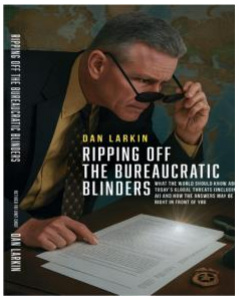
First Post - June, 2025

Hello, I realize that many of you don't know me, or what my life/work adventures have been, so I'll attempt to be brief in my introduction, and get to the primary message I'd like to share - at this time.

I'm a retired career FBI agent (with 24+ years with that agency) with jobs that spanned many field Offices, and FBIHQ (Criminal and Cyber Divisions) during that time. I've been fortunate to have had the opportunity to help mold much of what the FBI has come to be during that time, and establish previously unseen partnerships with Industry and Academia, in developing ways to better identify and combat, often international based organized criminals. I've also worked extensively with the Financial Services Industry and

I've advised/consulted a number of organizations regarding "Better-Best Practices" they might adopt to avoid becoming victims of such groups.

I've recently had a book of my experiences entitled "Ripping Off the Bureaucratic Blinders" published in which many more of my (hopefully relevant) life experiences are drawn out, helping readers realize the many opportunities we are all afforded along the way, to make much more of a positive impact, than we might have considered - across many sectors.



In reviewing the content and layout of this book, Editors and Publishing experts often asked, "what is the main message you're trying to convey?" While this question is reasonable and expected, the answer is a bit more complex. One significant take-away however would certainly be:

Who signed up to be a "Shrinking Violet"?

Avoid becoming a "Shrinking Violet" or adopting any version of a "Go along to get along" attitude, while working for one of the best equipped (personnel & jurisdiction wise) organizations in the world. Many times, if allowed to manifest- unchecked -, the pride you may have in the outfit you were fortunate to be appointed to, can quickly shift to organizational arrogance (with tightly fitted Blinders) where you disregard key partnerships with law enforcement or Industry- standing right in front of you- along the way.

A couple key points of pride – out of the gate:

I recalled shortly after taking my Oath of Office as an FBI Agent, reviewing the list of violations the FBI had jurisdiction in- finding more than 200 categories (now more than 300) of Criminal and Foreign Counter Intel matters. This combined with the FBI's jurisdiction across the U.S and many parts of the globe, made it truly international in scope. To me this meant we could follow the trail- pretty much- wherever it led, and whatever it ended up being called (criminal case wise). I found out soon thereafter that this was indeed the intention in creating the FBI, and I had not misinterpreted that. To me this was a real reason to be proud to be part of this outfit. For much of my first 10+ years in the FBI, this was in-fact the case. If we found a criminal group to have changed their Method of Operation (MO) or otherwise expand their scope criminal behavior, we'd just add that violation type to the title of the case, and in some cases open a parallel closely coordinated investigation.

As the case move from state to state, or county to country, we'd expand the character of the case to reflect that too. Stating is succinctly, the case would continue, and would more likely expand to involve other offices, as opposed to shutting down based on limited (perception vs reality) view of the allowed scope by field agents or Supervisors.

Sadly, later in my FBI career, FBIHQ (Cyber Division in particular) began chastising Field Offices (levelling resource penalties against them) for not opening enough cases in one category vs another. Field Offices became keenly aware of this and

started leaning toward only opening (or working) such cases, leaving many others largely un-addressed.

This situation was further worsened with the recognition (at that time) that a "Computer Intrusion" prosecution would need to involve a victim computer of "Government Interest" -meaning basically it was owned by the Government, and the tabulated loss had to be more than $5,000. This set of guidelines left any cases involving privately owned computer systems (including financial services and other major organizations) "out in the cold"- so to speak.

While some newly passed legislation helped change the available pertinent statutes, I was further frustrated when I learned – as recently as January of 2025, that the FBI had instituted a new (quite dysfunctional) acronym associated with how Field Offices and Agents would be trained and evaluated known as your Area of Responsibility or (AOR). Again, for those not aware, the AOR for any Field Office – translates to your specfic territory. In Many cases that only includes a portion of the state the office is located in, making the FBI's AOR scope smaller in many cases than that of the State Police.

I recall hearing of this new guidance while attending a national Cyber Crime conference, and after a couple of pointed "what the F…." bombs, I stated that "your AOR should be the planet Earth – not your backyard".

This "smack in the face" dose of reality in contrast to the "Key Points of Pride" noted above, serves up some real-life present-day opportunities to not be a "Shrinking Violet", in my view.

A remedy (also cited in my book) offered is that "People perform based on how they are evaluated". Simply put, the FBI should adopt immediately- with DOJ oversight- revised inspections of FBI Field Offices (Including SSA's and Squads) to determine what specific (actual not just on paper) partnerships the office leverages to advance priority investigative interests. This would be corroborated via interviews of key partnership leaders, and explore:

1) How the partnership functions – what cases/matters are addressed, and
2) What intelligence is developed/shared & how that occurs?
3) Roles defined for each partner and who develops/revises those?
4) Success achieved to date
5) How are partnerships expanded on - enhanced going forward?

I welcome any thoughts/feedback on this of course.

I'll be following this with two other posts regarding:

1) Testimony provided to House Financial Services Committee on this subject, and
2) Human Capital Academy program – for re-instituting program for recruiting/training/hiring Cyber Intel Investigators/Analysts