MAYBE NSA "MOONLIGHTING" IS ANOTHER NAME FOR "PUBLIC-PRIVATE PARTNERSHIP"?

As you've likely read, NSA's Chief Technology Officer has so little to keep him busy he's also planning on working 20 hours a week for Keith Alexander's new boondoggle.

> Under the arrangement, which was confirmed by Alexander and current intelligence officials, NSA's Chief Technical Officer, Patrick Dowd, is allowed to work up to 20 hours a week at IronNet Cybersecurity Inc, the private firm led by Alexander, a retired Army general and his former boss.
>
> The arrangement was approved by top NSA managers, current and former officials said. It does not appear to break any laws and it could not be determined whether Dowd has actually begun working for Alexander, who retired from the NSA in March.

Dowd is the guy with whom Alexander filed 7 patents for work developed at NSA.

> During his time at the NSA, Alexander said he filed seven patents, four of which are still pending, that relate to an "end-to-end cybersecurity solution." Alexander said his co-inventor on the patents was Patrick Dowd, the chief technical officer and chief architect of the NSA. Alexander said the patented solution, which he wouldn't describe in detail given the sensitive nature of the work, involved "a line of thought about how you'd systematically do

> cybersecurity in a network."
>
> That sounds hard to distinguish from Alexander's new venture. But, he insisted, the behavior modeling and other key characteristics represent a fundamentally new approach that will "jump" ahead of the technology that's now being used in government and in the private sector.

Presumably, bringing Dowd on board will both make Alexander look more technologically credible and let Dowd profit off all the new patents Alexander is filing for, which he claims don't derive from work taxpayers paid for.

Capitalism, baby! Privatizing the profits paid for by the public!

All that said, I'm wondering whether this is about something else — and not just greed.

Yesterday, as part of a bankster cybersecurity shindig, one of Alexander's big named clients, SIFMA, rolled out its "Cybersecurity Regulatory Guidance." It's about what you'd expect from a bankster organization: demands that the government give what it needs, use a uniform light hand while regulating, show some flexibility in case that light hand becomes onerous, and never ever hold the financial industry accountable for its own shortcomings.

Bullet point 2 (Bullet point 1 basically says the US government has a big role to play here which may be true but also sounds like a demand for a handout) lays out the kind of public-private partnership SIFMA expects.

> Principle 2: Recognize the Value of Public–Private Collaboration in the Development of Agency Guidance
>
> Each party brings knowledge and influence that is required to be successful, and each has a role in making protections effective. Firms can assist regulators in making agency

> guidance better and more effective as it is in everyone's best interests to protect the financial industry and the customers it serves.
>
> The NIST Cybersecurity Framework is a useful model of public-private cooperation that should guide the development of agency guidance. NIST has done a tremendous job reaching out to stakeholders and strengthening collaboration with financial critical infrastructure. It is through such collaboration that voluntary standards for cybersecurity can be developed. NIST has raised awareness about the standards, encouraged its use, assisted the financial sector in refining its application to financial critical infrastructure components, and incorporated feedback from members of the financial sector.
>
> In this vein, we suggest that an agency working group be established that can facilitate coordination across the agencies, including independent agencies and SROs, and receive industry feedback on suggested approaches to cybersecurity. SIFMA views the improvement of cybersecurity regulatory guidance and industry improvement efforts as an ongoing process.
>
> Effective collaboration between the private and public sectors is critical today and in the future as the threat and the sector's capabilities continue to evolve.

Again, this public-private partnership may be necessary in the case of cybersecurity for critical infrastructure, but banks have a history of treating such partnership as lucrative handouts (and the principle document's concern about privacy has more to do with hiding their own deeds, and only secondarily discusses

the trust of their customers). Moreover, experience suggests that when "firms assist regulators in making agency guidance better," it usually has to do with socializing risk.

In any case, given that the banks are, once again, demanding socialism to protect themselves, is it any wonder NSA's top technology officer is spending half his days at a boondoggle serving these banks?

And given the last decade of impunity the banks have enjoyed, what better place to roll out an exotic counter-attacking cybersecurity approach (except for the risk that it'll bring down the fragile house of finance cards by mistake)?

> Alexander said that his new approach is different than anything that's been done before because it uses "behavioral models" to help predict what a hacker is likely to do. Rather than relying on analysis of malicious software to try to catch a hacker in the act, Alexander aims to spot them early on in their plots.

One of the most recent stories on the JP Morgan hack (which actually appears to be the kind of Treasuremapping NSA does of other country's critical infrastructure all the time) made it clear the banksters are already doing the kind of data sharing that Keith Alexander wailed he needed immunity to encourage.

> The F.B.I., after being contacted by JPMorgan, took the I.P. addresses the hackers were believed to have used to breach JPMorgan's system to other financial institutions, including Deutsche Bank and Bank of America, these people said. The purpose: to see whether the same intruders had tried to hack into their systems as well. The banks are also sharing information among themselves.

So clearly SIFMA's call for sharing represents something more, probably akin to the kind of socialism it benefits from in its members' core business models.

In the intelligence world, they use the term "sheep dip" to describe how they stick people subject to one authority — such as the SEALs who killed Osama bin Laden — under a more convenient authority — such as CIA's covert status. Maybe that's what's really going on here: sheep dipping NSA's top tech person into the private sector where his work will evade even the scant oversight given to NSA.

If SIFMA's looking for the kind of socialistic sharing akin to free money, then why should we be surprised the boondoggle at the center of it plans to share actual tech personnel?

Update: Reuters reports the deal's off. Apparently even Congress (beyond Alan Grayson, who has long had questions about Alexander's boondoggle) had a problem with this.