cybersecurity measures is essential to prevent future breaches.

## VI. 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:

* 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.