Opening Remarks for the 36th Annual Federal Networks Conference

September 27 - 28, 2023

By Warren Suss

Conference Chairman and President, Suss Consulting, Inc.

Good Morning – welcome to the 36th annual Federal Networks Conference.

Today and tomorrow, we will hear leaders of our federal and Defense Department communities talk about their top network requirements and challenges. The IT industry executives, technologists, business developers, capture managers, and sales and marketing specialists at the conference will focus on how their companies can do a better job than the competition in addressing these requirements and challenges.

I'd like to start off by giving ourselves a pat on the back. In many ways, the government IT marketplace operates far more efficiently and effectively than its counterparts in Corporate America. Because of our scale, our requirements for competition, and our comparatively open information access, we are able to deliver to federal and defense department users more robust technical services at better prices than our counterparts in Corporate America. In wide area networking, through programs like EIS and the DODIN, GSA and DISA have saved taxpayers billions of dollars through smart acquisition strategies. We have identified technical and cybersecurity weaknesses in commercial products and services and have introduced enhanced standards and metrics to meet the heavy duty requirements of our agencies. Our enterprise-level organizations, led by DISA and GSA and supported by NIST, NSA, CISA, and the federal system integrator and engineering communities, have not only helped industry identify and fix security flaws in their products and services, but have also held their feet to the fire for product improvements needed to operate at the enormous scale and complexity of our departments, agencies, and military services. So let's get over our Federal IT inferiority complex. Sure, we have problems and challenges, and we often move more slowly than we'd like to, but let's give ourselves some credit for our successes in providing powerful technologies and services at great prices.

In my remarks this morning, I'd like to focus on how to build on these successes with a new generation of information technologies including next generation commercial cloud services, Secure Access Service Edge (SASE), Zero Trust, and Artificial Intelligence. These technologies are driving significant changes in competitive marketplace dynamics. Our successes in the past have depended on understanding marketplace dynamics and developing acquisition strategies that effectively tap into these dynamics. I've spoken many times before about the strategies that account for our successes in acquiring wide area networking technologies: demand aggregation, RFP development with a serious commitment to open buyer-seller communication, and the creation of a level playing field to accomplish a degree of commoditization necessary to enable fierce but well-structured competition.

So how do we need to change our formulas for success going forward as our technologies advance and our marketplace dynamics evolve?

One change pervading the commercial and federal IT marketplace is industry's dramatic shift to what's been called Everything-as-a-Service. The primary movers here are the cloud service providers, the CSPs, and the primary services gaining traction are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), but lately it's been hard to find any IT or network infrastructure tools and applications that aren't being repackaged as services.

The promise, here, the real prize, is the opportunity to get out of the business of building and running our own IT railroads. The government can let industry take over the costs of building, operating, maintaining, and upgrading IT infrastructure. The government can buy and use it as needed and change suppliers based on who's got the best technology at the best prices. To put it another way, the move to Everything-as-a-Service should enable us to get the benefits of both maximizing competition and minimizing investment risks.

The biggest challenge, here, is commoditization. In theory, it's easier to recompete services than systems. There's no need to worry about a forklift upgrade when there's nothing for the forklift to lift. The Everything-as-a-Service provider is stuck with amortizing the costs of the equipment, and the government can shop for better technology at a better price. This is the appeal of multi-cloud solutions. If we can plug-and-play into multi-clouds from multi-providers, then the costs of switching or rebalancing would be low. Dial up on the one that's cheaper or that offers more features or better technology. Dial down on the ones with poorer customer service. Play them off against each other.

I say "in theory" because the ability to change depends on the substitutability of one service for another, and the feasibility, pain, and costs of service substitution depend on which services you're talking about. Here, we're coming up against the challenges of market segment maturity.

I spoke about the incredible success of GSA and DISA in delivering value to their wide area network users. But competitive dynamics are very different in the carrier world than in the emerging market segments for cloud services, zero trust technologies, SASE, and AI. AT&T was over 100 years old when GSA released the first government-wide competitive acquisition for commercial telecom services and DISA took advantage of the growing global availability and dramatic drop in prices for network fiber and equipment as industry competition was reaching a fever pitch. Both GSA and DISA were able to leverage, shape, and add needed security and operational extensions to a rich, established set of standards and related processes that defined commercial industry's newly competitive telecom offerings.

There are two pre-conditions for IT service substitutability. First, there needs to be a reasonable technical equivalence between services. Second, there needs to be information that's clear and accurate enough to allow buyers to compare features and prices. Sounds simple enough. But today's cloud, zero trust, SASE and AI services didn't evolve in the same type of highly regulated environment that spawned competition for wide area network services. Not only are we in a relatively immature market space, where new competitors are popping up all over the place, and more established companies are repackaging old wine in new bottles, but the essence of competitive differentiation for technologies like Artificial Intelligence is based on closely guarded secret sauce.

So in order to maximize competition and minimize risk, we need to segment the emerging Everything-as-a-Service marketplace and design our acquisition strategies to fit the characteristics of each segment. For example, in cloud services, when we compare the characteristics of Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service, it's pretty clear that Infrastructure-as-a-Service offers the greatest potential for substitutability. There are two basic services – compute and storage. Both can be substituted from one vendor to the next, and the rapid evolution of containerization technologies eases the complexity and pain of moving from one CSP to another. It also enables hybrid cloud strategies. There is an emerging set of tools to help manage multi-cloud compute and storage workloads. And, of course, the value proposition is strong for Infrastructure-as-a-Service because this technology targets one of government's biggest IT cost drivers – data center operations, management and sustainment.

With Infrastructure-as-a-Service, we can check the box of reasonable equivalence of services between vendors – our first pre-condition for substitutability. Things become more challenging when we move to the second box – clear and accurate information to allow buyers to compare features and prices. Here, we run smack into industry's magic pill to combat commoditization – different styles of packaging and branding to provide competitive differentiation. Even for services like compute and storage, which you'd think would be pretty straightforward, vendors have created a bewildering array of ways to name and package permutations and combinations of their offerings. Add to this the complex differences between vendor pricing strategies including inconsistent service price breaks between vendors, different data transfer charges, and an array of vendor-unique discounting and buying options, including on-demand pricing; reservation pricing; term commitment; free service tiers; no-charge initial monthly usage; and utilization credits.

The information challenges are serious here. Without the ability to make apples-to-apples comparisons of technical offerings and pricing, agencies won't get the full benefits of competition. And remember the benefits of demand aggregation – the core strategy accounting for the success of the government's wide area network acquisitions. If it's too difficult for agency buyers to aggregate demand and make apples-to-apples comparisons of technical offerings and prices, there are plenty of other options

available to acquire cloud Infrastructure-as-a-Service, or any of the other emerging technologies we're discussing. Here's where the government's acquisition organizations, along with their supporting contractors, can ride to the rescue to help our agencies get the full benefits of competition in this wild west competitive environment. They have the analytical firepower and the acquisition tools to help agencies, at both the umbrella IDIQ and at the Task Order levels, create order out of this information chaos and maximize the benefits of competition. They've done it before with WAN services, and they can do it again with today's emerging technologies.

We don't have as much leverage with Platform and even less with Software, since substitutability declines as we move down the stack. That doesn't mean we shouldn't try to get the best services at the lowest prices, but as the ability to achieve a reasonable degree of commoditization declines, the challenge of making apples-to-apples technical and price comparisons between vendors increases. The challenges become even greater as we move into less mature market segments to acquire newer technologies like SASE, Zero Trust and AI. To add to the challenge, there are so many channels to market for these technologies that it's easy for vendors to get to agencies and for agencies to get to vendors. Vendors can, in effect, work their own deals using the easiest or least competitive available contract vehicles.

Take AI, for example. Why should agencies go through the pain and delays of setting up an acquisition for AI when Microsoft, within a few months, will be integrating AI into PowerPoint, Word, Excel, and the rest of its best-selling products, according to a piece in the Wall Street Journal earlier this month. On the one hand, we could say "Great! The market is evolving and, for minimal additional cost and no delays, federal users can get their hands on it." The problem, of course, is that there are all kinds of risks with introducing AI into Federal and Defense agencies. With bleeding edge technologies like Artificial Intelligence, even the most eager early government adopters can't - or at least shouldn't be allowed to - ignore the risks associated with unknown or uncertain information provenance, challenges in understanding, explaining and justifying automated decisions, and uncontrollable and unpredictable performance anomalies. Without controls over where AI applications are getting their information or what AI applications are doing with the government's information, we're opening up a huge back door to all the systems and processes for protecting and ensuring the reliability of sensitive government data. Another way to look at it is that our acquisition community has a bigger role to play than helping to buy the best technology at low prices. They also serve as guardians, along with the government's technologists and program officials, to make sure we're buying this new generation of technologies in a way that protects us against these types of risks.

One helpful strategy, which applies equally to industry and government players, is to create a steppingstone roadmap to build trust in these emerging technologies, which will allow the government customer to surface and address risks in a systematic way. Whether we're talking about Artificial

Intelligence, Zero Trust or Secure Access Service Edge (SASE), government and industry players promoting the technology can work with user organizations to build a risk hierarchy of applications or network components. The first steps are designed to build trust by applying the technology to the lower-risk applications or network components. The ROI may not be so impressive, but this first steppingstone gives the user organization hands-on experience to build confidence. It provides an opportunity to design risk mitigation strategies and tactics in an environment where technical and operational impacts are limited. The next steppingstones on the roadmap build increasing levels of trust by proving out the technology on applications and network components that are more closely aligned with critical operations. These steppingstones also provide a more realistic basis for an enterprise-level business case analysis.

A note of caution, here. Pathfinder programs and research OTAs are steps in the right direction, but they tend to treat technology transformation as a two-step process rather than a lifecycle management commitment. Step 1, we set up and assess some pilots. Step 2, we incorporate the lessons of the pilots into an enterprise-level initiative. Good as far as it goes, but this two-step often doesn't account for trust and power dynamics that can slow things down or bring them to a grinding halt.

In the federal IT space, we tell ourselves that we are selling or buying technologies, solutions, and services. This is true, but we are also buying and selling trust. Budgetary and decision-making power are distributed unevenly throughout our federal and military hierarchies. Especially for next generation technologies, the organizations with mission responsibilities have the formal power to say no or the indirect power to sandbag an initiative that they don't trust, and top-down technology adoption policy mandates rarely succeed unless both government and industry are able to earn the trust of the organizations at the point of the spear. A lifecycle management commitment involves not only understanding the technical and management environments in these organizations, but also understanding and addressing their real and perceived risks. One reason why so many contracts fail to achieve their potential is that we take our eye off the ball when it comes to building trust. We bid low to win and then under-resource projects. We trot out our best and brightest as key personnel and then slug in second-tier players or unknown new hires as soon as we can. Our BD and sales stars, who understand the customer's environment, aches and pains, hopes and fears, get reassigned to the next big opportunity and have no incentive to help manage the contract for problem solving and successful delivery.

I put a large part of the blame on the government's embrace of Low Price, Technically Acceptable or LPTA acquisition strategies. Fortunately, the community appears to have learned its lesson from LPTA and LPTA-like acquisitions, but the habit is hard to break. Fear of delays, costs, and hassle associated with bid protests still drives many acquisition officials to focus on price rather than turning to the more

complicated task of seeking a real balance between price and quality. Awards based on price are easier to measure and easier to defend against protests.

One solution is to place greater evaluation weight on the contractor Basis-of-Estimate (BoE), which is intended to provide a clear link between technical and management requirements, contractor strategies for meeting these requirements, staffing plans, and price. The BOE has become a necessary part of most complex proposals, but it doesn't get the attention it needs from either the government or the industry sides and, in many ways, has become a dying art. There is a clear hierarchy of BOE techniques, and placing greater evaluation weights on BOE will encourage the use of more precise techniques and will make it more difficult for bidders to play games with pricing.

At a more general level, a proposal should be a creative but realistic plan for action. As we move away from the LPTA era, winning proposals will be the ones that present clear, credible, creative solutions to the government's top technical and project management challenges. They will include transition and implementation plans that reflect deep insight into the customer's starting point, the "as is", and present a fine-grained analysis of the steps, the timing, and the resources required to achieve the target "to-be" system architecture and operational environment. A more comprehensive list of key personnel, more care in outlining key personnel requirements, and greater reliance on oral presentations will provide government with a more realistic idea of who will be implementing and operating the proposed solution and will provide less wiggle room for contractors to game contract requirements.

All of this is expensive. The development of an effective acquisition strategy and a solid RFP requires a serious investment of time and resources from both acquisition and program officials. On the industry side, proposed key personnel need to be engaged in win strategy design, solution development, and proposal preparation to be convincing at orals. And allocating budget for experienced BD, sales, and senior executives to stay engaged to manage risks and perceptions through the life of the program adds more costs.

But the ROI gets to the heart of the matter – how do we, on both the government and industry sides, do the best job of supporting the missions of our federal and Defense Department agencies. Isn't that why we're here?

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.