DEPARTMENT OF THE ARMY
OFFICE OF THE GENERAL COUNSEL
104 ARMY PENTAGON
WASHINGTON, DC 20310-0104

February 28, 2022

Ms. Tracy Biggs
Deputy Chief, Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, N.W. Suite 300
Washington, D.C. 20310-0101

Dear Ms. Biggs:

This letter responds to your office's request for additional information for Whistleblower Investigation Concerning Office of Special Counsel Referral DI-17-2168, Department of the Army, 1st Personnel Command, Washington-Moscow Direct Communications Link, Detrick Earth Station, Fort Detrick, Maryland. In an email dated October 22, 2021, the Office of Special Counsel (OSC) requested that the Army provide additional information regarding allegations of wrongdoing in the above OSC case. Specifically, OSC requested the Army provide responses to five additional issues. OSC's specific request for information (RFIs), are listed immediately below and the information provided by the command is addressed in subsequent paragraphs:

a. In the supplemental report dated March 21, 2021, the Army reverses its initial determination on Allegation 4 regarding security and operational deficiencies resulting from the lack of a fire suppression system and 24/7 personnel presence. Allegation No. 3, also involving security and operational deficiencies, is related to Allegation 4. Given that allegation No. 4 is now substantiated, has the Army reconsidered its finding that allegation No. 3 is not substantiated? If not, why not?

b. The reconfiguration of the Detrick Earth Station (DES) involved moving computers connected to the Russian Federation to the Gateway Telecommunications Center (GTC). How has the Army addressed security concerns related to the presence of those computers in a Secret-level facility that supports military communications?

c. Has the Information Assurance Plan (IAP) documenting the lack of fire suppression system been completed? If not, why not. If yes, has the facility received guidance on how to come up to code and comply with NIST 800-53 security control PE-13(4) and have inspections been completed?

d. Please provide an update on the status of the DCL CCB Charter.

e. Please provide an updated on the status of the RMF package; the IAP review, including any acceptance of remote operations; and the Strategic Vulnerability Assessment (SVA).

RFI paragraph a. Allegations 3 and 4 are best viewed as mutually exclusive issues. Allegation 3 is not just "security and operational deficiencies," it's "security and operational

deficiencies attributable to remote operations." In initially finding Allegation 4 unsubstantiated, the IO focused on the remote nature of the facility's operation in her analysis and did not focus on the fire suppression issue. While the complainant conflates these two allegations, the allegations need not be conflated and the IO does not conflate them. Further, it is worth noting that one related instance highlighted by the complainant involving these issues did not take into account particular aspects of the DES. Specifically, the complainant notes being in the DES during a power outage and contends that, but for the good fortune of his presence, others would not have been able to access the building. This is inaccurate. The building contained non-critical and assured power sources. The non-critical power failed, which powered the turnstile, but the assured power stayed on, meaning the mission never failed. Even without the turnstile access, there are two padlocked entrances to the DES compound, assuring access even if there is a loss of power. Finally, even assuming these allegations are connected, the technical/operational mission equipment of the DCL no longer resides in the DES. In other words, the concerns connected to Allegations 3 and 4 have been eliminated by the system modernization and relocation of the equipment.

RFI paragraph b. The presence of computers connected to the Russian Federation within the GTC were installed in accordance with the (U) Committee on National Security Systems Advisory Memorandum (CNSSAM) TEMPEST/01-13, RED/BLACK Installation Guidance. Specifically, that guidance explains how to install and operate multiple systems that handle national security information and non-national security information in the same facility. The RED/BLACK installation guidance is routinely used in US Government facilities that host NIPR, SIPR, JWICS, and various other communication systems that are connected to foreign nations.

RFI paragraph c. The IAP status is connected to the RMF process discussed in Para. 7 below. With respect to the DCL, the modernized equipment is now housed in the GTC building, which is compliant with the fire suppression system requirement.

RFI paragraph d. The DCL governing structure, including roles and responsibilities, is currently under review by DoD CIO and The White House Situation Room. The DCL stakeholder community continues to meet monthly.

RFI paragraph e. The NSA completed SVA with no major findings. A full Red/Blue team assessment will be completed when the modernized system is ninety percent complete and prior to full operational capability. The SVA cannot be used to issue an Authority to Operate (ATO). DISA RME has requested the U.S. Army Information Systems Engineering Command (ISEC) complete the RMF documentation and ATO process prior to DISA accepting responsibility of the modernized DCL system. The ISEC documentation and response is pending.

The Agency's point of contact is the undersigned via email at Michael.r.black.civ@army.mil

Michael Black
Attorney Advisor