Opening Remarks for the 37th Annual Federal Networks Conference

September 23 - 24, 2024

By Warren Suss

Conference Chairman and President, Suss Consulting, Inc.

Good morning.

Welcome to the 37th annual Federal Networks Conference.

To open the conference this year, though our speakers will cover a broad range of topics, from zero trust to cloud migration, I'd like to focus my opening remarks on the biggest opportunity in today's federal networks marketplace – Artificial Intelligence.

We will hear about the latest developments in AI from many of our speakers. To highlight a few: Laura Stanton and her colleagues Larry Hale, Jake Marcellus and Michael Berkholtz will lead off today's presentations with a discussion of GSA's approach to acquiring emergent technologies. Rear Admiral Chris Bartz will highlight the Department of Homeland Security's leading role in deploying AI solutions. Taka Ariga will give us an update on the government-wide deployment of AI. And tomorrow we'll hear from Daniel Holtzman, the CIO, Cyber Assurance Officer; Authorizing Official (AO) and the Senior Component Official for Privacy from the Chief Digital And Artificial Intelligence Office (CDAO) talking about their strategy for promoting the development of AI-enabled solutions to support DoD's most critical mission priorities.

Across Corporate America, the competition is on to lead in the race in applying AI to support strategic company objectives through greater operational effectiveness, improved market analytics, reduced cyber risks, and enhanced customer communications. Many AI innovations from Corporate America will provide use cases with enormous value when applied to supporting the core missions of federal agencies. For example, according to a Wall Street Journal Report earlier this month, Kaiser Permanente is focusing on the application of AI to reduce the administrative burden on clinicians by generating a first draft of clinical notes from recordings of patient interactions with their healthcare providers. This type of AI application could make a significant contribution to improving the quality and outcomes from appointments with patients in the VA, the Military Health System, and the National Institutes of Health.

According to the same report, Microsoft has developed an AI forecasting model, Aurora, that produces air pollution and weather forecasts 5,000 times faster than the models currently run by NOAA. And the commercial application of AI to improve the safety of autonomous vehicles through vehicle-to-pedestrian (V2P), Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications systems would deliver powerful benefits to improving the speed and cost-effectiveness of FEMA's disaster recovery operations and enhancing the US Transportation Command's global mobility capabilities.

These examples are just the tip of the iceberg. AI can improve the efficiency and effectiveness of the day-to-day internal government operations and can enhance service to the citizen through improvements to a wide array of citizen facing programs, supported by more effective automated help desk support and more useful agency web sites. We'll hear more examples from our speakers today and tomorrow.

With the enormous promise of Artificial Intelligence for almost every segment of our civil and defense agencies, the big question is how can we accelerate AI adoption in a safe, secure, and cost-effective way?

The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued last year on October 30th, highlights the importance of avoiding risks, but also encourages agencies to move forward rapidly to realize the benefits of AI.

Now, clearly, the government doesn't have the same deep pockets as corporate America, and we face a different set of AI risks and constraints, but agencies like Homeland Security are already rolling out applications that support key component mission objectives. According to a story in the New York Times on March 18th, DHS became "…the first federal agency to embrace the technology with a plan to incorporate generative A.I. models across a wide range of divisions. In partnerships with OpenAI, Anthropic and Meta, it will launch pilot programs using chatbots and other tools to help combat drug and human trafficking crimes, train immigration officials and prepare [for] emergency management across the nation." We'll hear an update on their progress later today.

The rest of the government isn't far behind DHS. As of December of last year, twenty of 23 agencies analyzed by the GAO reported about 1,200 current and planned artificial intelligence use cases—"specific challenges or opportunities that AI may solve." At that point in time, NASA was way ahead of the pack, with 390 use cases, followed by Commerce with 285, Energy with 117, and DHS with 87. Only three of the 23 agencies surveyed reported not having uses for AI. We'll get an update on the GAO study later today.

And DoD's Chief Digital and Artificial Intelligence Office (CDAO) has made a significant commitment to DoD AI policy development, research, and spending. According to Ken Evans, the Director of GSA FEDSIM, the CDAO enterprise plans to spend $3.5 billion this year on AI pathfinder initiatives. This includes $1.5 billion on AI Platforms, which represents 45% of CDAO's initial AI investments; $750 million on Data and AI Services, 22% of the pie, which includes data engineering, operations, and AI governance as well as AI and data management services; $500 million on commodity IT acquisition, representing 15% of the total, which includes procuring licenses, cloud access and cloud resources, commercial IT hardware and software; and $200 million, or 6% of the total, on Data and Business Analytics, including data science and enterprise analytics and application development. We'll get an update from CDAO tomorrow.

As the government IT marketplace moves past today's use case and pathfinder program phase, we are likely to see some fundamental changes in how the government conducts its business. Agencies involved in large scale modeling like NASA, the Department of Energy, the Environmental Protection Agency, and the Department of Interior, will not only use AI technologies to develop more powerful models, but they'll also be able to use AI's impressive ability to save significant costs and time in model development by generating code from simple, plain language instructions. This will allow agencies to allocate fewer resources for the time-consuming work of developing and debugging models and get more bang for the budget buck by reallocating resources to scientific research and analysis. As I mentioned, AI will help to improve the quality of citizen-facing websites, freeing up requirements for contact centers to handle routine inquiries, and allowing agencies to reallocate resources to hiring more specialists who can help citizens and federal employees address complex issues requiring individual attention.

We can anticipate similar shifts in IT support organizations across our civil and DoD agencies. AI will improve the quality of predictive analytics, network operations and management, and defensive cyber operations, reducing costs and improving the effectiveness of network and security operations centers and Tier 1 and 2 help desks. Here, again, we will have an opportunity to reallocate resources from routine operations to expand our government's higher skilled workforce to handling more complex IT troubleshooting and updating network technologies and network and security management processes. The payoff will be improved network defenses, greater network operational efficiency, and better end-user experience.

In other words, I'm suggesting that we're entering a new IT era when AI technologies will bring about levels of change in government and military operations similar in magnitude to those anticipated in the corporate sector. We will need to make dramatic changes in our tools, processes and procedures, skill sets, and training strategies to take full advantage of these changes.

For the remainder of my remarks this morning, I'd like to zero in on the implications of these changes for the federal networks marketplace.

First, a few words on the opportunities and challenges for industry.   When it comes to AI, there's no way to overemphasize the importance of first mover advantages. They can be summed up in one word

– Nvidia! But there are plenty more opportunities for federal AI first movers. The first companies that come up with reliable tools and strategies to minimize the risks from AI hallucinations, the first ones that develop systems and methodologies to help ensure the quality of AI data provenance, and the first ones that develop effective mechanisms to automate metadata tagging will certainly move to the head of the competitive pack. The opportunity space for industry is much broader than this. Of course, there's the burgeoning business of pouring old technology wine into bottles with new AI labels. But there's also the serious need to re-architect the government's networks and redesign its network services to help the government community get the most from AI. And there will be an explosive growth in demand for AI professionals, data scientists, and trainers. The bottom line for industry is that the companies that can move federal AI from promise and potential - to getting real-deal results for our government and military customers - will go to the head of the pack, and those that don't are likely to be left behind.

Now, how should agencies be adjusting their strategies for getting their hands on AI technologies and services that will get results, increase efficiency, and support the mission?

Let's start with one of the most obvious challenges – AI is expensive. As long as we're building use cases and experimenting with pilot programs, costs will be less of a problem. The Cloud Service Providers are enhancing their AI offerings, so it's natural for agencies like DHS that are looking for a quick start to turn to AI capabilities available in the cloud, including OpenAI, Anthropic and Meta, for their initial AI experiments. But as we move into an era of widespread, full-scale AI adoption, heavy duty AI model developers and users like the Department of Energy, will be able to belly up to the bar for upgrading their data centers with the latest high-cost AI chips, software and supporting hardware. But many other agencies, departments and programs won't have such deep pockets. If we're not careful, we'll end up with AI "haves and have-nots" or those who can benefit from AI economies of scale and those that can't.

One answer is to turn to a solution developed during the era of data center consolidation – shared services. Let's let the big guys who have the large-scale requirements and who operate the major data centers invest in the AI hardware they need, and allow the medium and smaller agencies to tag along and benefit from the lower unit costs available to their big brothers?

Another answer, pioneered by DISA, is the "Capacity Services" model. Let Value Added Resellers (VARs) and other industry system providers co-locate in government data centers, install and maintain the required AI chips and related hardware and software, based on changing levels of demand, and resell them to end user programs as usage-based services. This model has worked well for DISA and its customers. It avoids capital expenses and currently provides DoD access, by the drink, to processing, storage, and communications services in DISA data centers. The biggest challenge here is the unpredictability of demand for a technology as brand spanking new as Artificial Intelligence. To a degree, VARs can acquire hardware and software incrementally by following the AI demand curve, but it's a real guessing game to anticipate technology obsolescence and to predict cost changes in the wild west of today's AI marketplace.

And talking about unpredictability, I'd like to wrap up my remarks with a quick look at acquisition strategies appropriate to promoting accelerated growth in the adoption of AI technologies by the government in this immature market segment.   This non-technical issue may be the greatest determinant of whether we succeed in giving agencies access to the technologies and associated services needed for them to reap the benefits of AI.

Despite the inherently dynamic nature of the IT marketplace, in recent decades the government has too often approached IT acquisition using strategies more appropriate to the acquisition of stable commodities. I would argue that they have paid the price for this mistake, but things will get much worse in the coming AI era unless the government realigns its acquisition strategies with the unpredictable, high-risk nature of AI. This doesn't just apply to the costs of AI chips, software, and hardware, but also to the high-end professional services that the government will need to get targeted results from the technology.

Let me explain. After many years of pressure from industry, the government has largely backed off from "Low Price, Technically Acceptable" or LPTA acquisitions, which treated the purchase of IT professional talent, integration services, and even technology enhancement solutions as if they were standard nuts and bolts that could be bought from the lowest bidder who meets the specs. Not only did LPTA run counter to the spirit of the Federal Acquisition Regulations, but it caused a race to the bottom, resulting in an impossible mismatch between required skills and contracted hourly rates. After many years of experience, the results were predictable. Contractors couldn't pay the salaries necessary to attract the right talent, contractor performance suffered, and government program officials were disappointed. Incumbents lost recompetitions due to poor performance, and the same cycle repeated itself with the new contractor. I'd say, "rinse and repeat", but the metaphor is too clean.

Unfortunately, though the government has minimized the use of LPTA, it has substituted practices that result in LPTA-like acquisitions under the name of "Best Value".   They accomplish this slight-of-hand through what industry calls "levelizing", often accomplished through enough rounds of calls for clarifications from bidders so that weak proposals get stronger and, in the end, technical and management evaluation scores are so close that the bid is awarded based on lowest price.

Another strategy in widespread use that is a poor match for today's complex IT requirements and will be even less appropriate for the acquisition of tomorrow's AI solutions is to force contractors to bid fixed prices to design, install, operate, maintain and sustain IT environments when the government provides insufficient details about both the baseline environment and the technical requirements. In the ongoing cat and mouse game between government and industry, bidders have adapted to this type of acquisition with several strategies. Industry has incorporated clarifying assumptions in their bids to limit their risks. Now, some agencies are prohibiting bidders from including any assumptions in their proposals. Other tricks of the trade include "get well" post-award strategies, that hold the government to a literal interpretation of the contract. Given the impossibility of writing a contract that anticipates every slight change in requirements for complex IT systems and solutions, contractors are able to "Mod" their way to profitability through an ongoing series of charges for contract modifications.

The point of bringing up these examples of the ugly side of our federal IT marketplace is that if we continue to use inappropriate acquisition strategies like those I've just described, we'll poison the results and slow down our progress in achieving the potential from applying Artificial Intelligence solutions to support many of our civil and defense agencies' most important mission objectives.

So what's the alternative? In a nutshell, it's using acquisition strategies that do a better, fairer job of sharing risks between government and industry. Or, to put it more bluntly, the government needs to be willing to take on more risks to get the rewards from Artificial Intelligence. There are many ways to do this. The simplest is to use Cost Plus contracting. On projects with high degrees of uncertainty, the government agrees to pay what it costs. This puts a much greater burden on the government to manage the contract closely to minimize unnecessary costs. The government can throw in sweeteners by adding award fees and other incentives to promote superior contract performance.

Another alternative is to provide guaranteed minimums to allow contractors to recover a reasonable proportion of their costs for implementation and ongoing operations. This will be an important strategy since demand levels for AI-as-a-Service offerings are currently hard to predict.

My point here isn't to give a comprehensive laundry list of acquisition strategies to accelerate federal adoption of AI, but rather to highlight the need to give as much attention to thinking about how we will buy AI products and services as we give to thinking about how we will use this promising new technology. Let's add this to the long list of challenges facing our speakers today and tomorrow and their colleagues who are working their tails off to making sure that our technology does what's needed to support the vital missions of our nation's civil and defense agencies.

Thank you!

Warren Suss is President of Suss Consulting, Inc., headquartered in Jenkintown, Pennsylvania. The company has been helping leading corporations "Suss Out" the federal government information technology marketplace for over 40 years.