Prepared Statement by

Nick Sinai

Senior Advisor, Insight Partners; Adjunct Lecturer in Public Policy at the Harvard Kennedy School; Former U. S. Deputy Chief Technology Officer

Before the

The House Permanent Select Committee on Intelligence's Subcommittee for Strategic Technology and Advanced Research Hearing on "Emerging Technologies and National Security: Posturing the U.S. Intelligence Community for Success"

Chairman Himes, Ranking Member Stewart, and members of the STAR subcommittee, thank you for the opportunity to testify on this important subject.

My name is Nick Sinai. I served for over five years in the Obama Administration, including four years in the White House Office of Science and Technology Policy (OSTP), and two years as U.S. Deputy Chief Technology Officer. I led President Obama's Open Data and Open Government Initiatives, helped start and run the Presidential Innovation Fellows, and helped in the early days of the U.S. Digital Service.

I'm adjunct faculty at the Harvard Kennedy School, teaching a field class on technology and innovation in government, with clients in local and Federal government. Several of my students have started a non-profit, Coding It Forward, to place technical students in government agencies for a summer internship.[1] Many of my US students aspire to serve in the Federal government. At Harvard, I'm also a faculty affiliate of the Belfer Center for Science and International Affairs and the Shorenstein Center for Media, Politics and Public Policy—and previously was a Walter Shorenstein Media and Democracy Fellow.

I serve as a Senior Advisor to Insight Partners, a large venture capital and growth investor headquartered in New York City. Insight is one of the larger investors in software, with a current fund over $6 Billion and over $20 Billion of assets currently under management. I've

[1] https://www.codingitforward.com/

been with Insight since late 2014, and before my time in government, I worked at two other VC firms in the Boston area.

Insight Partners invests in fast-growing software companies in a number of areas—including customer experience, cyber security, software development infrastructure, and analytics. Insight-backed companies generally have strong product-market fit, commercial traction, and are growing quickly.

In my role at Insight, I work with Insight portfolio companies that are contemplating entering the Federal market, and with those that are already serving Federal customers. Insight has over 175 portfolio companies currently, roughly 30 of which are serving government customers or are contemplating entering the market.

It might be helpful for this subcommittee to understand how our CEOs think about entering the Federal market. At a high level, they weigh Federal market entry against putting resources in other vertical markets (healthcare, financial services, etc.) and new geographic markets (Europe, Asia-Pacific, etc.). All of these new market segments require market presence, localization, and product investment. Our companies have a limited pool of people, resources, and time so these choices can be difficult. They need to make investments that lead to revenue in the reasonably foreseeable future. Unfortunately, it can take years and a substantial investment to get into the Federal market. So companies that are earlier in their growth trajectory often pass and invest in higher return markets—which deprives the government of a broad swath of potential innovation.

When an Insight-backed company does decide to enter the Federal market, I strongly encourage the CEO to hire experienced talent. As a result, I have the privilege of working closely with experienced Vice-Presidents of Federal, many of whom have been selling into and supporting the intelligence community for years, or even decades.

These Federal executives have extensive experience taking fast-growing venture-backed technology companies and entering the Federal market, including Federal civilian agencies, Department of Defense (DoD), and the Intelligence Community (IC). But they also know how hard it is to enter these markets—it usually takes several years and millions of dollars of investment.

There is a common joke in the business: everyone wants to be the third Vice President (VP) of Federal.

It's because the first VP of Federal gets a lot of infrastructure set up internally and externally. They also spend a lot of time educating their own management team about the challenges of the market. The second VP of Federal educates the market about the new technology and does trials with prospective customers. But it's the third VP of Federal that makes the money. This is a well-known joke because it is true, sadly too often.

In preparation for this opportunity to testify, I spoke with a dozen experienced VPs of Federal that I work closely with. All of them felt that there is substantial friction to serving the IC from a venture-backed technology company. Many of them remarked that they typically enter the IC last, typically a few years after they have already entered the Federal civilian and DoD markets.

The net result is that the IC is perpetually years behind in seeing many venture-backed next-generation technologies.

I commend this committee for its inquiry into the opportunity for the Intelligence Community to better leverage next-generation technology, especially from fast-growing commercial software companies. I recognize that venture-backed software companies aren't the only type of innovation this subcommittee cares about, but it's impossible to talk about the future of the IC without talking about advances in software.

Software is eating the world, as the saying goes. Software and the Internet is changing transportation, banking, hospitality, manufacturing, and much more. Software is changing government too, including defense and intelligence. When we talk about next-generation technology in artificial intelligence, analytics, software development, cloud, or cyber—we are fundamentally talking about software innovation. To adopt the new capabilities we need to compete with our adversaries in great power competition, every IC agency needs to be a software agency.

How the IC builds and buys better software faster is a central question for this subcommittee—because it will directly impact whether the IC agencies are successful in their missions.

I recognize that this is not a new problem. I'm heartened by the efforts in the past decade to get the DoD and IC closer to the private-sector innovation ecosystem, and I want to especially commend former Secretary of Defense Ash Carter for his focus here—especially the creation of the Defense Innovation Unit (DIU), Defense Digital Service (DDS), and the Defense Innovation Board (DIB). Secretary Carter showed that strong leadership in this area can make a substantial difference.

Let me start with a few observations about the problem space, and then conclude with a few suggestions for the committee to consider.

1. Impediments to Adoption of Innovative Technology in the IC

Venture-backed software companies face logistical, technical, financial, cultural, and contractual barriers to effectively serve IC customers.

- **Logistical**: Simply engaging with members of the IC for product presentations, technical discussions, and discussion of future requirements is a real logistical hurdle. Most senior level technical individuals are physically located at sites that are subjected to the physical

limitations of a classified environment. Commonly used remote collaboration tools are often restricted from use on the networks or not accessible from the location of the IC employee. Although logistical challenges can be overcome, overall, they make it challenging for business development and field engineering professionals to meaningfully and repeatedly engage with technical IC members on a productive time frame.

- **Technical:** Next-generation technology companies that primarily serve commercial enterprises often struggle with the technical requirements to actually operate within the IC—this includes the lack of access to cloud services, encryption requirements, compliance, and certifications. To satisfy specific government requirements, companies often have to undertake significant product and engineering changes. This is costly, time-consuming, and an opportunity cost for companies that are pursuing other markets simultaneously. These changes are often required without any guarantee to the company that there will be business on the other side.

- **Financial:** One of the biggest hurdles for next generation technologies is determining whether or not to invest in selling and delivering products and solutions into the IC. More often than not this is the last market in North America for these companies to address because of the financial burden. If the technology is not specifically requested by the IC, then the risk of recruiting specialized staff and modifying the product to meet the specialized infrastructure often is too much to handle. Many VPs of Federal recommend entering the IC after first setting up a Federal practice for 3 to 5 years. Most of the IC engagements before then are very opportunistic or sporadic.

- **Cultural:** The cultural hurdles are bi-directional. The perception from the private sector is that the IC is slow moving, bureaucratic, and change resistant. The perception is that there are still too many in the IC with "not invented here" syndrome. Conversely, my sense is that the IC perception of the private sector is that they don't understand the unique technical challenges or understand the importance of the mission.

- **Contractual:** There are several phenomenal and capable technologies that are being developed outside of the US and within Trade Agreement Act (TAA) compliant countries. It can be challenging for companies to get a clear understanding of what is needed to mitigate Foreign Ownership, Control, of Influence (FOCI) restrictions. Most companies that have opportunities to partner with the IC and provide next generation technology are willing to comply with FOCI mitigation needs. But for smaller companies, however, navigating this process is a real challenge.

2. Innovation Onramps

The IC has a variety of mechanisms for engaging the private sector, including the venture-backed software companies that I have direct experience with. These mechanisms include new vendor programs offices, unclassified evaluation labs, In-Q-Tel sponsorship for onsite evaluation, evaluation through Federal System Integrators, and Amazon Web Services C2S program onboarding.

One challenge with new vendor processes inside the IC agencies is the timing. Based on talking with VPs of Federal, it takes an average of 18-36 months to progress from introduction to a potential product lab evaluation to an initial procurement—and sometimes much longer.

In-Q-Tel plays an important role, and I'm honored to testify along CEO Chris Darby today. I've co-invested with them in the past, and several current and former Insight Partners companies are also In-Q-Tel backed. In the best-case scenario, In-Q-Tel helps fund product development that will be broadly useful for the company, and helps raise awareness in the intelligence community —even leading to a production deal in an IC agency.

But there are important limitations to the model. In-Q-Tel sometimes invests ahead of demand in the IC. In-Q-Tel does not focus on helping companies navigate clearance issues or getting certified on IC cloud infrastructure. I've also seen firsthand scenarios where In-Q-Tel has inadvertently created a bottleneck, or funneled IC agency interest back into an existing work program.

It's worth noting the newer **Defense Innovation Unit** (DIU) model, even though it's not exclusively focused on the IC today.

DIU accelerates commercial technology adoption by partnering with customers across the DoD—including the services, combatant commands, and component organizations—to rapidly prototype and field advanced commercial solutions that address national security challenges. DIU matches internal defense customers with commercial technology companies, often via Other Transaction (OT) authority contracts that are completed under 60 days. DIU actively engages with VCs and VC-backed companies, especially in Silicon Valley, Boston, and Austin where they have offices. DIU is focused on delivering a low-friction process and getting commercial companies a quick answer.

One important thing that In-Q-Tel and DIU have in common is that they hire people from the start-up and VC ecosystem, and they are physically located in key markets. As this subcommittee continues to explore the topic of innovation, it's worth recognizing the importance of going where commercial innovation is happening, and hiring people native to that ecosystem.

Finally, there are a number of **new ventures, innovation, and industry liaisons offices** inside the individual intelligence agencies. I have had firsthand experience with some, and Insight Partners-backed companies have had many more. Although a promising initiative, I would say there is significant room for improvement. They often perform a gatekeeping function and don't have strong track records of finding and coaching innovative new companies through their agency. Most experienced sales professionals I know haven't had much luck with them, and they typically find ways around them to engage with senior technical and mission executives directly. I would urge the subcommittee to think about how these offices can be improved, or conversely, eliminated outright.

3. Commercial Technology vs Custom Built Systems

The specialized and complex mission requirements of the IC mean that there are often good reasons why the building of a custom IT system is contemplated. Large commercial enterprises build plenty of custom systems too. But too often in government, it takes years to write requirements, years to procure, years to custom-build technology, and years to test and deploy. We cannot build software the way we build battleships.

There are many examples of government failure in IT. I remember the failure of Healthcare.gov quite vividly—it was the U.S. CTO's office that spearheaded the recovery of the system. My boss at the time, U.S. CTO Todd Park, assembled a team that was instrumental in turning around a failing system. But large IT projects in government fail all the time—just usually very slowly and not in the headlines.

General Hyten, the Vice-Chairman of the Joint Chiefs of Staff, has recently talked about the importance of putting speed back into every element of the DoD.[2] He has talked about the importance of DoD accepting risk and learning through failure. While I commend his desire to inject speed into the system, I'd somewhat disagree about his point about risk. We already accept a lot of risk by continuing the status quo of large IT and mission systems that are failing or underperforming. Moving quickly with faster feedback cycles, at least with software, can reduce risk.

The Air Force's **Kessel Run**[3], the leading DoD software factory, located in Boston, has shown there is another way. They have demonstrated that the government can build software with quick feedback cycles, regularly involving the end-user at every stage. Kessel Run works with small product teams, collaborating in close partnership with its vendors and contractors to get new capabilities to airmen almost daily.

---

[2] https://www.defense.gov/Explore/News/Article/Article/2060538/speed-must-be-put-back-into-dod-hyten-says/
[3] https://kesselrun.af.mil/

Start-ups and scale-ups have an intense focus on speed, since they need to prove relevance or they will fail. VC-backed companies are mostly building a product, or a suite of products—that are designed to get better iteratively, as the company listens to its customers and incorporates that feedback rapidly into the next version of the product.

I'd urge this subcommittee to get data about the balance between commercial technology and custom-built systems in the IC, both for enterprise and mission systems.

4. Role of Federal System Integrators

The IC is supported by numerous Federal System Integrators (FSIs) who exist to build and operate current capabilities. FSIs typically have deep relationships in the agencies, through large multi-year contracts, and have many people onsite at the agencies. Unfortunately, FSIs are also part of the problem, as they have structural disincentives towards adoption of next generation technology.

FSIs have clear financial incentives to sell services or the development of custom technology rather than promote the adoption of commercial technology. They are not incentivized to adopt commercial technology on behalf of their IC or DoD customers. Any new technical capability that threatens to replace significant man hours with automation is naturally resisted by incumbent FSIs who have a financial incentive to bill the government to maintain current capabilities.

FSIs also play a critical role in vetting and recommending new technology for the IC. In my opinion, this vetting function is problematic given their business interests. FSIs may see the interest by the government in a new technology as a business opportunity for them to propose something similar but more "tailored" to the specific needs of the government—which in practice means custom-developed by the FSI. The net result undermines the ability of innovative new companies to get traction in the government. And even in those cases where the government prevails and procures a promising new technology, the FSI can greatly hinder the adoption and success of the technology if it represents a threat to its business.

This clear conflict of interest, especially when a FSI is evaluating new commercial technology that might cannibalize current or future services revenue, is why many of the experienced VPs of Federal I work with are wary about the role that FSIs play. They feel that FSIs can hinder adoption of commercial technology, even copying new technology approaches with their own custom development teams.

We also have to look at the problem over time. Custom built systems may meet near-term mission objectives, but the ongoing Operations and Maintenance (O&M) tail also becomes expensive and burdensome for the government. Further, as commercial software often continues to improve (because product development investment is spread across an entire customer base,

not just government customers), the gap between commercial technology and custom systems can grow significantly over time.

The structural incentives for Federal system integrators simply aren't in the best interest of the government. Consider this hypothetical: suppose a FSI has a $200m contract with an Intelligence agency, say $1B over five years. What incentives do they have to deliver more than the contract requires, either more capability or delivering faster? If they figure out how to accomplish the mission set faster or better, leveraging new commercial technology, and only charge the government $100M that year, the executive in charge would be fired. If the contractor in this hypothetical is a public company, they'd scramble to find the revenue shortfall or get punished by the shareholders.

But I think it's too easy to critique the Federal system integrators—they are a reflection of the complexity of government. We have created an ecosystem of large and small contractors that are dependent on the government. While they do important mission work, part of their core competency is mastering the complexity of government procurement and acquisition.

I know many honorable and talented people that work at FSIs. They do important and hard work, and many of them are former DoD and IC professionals with very distinguished careers. But the overall system we've collectively created is not one designed to best leverage next generation commercial innovation. And that is a real problem for the IC.

5. <u>Security Clearances</u>

Any conversation about bringing innovative technology into the IC would be incomplete without a discussion about security clearances. It is a major impediment to the adoption of emerging technology, and this subcommittee ought to explore how problematic it is.

It typically takes VC-backed companies a long time to get a facilities clearance. (A non-possessing Top Secret Facilities Clearance allows a company to hold the clearances of their employees without actually storing any classified data.) Without a facilities clearance, it is hard for a company to recruit employees with clearances. And if sales executives don't have the appropriate level of clearances, it's difficult for them to have discussions about the problems that the government is trying to solve. Furthermore, it's almost impossible to install and configure products into classified environments if the company doesn't have a cleared sales engineer.

In order to evaluate and demonstrate the potential benefit of next-generation technologies, the IC needs subject matter experts in the new technology that also understand how it might be applied to mission requirements. Invariably this requires security clearances for the subject matter experts with access to classified data and operational activities. This creates a proverbial "Catch 22" scenario: by requiring clearances of industry subject matter experts, the IC inherently limits

itself to technical experts who are already engaged in the community and who are not engaged in the cutting-edge capabilities that the IC wants and needs.

Solutions

Let me offer a few ideas for solutions:

1. Leverage the VC Community

The intelligence community should better leverage VC and Growth Investors. Insight Partners tracks tens of thousands of software companies, talks with thousands of companies per year, and yet we only invest in a few per year. If the IC were to better leverage the top VC and Growth firms, the IC would disproportionately have better access and information about the leading companies in each technology category.

2. Explicitly Focus on Scale-Ups

The IC should focus on scale-ups, in addition to start-ups. Start-ups are incredibly important, and the government needs to engage them. But the majority of start-ups aren't financially successful. The IC needs to focus on those venture-backed software companies that are winning in the marketplace, attracting additional capital, and are becoming the category leader—i.e. the scale-ups.

Let me give you a DoD example: The Air Force has started doing Pitch Days to quickly award Small Business Innovation Research (SBIR) money to innovative start-ups.[4] This is commendable, and the Air Force has demonstrated an ability to award contracts quickly. But the SBIR mechanism wasn't really designed for VCs owning a majority of a company, or for companies with over 500 employees. A scale-up may have raised enough VC investment where the founders own less than 50% or may have recently grown past 500 employees. Why would we disqualify those scale-ups at exactly the moment they are becoming successful? Why would we make it harder for a company that is finally in a strong position to support the DoD?

3. Improve Incentives for Commercial Technology Adoption

We get what we incentive. FSIs should be incentivized to adopt commercial technology on behalf of their IC customers and the large programs they run. FSIs that play a technology vetting role for IC agencies should be evaluated on the velocity of adoption of next-generation

[4] https://www.afwerx.af.mil/stories/space-pitch-day.html

commercial technology. If we can't get the incentives right, then the big FSIs shouldn't be in the technology vetting business for the IC.

4. Create a Centralized IC Onramp.

I would encourage this subcommittee to explore reforming and strengthening existing IC agency efforts to engage companies that don't traditionally operate in the IC. But it should also consider creating a brand-new government unit that focuses on testing existing commercial products, helping vendors navigate IC clearance and acquisition issues, and connecting those companies to funded IC programs and users. As many exciting next-generation technologies are cloud-based, this new effort could also include a "cloud on ramp" service to advise and support faster certification of commercial products in a C2S cloud region. If there is hesitancy about starting a brand-new organization in the IC, consider expanding and adapting DIU to include the activities described above, and to partner with non-defense IC agencies and components.

5. Start an Intelligence Innovation Board

I would suggest creating a federal advisory board with a mandate and profile similar to the Defense Innovation Board (DIB).[5] The DIB has offered a number of important recommendations about how DoD should reform how it builds, buys, and evolves software. The DIB concluded:

- "The current approach to software development is a leading source of risk to DoD: it takes too long, is too expensive, and exposes warfighters to unacceptable risk.
- Software is not being used to enable a more effective force, strengthen our ability to work with allies, and improve the business processes of the Department.
- Speed and cycle time are the most important metrics for managing software. DoD needs to deploy and update software that works for its users at the speed of (mission) need, and execute inside the OODA loop of our adversaries to maintain advantage.
- Software is made by people and for people, so digital talent matters. DoD's current personnel processes and culture will not allow its military and civilian software capabilities to grow nearly enough to meet its needs. New mechanisms are required.
- Software is different than hardware (and not all software is the same). Hardware can be developed, procured, and maintained. Software is an enduring and evolving capability."[6]

At the very least, the entire IC should have a respected process to consider the DIB's existing recommendations, as most of them appear very relevant to the IC broadly. The DIB's mandate is DoD-wide, so I'm hopeful the intelligence agencies and components inside the DoD are already addressing the DIB recommendations.

---

[5] https://innovation.defense.gov/

[6] https://media.defense.gov/2019/May/01/2002126691/-1/-1/0/SWAP%20FLYER.PDF

6. Develop Training on Next-Generation Commercial Innovation

The IC should provide training for its executives and staff about the commercial innovation ecosystem, as well as training on business and acquisition practices to better accommodate fast-growing startups and scale-ups. Imagine a training that helps IC professionals learn how to identify the best technologies, how to effectively scope and deliver prototypes in a short time, and how to use all available procurement authorities for rapid adoption. The DoD and the Air Force, specifically, have taken initial steps in conducting new training in some of these areas, and the IC ought to investigate what is working and adapt accordingly.[7]

7. Facilitate Bi-directional People Flow

We should encourage term-limited "tours of duty" in the IC. In my mind, we want more people serving our nation. My experience with the Presidential Innovation Fellows, U.S. Digital Service, and GSA's 18F have shown me that talented midcareer professionals will take a pay cut to serve their country. Getting technologists, entrepreneurs, and technology industry executives to do a tour in the IC will help the IC, and our country. Large technology companies, and large companies more generally, could improve their civic leave processes. We should also find ways for IC members to do tours of duty in large technology companies, start-ups, and even venture capital firms. I suspect that this already happens to some degree—but how can we do more of it, and make it more impactful? The intelligence community is only as strong as its people, and getting the best of America to serve will help us all.

I thank the subcommittee for its interest in this topic and would be happy to answer any questions.

[7] Examples include the Air Force's Project Banshee (https://www.hanscom.af.mil/News/Article-Display/Article/1894784/peos-to-churn-out-acquisition-banshees-through-training/) and the DoD's partnership with DCODE https://workscoop.com/2019/10/01/dcode-training-tech-government