

Sent Time: 2016-11-10 09:12:03 GMT-05:00(Eastern Standard Time)
From: Joshua Schulte <schuljo@cia.ic.gov>
To: Report-Fraud Mailbox [REDACTED]
Subject: Report to House Intelligence Committee
Attachments: 'smime.p7s'



Classification: UNCLASSIFIED

OIG,

As my last day at the Agency, I wanted to inform OIG that I have reached out and been in contact with representatives from the House Intelligence Committee. They said someone from their office would be coordinating with you to look into my report. I firmly believe that my treatment after reporting security issues and the Agency's ideology of "promoting people out of the problem" and "ignore the problem until it goes away" is unsatisfactory. The CIA has a real problem with its management that stems from the corrupt culture in middle management and extreme lack of character from SIS officers. This appalling and illegal behavior should be and will be investigated directly by congress.

I am resigning from the CIA because of deep injustices and illegal behavior by multiple SIS officers. They ignored the issues I raised about security concerns and attempted to conceal these practices from senior leadership. They retaliated against me when I contacted security, they lied and mishandled classified to up-classify documents that could be used as evidence against them, and they directly targeted me to destroy my agency career and prevent me from promotion. Every security report was met with disdain as SIS officers employed the "ignore the problem until it goes away" technique.

Specifically, Karen [REDACTED] ignored my complaints that our development network and product solution were incredibly vulnerable. Since the inception of our Atlassian product replacement of TeamForge, I have acted as a de-facto system administrator for the network despite no official job title or training because the contractors hired to do this job were incompetent. They could not handle the position, so myself and others had to take it upon ourselves to manage these complex systems. I first reported this issue when the main person supporting this system went overseas to

Foreign Office
West

and left me in charge simply because I had previous system administrator experience. However, there was no official hand-off, no official exchange, and no official training because we were not even supposed to be managing this infrastructure. For two full years I reported through my management chain these security concerns. I continued to help maintain the infrastructure out of need of it since those responsible for it would not and could not maintain it themselves. In fact, it was so bad that whenever people would go to the infrastructure team for assistance, they would simply route them to us! We were still mainly developers, so we largely just relied on trust. This left it open and easy for anyone to gain access and delete our entire EDG source code repository or even easily download and upload it in its entirety to the internet through the FIN network since both were unmanaged and gave developers full administrator privileges and ability to use removable media. Luckily, nothing happened, but it still illustrates the lack-of-security and pure ineptitude of Karen. Not only was she aware of the issue, but she did nothing to transition to the contractors charged by the government to support it. Karen [REDACTED] is as incapable and

incompetent a manager as she is a leader. She exhibits all the qualities of SIS middle management—A pure politician with zero leadership and management qualities, but the ability and capacity to stab anyone in the back to get ahead. She clearly didn't care about anything but moving up in the ranks and promotion to senior leadership. Once this failure of leadership was discovered, she would later attempt to evade responsibility and blame the decentralized and insecure environment entirely on me.

Her poor leadership and management began with my branch chief's poor management. In October of 2015, I reported to my manager, Sean [REDACTED], of the horrific actions of Amol [REDACTED]. His incessant harassment and threats were appalling, however, my management did nothing to help the situation. Then, in March of 2016, Amol [REDACTED] threatened to kill me so I directly called security.

I was told by Sean [REDACTED] that Karen [REDACTED] was furious with my report because I jumped my chain of command and it made her look bad to the front office. Never once did Karen reach out to me or attempt to assist me during this situation. In fact, my management literally did NOTHING after security spoke with them. They informed security that it wasn't a real threat, and continued to force me to sit next to the individual who threatened me. Yes, that's right—I was forced to continue to work next to an individual who threatened to kill me. Sean [REDACTED], who was not even in the office on the day of the incident, directly told security that it did not happen and there was no issue. So, with no options left, I went to the courts to request a protective order. Once again, this infuriated my management and security. Colleagues told me that the correct response was never to involve security. They told me that security always makes it your problem, and in the end all security reports hinder your career. The fact that this notion about security exists at the CIA is astonishing...

On the defensive, Karen realizes the extra scrutiny will reveal all the issues with the security of EDG's systems, so she attempts to pin it on me and issues me a "Memo of Warning" after I was simply doing the administrator job to maintain our system. Her argument was I was not expressly given permission, and since her faithful pawn Jeremy Weber [REDACTED] had removed my accesses of specific projects without telling me, as soon as I accessed those projects then I was hit with this memo of warning. Up to this point, Karen has still never talked to me directly or communicated in any way since the Amol incident. Instead, she sent the division chief, Anthony Leonis [REDACTED], to issue me the warning. When I request specifics in writing, it is denied. I write emails requesting written clarification and I'm told that both Karen [REDACTED] and Bonnie [REDACTED] will not respond in writing. Yes, that's correct—to evade government accountability and records keeping, these SIS officers specifically state that nothing will be in writing.

So, at this point, with no end in sight and continued abuse of the system, I reach out to lawyers. Since I am required to fill out Outside Activities requests, the Agency is promptly notified. Only at this point is anything done. Immediate backlash begins as SIB begins investigating my Outside Activities request. I am reprimanded for taking pure unclassified out of Agency space for my protective order court case, and I am told that the agency doesn't care or support my case so I am not authorized to take any documentation from the building. SIB then picks up on a random fight that I was allegedly involved in that has nothing to do with anything, and begins questioning me and attempting to discredit my security reports due to this fight. I am then told by DC/CCI John [REDACTED]

that my complaint against Amol [REDACTED] is laughable and “doesn’t even come close to real harassment”. He tells me I should resign.

Karen [REDACTED] then issues a Letter of Warning following another attempt by me to do my job. Despite the overwhelming proof I present that completely nullifies this charge, she issues the Letter anyway. This is the first time Karen meets with me following the Amol incident. It shows her true leadership—she never even meets with me, talks to me, or even email me regarding the security incident(s). She then takes the very reports I sent her regarding my security concerns and spins them to blame me and cover herself. At every corner, this SIS officer evades responsibility and blames others.

CIA management has a very toxic culture. Managers cover themselves and point blame elsewhere anytime something happens. Their issue resolution is to ignore the problem until it goes away. If the issue persists, instead of face it directly they opt to attack the individual(s) rocking the boat. In direct retaliation to me, my management illegally mishandled classified in an attempt to cover themselves. They up-classify UNCLASSIFIED emails so that issues involving themselves will never be brought to the court system. There are several instances, where, once management actually DID reply to me in writing, they would always classify emails that did not contain any classified information to CYA. Management also attacked and fought me through any and all daily processes. Specifically, Anthony Leonis [REDACTED] issued sweeping HR policy changes that limited the amount of S/L that I could take, and even went so far as to commit timecard fraud and modify my timecard to replace S/L with A/L without my consent. I went to main HR and complained about this, but the issue was never resolved. Sean retaliated against me by rating me very poorly in my PAR. When I complained to him and reminded him it was illegal to retaliate against an employee, he then changed my PAR with a higher rating. I then reached out to HR and EEO to complain that my PAR process could not be fair if my manager was directly attempting to hinder my career. I feared that I would not receive a fair promotion consideration, and then would not be promoted. No one cared or responded, and as I feared, I was passed over for promotion. Despite my direct contributions to the mission including many intelligence reports and an EPA, I was passed over for promotion. Even though I had been in my position slightly longer than the average time for promotion and contributed to far greater success than most of the individuals promoted, I was considered in the bottom 50% of my grade and was not promoted.

=====
Classification: UNCLASSIFIED

.....