Myers & Galiardo, LLP | 52 Duane Street, 7Fl., New York, NY 10007 | 212-986-5900 | www.citylaw.nyc

BY ECF

August 16, 2022

The Honorable Katherine Polk Failla
Unites States District Judge
Southern District of New York
40 Foley Square
New York, NY 10007

Re: United States v. Nickolas Sharp
21 CR 714 (KPF)

Your Honor:

I represent the defendant in the above referenced matter. Pre Trial Services in Portland, Oregon is supervising Mr. Sharp at the request of SDNY.

Mr. Sharp has been collecting unemployment compensation over the last six months in Oregon. As part of his obligations under that state program he is obligated to continually apply for jobs. Mr. Sharp has finally landed a job at Atlassian. He would be employed as a "solutions architect." He will not be coding.

To assure Pre Trial Services that he is in complete compliance with his conditions of bond the defendant advised his Pre Trial Service Officer Mr. Nischik that he would be using the court monitored laptop to "Remote Desktop" to a secured workstation, and that this would meet Pre-Trial Service requirements as they would have a view into the window from the monitored laptop.

As planned/approved, Mr. Sharp was able to "Remote Desktop" to his Atlassian workstation via the monitored Pre-Trial approved laptop. However, the process is error prone. In his discussions with Atlassian IT they will soon be changing the process and begin requiring employees to use a provided (IT secured and monitored) laptops directly/physically.

- To be even more specific, Mr. Sharp is not part of any management team which controls the software servers. His role encompasses architecture, design and planning solutions. Other members of the company implement code. Mr. Sharp has no access to clients. Mr. Sharp will only have "permissions" to develop planning solutions. Atlassian follows the principle of "Least Privilege" and has scoped his role accordingly.

- Secondly, Atlassian workstations have MDM (mobile device management) controls enabled. With these controls Atlassian enforces strict firewall controls and audits the installed software. The controls implement backups and audit logs of all employee actions on the devices. Atlassian IT is the root owner/admin of their devices, and have

full visibility into all actions taken. They can take any and all steps to remotely lock any workstation.

- Atlassian workstations connect via an office VPN, where all "network/internet" traffic is monitored and auditable by Atlassian IT.

- Any deviation from Atlassian IT standards on their workstations results in the automated "cutting off" of the workstation from their systems. Until the device is brought back into standards (controlled and automated by IT) it cannot connect to company systems. Employees do not have full permissions to change system settings, and cannot remove these controls.

- Atlassian controls and can monitor/audit the installed/running applications, programs, and software on their workstations.

- We request that Mr. Sharp be approved to utilize the Atlassian/Employer provided workstation directly, without the third party monitoring. His actions will still be controlled, regulated, secured, and audited by Atlassian.

We respectfully ask the Court to permit Mr. Sharp to be gainfully employed at Atlassian during the pendency of our case. To help alleviate the tremendous financial burden placed on his family this issue is of utmost importance.

Respectfully,
/s/Matthew D. Myers
Attorney at Law

Cc: AUSA Vladislav Vainberg