DEFENSE DIGITAL SERVICE
9010 DEFENSE PENTAGON, ROOM 3A268
WASHINGTON, D.C. 20301-1600

October 27, 2020

MEMORANDUM FOR DEFENSE DIGITAL SERVICE (DDS)

Subject: Policy on Use of Communication Applications - *Signal*

References: (a) DoD Dir. 5105.87, "Director, Defense Digital Service," Jan. 5, 2017, Change 1, December 4, 2019
(b) DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," Jan. 2, 2019

In a world where the bad guys are always listening, an organization like ours needs secure communication. However, as public servants we are required to balance our mission's need for security with the public's right to access records of our work. The result is that DDS is required to work in a space far more constrained than the general public. Operating in this constrained spaces, DDS must still ". . . continue to innovate via electronic messaging services to achieve capabilities that are faster, better and less expensive, while simultaneously ensuring implementation of cybersecurity appropriate for the risks, and the magnitude of harm that could result from the loss, compromise, or corruption of the information." Reference (b).

The practical impact of this restriction shows up in the use of the communication application, *Signal*. The developers envisioned strong encryption paired with automatic deletion of content in order to provide secure messaging – and they succeeded. The consequence of this success with the addition of voice calls in 2017, has made Signal a preferred method for hosting secure communications.

Of course, the downside is that *Signal* does not require messages to be stored, and allows the user to set up auto-deletion for specified periods ranging from 5 seconds to 7 days. As a result, DDS cannot track this activity – or comply with FREEDOM OF INFORMATION ACT (FOIA) requests for files. 5 USC § 552, *et seq*. Yet, unless someone officially records them, voice communications – ordinary calls over ordinary providers using ordinary encryption – are too ephemeral to capture and too impractical to store. So, at present FOIA does not require agencies to record phone calls.

That, of course, is the problem. There is nothing illegal in using *Signal* and it does not violate FOIA inherently, but because *Signal* is not readily FOIA-compliant, it can look like a government employee is avoiding FOIA if the employee uses Signal. To

avoid this appearance and to ensure we comply with FOIA, I am setting out DDS' policy on the use of *Signal* here:

- You may continue to use *Signal* for routine voice communications;
- You may not transfer any files, without my prior approval;
- You may not conduct any classified discussions;
- You may not send written messages conducting official business; and
- You should, when reasonably possibly, use Signal's "verify" function with contacts to further secure your communications

To clarify, official business means any work directly or indirectly related to DDS projects or the authorized duties performed by an employee of DDS. Admittedly, this is a broad category, so the best practice is to stay out of *Signal* for any activity beyond simple voice communications or perfunctory messages. If you have questions or suggestions, let me or the legal team know and we will get you clarification.

BRETT GOLDSTEIN
Director
Defense Digital Service