Office of the Provost
UNIVERSITY OF COLORADO **BOULDER**

MEMO

TO: Alastair Norcross, BFA Chair, Professor
Markus Pflaum, BFA At-Large Representative, Professor
Jed Brown, Professor

FROM: Ann Stevens, Provost and Executive Vice Chancellor for Academic Affairs

DATE: October 7, 2025

SUBJECT: Response to BFA Report

I am writing in response to the interim Faculty IT Security Working Group's Preliminary Report. I want to thank the working group for its dedication to academic freedom and its perspective on cybersecurity on our campus. Before I clarify and outline four key areas of action during this interim period, corresponding to the core points raised by the working group, I want to ensure we continue open dialogue around these important issues and commit to future conversations.

Academic Freedom vs. Speculative Risks
Academic freedom is a bedrock principle of this university and as provost I will vigorously defend every faculty member's right to create and disseminate knowledge and seek truth, subject to the standards of their disciplines and the rational methods by which truth is established. We, as faculty, also have responsibilities that are bound to these rights, including upholding the highest standards of evidence and inclusion. The working group's report rightly underscores the importance of academic freedom, and I am mindful of its concerns about corporate providers.

My respectful counterpoint is that we have a shared responsibility to respond to very real current threats to campus security. We also need to meet current and proposed standards required by the federal government so that we can ensure our faculty have the ability to continue to be competitive for federal and private sector research dollars. I have faith that we can do so without putting academic freedom at risk, and many of the hypothetical concerns noted in the report would only come true if we abandoned our core values — and you have my pledge we're not going to do that.

Office of the Provost and Executive Vice Chancellor for Academic Affairs
Regent Administrative Center • 40 UCB • Boulder, Colorado 80309-0040
t 303 492 5537 • vcaa@colorado.edu

My suggested approach, in cooperation with OIT and in dialogue with the BFA, is to further refine a strategy to implement appropriate checks and balances that will protect our university and our data while preserving faculty members' academic freedom. An example of this work is that OIT, working with campus embedded IT Directors, have developed a process for creating exceptions in certain situations tied closely to specific use cases. Another example is OIT's willingness to create a pilot in which a PI/lab work closely with OIT Security to draft and document a concise security plan that is unique to that lab. This would include an inventory of lab systems, data classification of research data, and a section addressing each item in the responsibility matrix (who handles access management, how patching is done, backup procedures, etc.) The process of creating this plan could clarify expectations and responsibilities for the lab and for OIT.

Research Use Cases and Exceptions to Security Controls

The working group report highlights several specific research use cases where our current Secure Computing Standard might impede research. I am aware of these and other examples and know that OIT is committed to working through such cases.

The goal for the Secure Computing Standards is that they will cover most use cases — 85% to 90% of our campus community. The report suggests that obtaining such exceptions has been onerous or unclear. This is constructive feedback that I have already discussed with OIT leadership and they have already begun to streamline and clarify the exception process so that legitimate research needs can be addressed more quickly. Depending on the specific use case, there may be easy-to-apply compensating controls (for example, isolating a machine from the network if it can't encrypt its disk or run certain scanners) and documentation of the decision via OIT's risk acceptance process.

These exceptions cannot be granted lightly — they require strong justification and acceptance of any residual risk by the department and the respective dean or vice chancellor. OIT has recently published clearer guidance on how faculty, working in coordination with their respective embedded IT director, can request such exceptions, with a goal of a determination being made within 10 business days.

Beyond exceptions, I agree with and recognize the report's recommendation for IT personnel who understand specialized research needs and can coordinate and facilitate specific needs and adjustments. As I discussed last month with the subcommittee, this already happens in parts of campus, particularly some of our Institutes. I am in discussions with the leadership of OIT — and soon will bring college leadership into the

discussion — to create some new IT director positions embedded in academic units to provide local, highly specialized IT coordination and knowledge of cybersecurity for unique academic and research needs. These positions will be embedded in their respective school or college and work in close partnership with OIT.

IT Governance and Faculty Involvement

Another critique in the report is that IT security decisions were made without sufficient faculty governance input. Shared governance is a bedrock commitment of CU Boulder, embedded not only in Regent Law and Policy but also in our culture. As required in those policy documents, there is continuing collaboration between faculty and IT staff and leadership. Faculty (including BFA representatives) are already embedded in all the IT governance committees — for example, a computer science faculty member serves on our CyberRisk Governance Committee and the BFA chair on our campus-wide IT Executive Board. While more can always be done, the IT governance framework provides a solid foundation to embed the faculty voice into IT decisions. Specific suggestions in this area should be part of our ongoing conversations.

Rebuilding Trust – A Core Value of OIT and Our Campus

The Working Group's report, and the conversations among faculty this past year, make it clear that trust between faculty and OIT has been frayed. This is deeply concerning to me, and restoring trust is essential.

With this in mind, OIT has committed to provide more information to the campus community regarding the data collected by our current EDR tools (i.e. Microsoft Defender and Crowdstrike Falcon). This will include providing information about the data the EDR tools collect and the protocols governing access and use of that data. On this point, however, we can only address the current state of these matters, and will have to avoid hypothetical scenarios of what could happen if vendor contracts and core values are abandoned.

We should also proceed with some conversations between the BFA chair and members, me, and the Vice Chancellor for IT. As we expand our conversation, I would propose a process driven by smaller group meetings — perhaps brownbag informative lunchtime sessions — and we are open to larger constituent meetings down the road. The key to moving us forward in this conversation, as I noted at the beginning of this letter, is dialogue and conversation.

To close, I believe that we can meet our commitment to academic freedom, protect the university and our faculty from cyber threats, and meet current and upcoming requirements of the federal government and private sector, but we can only do so through honest and respectful conversation and adherence to our principles. How we engage together matters just as much as what we engage upon. I ask the working group members and the BFA at large to remember that OIT leadership and staff have a university-wide mission to both support research and protect the institution from cyber threats. They deserve our respect for their expertise and their long-demonstrated commitment to supporting the work of our faculty, and that respect is sometimes absent from the tone and substance of the interim report. Similarly, our faculty deserve respect and support for their broad range of research and creative work and the technology that facilitates the work. I am confident that we can foster a culture of stronger trust where security is seen not as an imposed burden but as a jointly managed responsibility, and faculty research is supported and celebrated.

Thank you for your engagement on these issues. Please don't hesitate to reach out to me with further ideas or concerns. I look forward to our continued dialogue and to strengthening the partnership between faculty and OIT in service of the university.