

Why is Mattis Declaring War on Whistleblowers?

Patrick Eddington

August 3, 2017

Is Secretary of Defense James Mattis creating a hostile workplace for Defense Department whistleblowers? Or is he simply carrying on an anti-whistleblower organizational tradition at the Pentagon that stretches back decades? An examination of recent events and the historical record suggests it's both, and the implications for taxpayers and American national security are stark.

As the Project on Government Oversight first reported in December 2016, a three-member interagency Inspector General External Review Panel concluded in May 2016 that the then-Inspector General of the National Security Agency (NSA), George Ellard, had, according to POGO, "himself had previously retaliated against an NSA whistleblower[.]" This apparently occurred during the very same period that Ellard had claimed that "Snowden could have come to me." The panel that reviewed Ellard's case recommended he be fired, a decision affirmed by NSA Director Mike Rogers.

But there was a catch: the Secretary of Defense had the final word on Ellard's fate. Outgoing Obama administration Defense Secretary Ash Carter, apparently indifferent to the magnitude of the Ellard case, left office without making a decision.

In the months after Donald Trump became president, rumors swirled inside Washington that Ellard had, in fact, escaped termination. One source, who requested anonymity, reported that Ellard had been seen recently on the NSA campus at Ft. Meade, Maryland. That report, it turns out, was accurate.

On July 21, in response to the author's inquiry, the Pentagon public affairs office provided the following statement:

"NSA followed the appropriate procedures following a whistleblower retaliation claim against former NSA Inspector General George Ellard. Following thorough adjudication procedures, Mr. Ellard continues to be employed by NSA."

The Pentagon offered no explanation as to why Mattis chose to overrule the IG External Review Panel and NSA's current director, but the message is abundantly clear: If you work in Pentagon management and retaliate against a whistleblower, there's a good chance you'll keep your job. And if you are a prospective whistleblower, the message is equally clear: You blow the whistle at your own risk.

Unfortunately, the Ellard case is not unique within the Pentagon. And as a series of these cases demonstrate, when the internal watchdog function breaks down at the Defense Department, not only are taxpayers ripped off, but intelligence failures costing the lives of thousands of Americans can result.

Thanks to help from the law firm of Loevy & Loevy, as well as the Government Accountability Project, an ongoing lawsuit I filed earlier this year is shedding new and disturbing light on these problems at NSA and elsewhere in the national security establishment. The events that eventually motivated the lawsuit are straightforward.

In the late 1990s, a small team of NSA employees—Bill Binney, Kirk Wiebe, Ed Loomis, and senior manager Tom Drake—came up with a revolutionary digital intelligence collection and analytical system called THINTHREAD. The system would've allowed NSA to, in real time, sift through the trillions of digital communications passing over the airwaves and the internet, find any bad actors in communication with Americans, segregate and encrypt that traffic for further analysis (and where necessary additional collection or legal action), and discard the remaining digital junk.

The system was cheap—the prototype cost around \$3 million, made possible by then-GOP House Intelligence Committee staffer Diane Roark—and could be deployed NSA-wide quickly. Preliminary testing showed that THINTHREAD was developing actionable intelligence not discovered by any other NSA systems.

The THINTHREAD team was convinced that their system could spot threats far enough in advance to allow the United States to thwart attacks at home or abroad. There was just one huge problem: then-NSA Director Michael Hayden vehemently opposed the system.

Hayden preferred to go with a completely unproven, outsourced, contractor-produced and run system called TRAILBLAZER, spearheaded by defense contractor behemoth SAIC. But throughout its existence, TRAILBLAZER was plagued by repeated delays and huge cost overruns, producing zero actionable intelligence. The internal battle over the programs led Hayden to retaliate against the THINTHREAD team for briefing Roark and other House Intelligence Committee staffers on their success, even as TRAILBLAZER foundered.

Hayden's subordinate, Maureen Baginski, officially killed THINTHREAD development just three weeks before the 9/11 attacks. By the end of October 2001, the original THINTHREAD development team had left NSA, motivated to leave upon learning that key THINTHREAD technologies—minus the Constitutional safeguards built into it—was being misused to conduct warrantless mass surveillance against the American people.

Furious at TRAILBLAZER'S waste of taxpayer money and Hayden's refusal to field THINTHREAD—which the developers believed could have prevented the 9/11 attacks—in September 2002 Binney, Wiebe, Loomis, and Roark filed a whistleblower complaint with the Pentagon Inspector General (DoD IG). Drake remained at NSA to support the complaint, providing IG investigators with key documents and reports showing clear malfeasance by senior NSA officials.

And according to Drake, as revealed in the new documentary on this episode, “A Good American,” post-9/11 application of the existing THINTHREAD system against NSA databases not only discovered evidence of Al Qaeda’s attack plans that other NSA systems and analysts had missed, but other parts of the plot that had been attempted but failed. The implication was clear: THINTHREAD could’ve prevented the September 11 attacks on America. Drake said NSA management ordered that study to be buried.

Indeed, being right and raising a stink over the lethal intelligence failure backfired on Drake and his former colleagues.

On July 26, 2007, the FBI raided the homes of the former THINTHREAD team members, along with that of Diane Roark. All were alleged to be suspects in an ongoing leak investigation that had exposed the largest acquisition and intelligence failure in the history of NSA. But the allegations that led to those FBI raids were bogus, as subsequent legal proceedings would demonstrate over the next several years.

Drake initially faced multiple charges under the draconian Espionage Act, but as the illegitimate nature of the case became clear, all those charges were dropped. Drake, in an effort to end the case and avoid total poverty, pled to a single count of misuse of a government computer. But none of the NSA managers or SAIC contractors responsible for the TRAILBLAZER fiasco, or those responsible for Drake’s vindictive and bogus prosecution, were ever charged with a crime.

While working as a House staffer for then-Rep. Rush Holt (D-NJ) in 2013, I had the chance to review that classified IG report and became determined to get it out. It completely validated all the core allegations of the THINTHREAD team and Roark. In my view, NSA was misusing the classification system, especially an obscure 1959 law, to prevent the public from learning the truth about the episode.

This past week, the Pentagon provided to me a less redacted version of the report that was originally released in 2011. While well over half of the report given to me remains redacted (and the subject of ongoing litigation), enough of it has been released to show beyond all doubt that the IG validated the whistleblowers allegations—and that fear of NSA management retaliation for exposing the fraud was pervasive among the many NSA employees interviewed by the DoD IG.

The report found that THINTHREAD, “a less costly and more capable solution” than TRAILBLAZER “was already operationally available and ready for deployment. As a result, the National Security Agency is inefficiently using resources to develop a digital network exploitation system that is not capable of fully exploiting the digital network intelligence available to analysts from the Global Information Network” (p. ii).

The IG report also noted that Hayden had ignored multiple internal reviews that showed THINTHREAD superior to his moribund TRAILBLAZER, and that he delayed deployment of THINTHREAD to multiple NSA collection sites, in violation of Congressional direction to do so (p. 4). Hayden’s mismanagement of NSA and insubordination with Congress cost taxpayers hundreds of millions of dollars and arguably the lives of nearly 3,000 Americans on 9/11.

Sadly, the misconduct of Pentagon officials didn't end with the publication of that DoD IG report over a decade ago.

After his trial was over, Drake filed a whistleblower reprisal complaint with the Office of Special Counsel (OSC), the federal watchdog responsible for investigating whistleblower reprisal cases. In 2016, OSC concluded that DoD IG officials engaged in evidence destruction during Drake's trial, and referred the matter to the DoJ IG for action. Drake confirmed to the author in June 2017 that DoJ IG investigators had interviewed him last summer but that he's heard nothing since.

As the foregoing post-9/11 history of the Pentagon demonstrates, Ellard's misconduct is just the latest example of the culture of corruption at NSA that Ellard's nominated replacement, Robert Storch, will have to end if NSA employees are to believe that fraud or criminal complaints can be reported without fear of retaliation.

At Storch's all-too-brief confirmation hearing last week before the Senate Intelligence Committee, he was not asked about the status of Drake's case or the misconduct of his predecessor—amazing omissions by one of NSA's chief Congressional oversight bodies. Unless Congress invests the time to thoroughly investigate, in open session, these past episodes of whistleblower retaliation and programmatic misconduct, we risk still more of the same—more taxpayer money squandered, and more Americans needlessly killed in avoidable intelligence failures.

Patrick G. Eddington is a policy analyst in homeland security and civil liberties at the Cato Institute.