

Kel McClanahan, Executive Director
National Security Counselors¹
Testimony Before the House of Representatives
Financial Services and General Government Appropriations Subcommittee
27 March 2019

Chairman Quigley, Ranking Member Graves, and members of the Financial Services and General Government Appropriations subcommittee, thank you for the opportunity to speak with you today.

I come before you today to discuss two separate areas where we believe that Congressional action is needed to address subtle issues which nonetheless have significant deleterious effects for transparency and accountability. The first subject pertains to agencies' expansive use of secret filings in Freedom of Information Act ("FOIA") cases and the resulting inability of journalists, academics, and members of the public to access these court filings years or even decades later. The second subject pertains to the problems posed when agency Inspectors General rely on the information technology and information access resources of the agencies they oversee.

In Camera FOIA Declarations

FOIA cases are somewhat unique in civil litigation, due to the fact that the agency being sued must demonstrate through admissible evidence that information must be withheld from disclosure without disclosing the information in question. Agencies generally do so by submitting sworn declarations from FOIA officers which "must prove that each document that falls within the class requested either has been produced, is unidentifiable, or is wholly exempt from the Act's inspection requirements."² These declarations "must be 'relatively detailed' and nonconclusory,"³ but "would not have to contain factual descriptions that if made public would compromise the secret nature of the information."⁴ In some cases, an agency will assert that it cannot meet its burden on the public record, and in such cases it generally attempts to file a declaration *in camera* and *ex parte* so that only the judge—and not the plaintiff or their attorney—sees it. This mechanism is an imperfect compromise at best, but it is increasingly overused and abused by agencies with the passive acquiescence of judges, who cite the presumption of good faith that they must afford to agency declarations and virtually never refuse to accept such filings.

It is not unheard of for a judge to grant summary judgment to an agency solely on the basis of an *in camera* declaration, in which the agency kept from public view not only the facts which would support its case but even the legal arguments. In such cases, the actual legal brief for the agency's motion includes little more than boilerplate language about the burden of proof and the proper conduct of FOIA litigation, and then refers the judge to the *in camera* declaration for all the relevant analysis. In one such case, the judge found not only that the

¹ Joined by the Government Accountability Project and the Project on Government Oversight.

² *Nat'l Cable Television Ass'n. v. FCC*, 479 F.2d 183, 186 (D.C. Cir. 1973).

³ *Goland v. CIA*, 607 F.2d 339, 350 (D.C. Cir. 1978).

⁴ *Vaughn v. Rosen*, 484 F.2d 820, 826-27 (D.C. Cir. 1973).

declaration filed *in camera* by the Federal Bureau of Investigation (“FBI”) was proper, but that **the plaintiff did not even deserve a chance to file an opposition brief because “the evidence presented *in camera* was so conclusive as to the questions presented that further briefing and argument was clearly unnecessary.”**⁵ Bizarrely, that same judge had the following to say about this purportedly incontrovertible proof:

Nonetheless, the court must state that **Hardy’s unredacted declaration is the quintessence of bureaucratic obfuscation.** While attempting to decipher its meaning, I recalled one of Orwell’s observations when confronted with such writing:

As soon as certain topics are raised, the concrete melts into the abstract and no one seems able to think of turns of speech that are not hackneyed: prose consists less and less of words chosen for the sake of their meaning, and more and more of phrases tacked together like the sections of a prefabricated henhouse.

George Orwell, “Politics and the English Language,” *in A Collection of Essays* 162, 165 (Anchor Books 1954). Which begs the question, why did the government resort to hackwork here? Orwell again:

The inflated style is itself a kind of euphemism. A mass of Latin words falls upon the facts like soft snow, blurring the outlines and covering up all the details. The great enemy of clear language is insincerity. **When there is a gap between one’s real and one’s declared aims, [the writer] turns, as it were, instinctively to long words and exhausted idioms, like a cuttlefish squirting out ink.**⁶

My research has determined that the number of such filings has shown a slow increase over time, from approximately 15 instances in 1994 to the high-water mark of approximately 56 in 2017.⁷ **I was only able to identify three instances of a judge denying an agency’s request to file an *in camera* declaration since 1993.** My personal litigation experience has suggested an increase in the expansiveness of agencies’ claims that information must remain secret. **I have in fact received redacted versions of such declarations through FOIA or similar means that the agency insisted could not be filed on the public record.** Some of the newly released information has been mundane, and some has been of significant historical importance. For example, in the landmark FOIA case *Weberman v. NSA*, the National Security Agency (“NSA”) argued that it could neither confirm nor deny the existence of records about a telegram that Jack Ruby was alleged to have sent to Havana the year before the assassination of President Kennedy.⁸ The district court and the 2nd Circuit granted summary judgment to NSA on the basis of an *in camera* classified declaration, and it was not publicly revealed whether NSA had

⁵ *Truthout v. DOJ*, 20 F. Supp. 3d 760, 770 (E.D. Cal. 2014).

⁶ *Id.* at 768-69.

⁷ This research was performed by searching court dockets from 1993-2018 for the term “in camera” and then parsing out the appropriate entries. These dockets were provided by the Transactional Records Access Clearinghouse’s FOIA Project. The degree to which these dockets accurately reflect court filings during this time period cannot be ascertained at this time, and so these figures may not represent the totality of the practice. Detailed information about this analysis and my bases for making any other claim in this testimony is available upon request.

⁸ 668 F.2d 676, 677 (2d Cir. 1982).

intercepted such a telegram. However, in 2011, I obtained a redacted version of the classified declaration from NSA, which revealed for the first time that NSA had not intercepted the alleged telegram because it had lacked the technical capacity at the time.⁹ **This was historically important information which would never have seen the light of day but for my efforts.**

It is for these reasons that I bring this issue to the Subcommittee's attention. It is arguably beyond the jurisdiction of this subcommittee, or even of the Appropriations Committee as a whole, to make a significant change to the way in which *in camera* declarations are handled in FOIA cases, but such an effort should not be undertaken without hard data. It will be important for legislators to understand how prevalent this practice truly is and under what circumstances these filings are made by agencies and accepted by courts. To this end, **I ask that the Subcommittee appropriate sufficient funds to the Administrative Office for U.S. Courts to conduct a comprehensive survey of all *in camera* agency declarations filed in FOIA cases within the past 10 years (or another reasonable time period)**, specifically for the purpose of: 1) identifying with certainty the number of such filings; 2) identifying any geographic or temporal trends; 3) specifying whether the agency sought leave for the filings or simply filed them without asking; 4) indicating the depth of the court's discussion of the appropriateness of the *in camera* filings; 5) indicating the nature of the claims being supported by the *in camera* filings; and 6) providing any other relevant data.

I also ask the Subcommittee to appropriate sufficient funds to the Administrative Office to perform a feasibility study for a process in which all agency declarations filed *in camera* in FOIA cases would automatically be filed on the public record after 5 years (or another reasonable time period). This study would allow Congress to intelligently decide whether it would be appropriate to legislate such a proposal, so that these important court records would ultimately become accessible to journalists, academics, and the general public without relying on individual persons to pursue their release as I did. **If any type of sealed court filings should be presumptively open after a period of time, it would most assuredly be filings made in litigation over government transparency.**

Practical Independence of Inspectors General

Offices of agency Inspectors General are designed to be legally unique entities within the government because their purpose is to conduct audits and investigations of agency operations.¹⁰ However, even though these offices retain *legal* independence from the agencies they oversee, in many cases they are still *practically* compromised. This problem primarily arises in the context of information technology and information access.

When an Inspector General's office relies upon the agency's IT infrastructure, it creates vulnerabilities and conflicts of interest. For example, one need only consider the case of Daniel Meyer, formerly the Director of Whistleblowing and Source Protection for the Intelligence Community Inspector General ("ICIG"). Mr. Meyer exchanged emails about confidential whistleblower disclosures with Senator Grassley's office, and the Central

⁹ I obtained this record by filing a Mandatory Declassification Review ("MDR") request with the NSA pursuant to Executive Order 13,526. MDR is a different mechanism than FOIA which is limited to classified documents.

¹⁰ Inspector General Act of 1978, Pub. L. No. 95-452 (Oct. 12, 1978), 5 U.S.C. app. 3.

Intelligence Agency (“CIA”) intercepted and reviewed those emails, allegedly for security reasons.¹¹ **CIA was able to do this because the ICIG, even though it is housed in the Office of the Director of National Intelligence and exercises oversight over the entire Intelligence Community, uses CIA email servers.** ICIG employees have email accounts on the ucia.gov domain (the domain used by CIA employees), and as a result CIA claims the right to review any information stored therein, arguing that the fact that the information is stored on a CIA computer brings it within the scope of CIA’s counterintelligence mission. As a result, an operational office of CIA is given virtually unlimited access to the confidential whistleblower files of the Inspector General charged with its oversight. Moreover, there appear to be little restrictions on CIA’s use of this information; Mr. Meyer’s emails were then given to the CIA OIG, which itself falls under the ICIG’s oversight jurisdiction.

This arrangement stands in stark contrast to the relationship between the Department of Homeland Security and its Inspector General. In that case, the DHS OIG possesses its own dedicated IT staff and has established numerous firewalls and protocols to ensure that its files cannot be accessed by non-OIG staff. The General Services Administration (“GSA”) OIG has a separate domain of its own: gsaig.gov. However, it is currently unknown whether DHS and GSA represent the norm, or whether CIA does.

A similar issue can be seen with respect to the control of access to information. For example, **it creates an unavoidable conflict of interest for an agency’s security office to make adjudications about security clearances or other access to information restrictions (e.g., public trust suitability determinations) about employees who might be in a position to investigate the security office.** While a total duplication of effort would likely be wasteful, it is reasonable to expect a truly independent Inspector General’s office to have its own personnel security staff to handle its own personnel security issues such as access determinations, to avoid this conflict. Such a dedicated staff could share resources and coordinate with the agency’s security office, but decisions about what access to grant to OIG employees would need to be made by OIG security staff, just as Inspectors General are required by law to obtain and maintain legal counsel separate from agency counsel.

Because the extent of these problematic relationships is currently unknown, **I ask the Subcommittee to appropriate sufficient funds to allow the Council of the Inspectors General on Integrity and Efficiency (“CIGIE”) to conduct a comprehensive survey of all Inspectors General to determine the extent to which their offices are entangled with the agencies they oversee in an IT and information access context. In recognition of the tension between CIGIE and several agency Inspectors General, I also ask the Subcommittee to prohibit the use of appropriated funds by any agency to obstruct or refuse to cooperate with this survey.**

¹¹ Charles Clark, *Grassley Wins Declassification of CIA Documents on Monitoring Whistleblowers*, Gov’t Exec. (Nov. 2, 2018), at <https://www.govexec.com/oversight/2018/11/grassley-wins-declassification-cia-documents-monitoring-whistleblowers/152546/>.

Kel McClanahan Biography

Kel McClanahan is the Executive Director of National Security Counselors, a Washington-area non-profit public interest law firm which specializes in national security law and information and privacy law. Before chartering National Security Counselors with his fellow directors, he served as Director of FOIA Operations for the James Madison Project and Of Counsel to the Law Office of Mark S. Zaid, PC. He is an adjunct professor at the George Washington University Law School and the American University Washington College of Law, where he teaches various topics in national security law. He sits on the Board of Directors of the National Military Intelligence Foundation, the Board of Directors of the Bar Association of the District of Columbia, and the Steering Committee of the BADC Committee on National Security Law, Policy, and Practice, and is a charter member of the Security Clearance Lawyers Association.

He received his Master of Arts cum laude in Security Studies from the Georgetown University Edmund A. Walsh School of Foreign Service, his Juris Doctorate from the American University Washington College of Law, and his Master of Laws in National Security Law from the Georgetown University Law Center.

He belongs to the bars of New York, the District of Columbia, the U.S. Supreme Court, and several other federal courts.