Opening Remarks for the 33rd Annual Federal Networks Conference

February 26 – 27, 2020

By Warren Suss

Conference Chairman and President, Suss Consulting, Inc.

Good Morning. Welcome to the 33rd annual Federal Networks Conference.

Today and tomorrow, we will hear about upcoming civil and defense agency requirements for network-related technologies and services.

I don't think it's an exaggeration to say that this year, industry and government will have the greatest opportunity in over a decade to design and implement innovative, next-generation network and cyber technology solutions for our nation's civil and defense agencies. I mention cyber along with network services because it's becoming more and more difficult to separate one from the other. We used to highlight the government's need for speed, the insatiable appetite for bandwidth. But to quote DISA Director Vice Admiral Nancy Norton from her AFCEA DC luncheon keynote presentation last month, "Security is more important than speed."

2020 will be a tipping point for technologies that will define next generation network performance and defensive cyber operations, including Software Defined Wide Area Networking (SD/WAN), Artificial Intelligence and Machine Learning (AI/ML), and 5G mobile technologies, as well as the latest in Zero Trust Networking (ZTN) products, services, and architectures. We will also see the rollout of Trusted Internet Connection (TIC) 3.0 Use Cases, which represent a new frontier in the competitive race to establish federal network market leadership by incorporating trusted internet technologies in more flexible and more cost-effective ways.

For a number of years, we've been worrying about whether we are about to enter into a period of network transitions with minimal change or an era of transformation. To focus on the requirement to move from GSA's Networx contract to their EIS contract vehicle, the question is whether we'll put old wine in new bottles by replacing the 8 million services that are supposed to be disconnected from the older Networx contract within less than 30 months with the same old architectures and technologies on the new EIS contract or whether we'll use new architectures, technologies, and improved network and cyber management tools and processes to reduce costs, improve operational efficiencies and do a better job protecting our federal institutions from the growing cyber threat.

Based on the EIS Fair Opportunity requirements we've seen so far, things are looking good for transformation. In addition to the motivations associated with the growing cyber threat that we've just

discussed, there won't be as much old technology wine to put in the new contract bottles. To reduce costs and improve efficiency, carriers around the globe are rushing to dump their 150-year-old vintage Time Division Multiplexing (TDM) gear in favor of newer network technologies. Most agencies have had a hard time kicking the TDM habit. I don't know the proof of this old wine, but as proof that the government needs to kick the habit, GSA's government-wide statistics from right before the EIS contract awards, which includes data on traffic to 38,000 federal sites, tells the story: 37,000 sites – that's 97% - were still using TDM access. As the marketplace accelerates the move away from legacy TDM circuits, it will be harder and harder for our federal decision-makers to kick the technology can down the road and opt for plug-for-plug transitions rather than transformative network solutions.

So, between the carrots of lower costs and orders-of-magnitude greater performance, and the stick of industry pulling the plug on TDM, most agencies across the government will be buying a new generation of transformative network and cyber technologies and services. This raises important questions for everyone in this room and for our government and industry colleagues. The bottom-line question for industry focuses on how to compete for and win the government's next generation of transformative network contracts. The bottom line for the Defense Department and civil agencies focuses on how to acquire this next generation of network technology in a way that delivers the greatest value in terms of support for the mission, improvements to citizen services and increased productivity and effectiveness for internal government operations.

These aren't simple challenges, but I think we can find some answers in a closer look at the most significant trend in the 2020 federal networks marketplace: the acceleration and broadening of the move to the enterprise - a trend that has been gathering steam recently, but that started over 30 years ago. In 1988, GSA awarded the first government-wide network acquisition, FTS2000, and in the subsequent follow-on contracts – FTS2001, Networx, and now EIS – they have stayed true to the core of their original acquisition strategy. Aggregate government-wide demand to maximize competition, establish a clear and consistent set of standards to meet the heavy-duty needs of government agencies, and invest in an in-depth, open dialog with industry to create a level competitive playing field. It's worked – saving the government billions of dollars, providing up-to-date, highly reliable network services, and allowing agencies to minimize in-house engineering and program management personnel. GSA has been the victim of their own success, providing such high quality, reasonably priced services on each generation of contracts that it's always been a challenge to get agencies to move on to the next contract. The Federal CIO community has to deal with plenty of day-to-day operational challenges and mandated government-wide initiatives. The old Russian proverb still applies - Shoot the wolf closest to the sled. And the need to transition to the next generation GSA network contract is way behind the rest of the wolves, and *way* less vicious.

The GSA network services contracts aren't the only early example of the move to the enterprise. DISA has had an even longer track record in providing enterprise-level Wide Area Network services to the Defense Department. DISA has also aggregated demand to maximize competition and has established clear, rigorous technical standards. But DISA takes a more hands-on approach to engineering and running their global network. Their strategy is based on driving down costs by competing network transport, infrastructure, and Operations & Maintenance separately, while using a tightly controlled process, including regularly updated Security Guidance, Security Readiness Review Scripts, and Benchmarks to ensure that the network services for the Defense Department meet their heavy-duty warfighting and related support requirements.

In 2020 we will see three major trends shape the move to the enterprise in federal networks: Accelerating integration of the WAN; A new, broader definition of the enterprise network to includes lots more than transport; And a redefinition of the boundaries of the network.

The accelerated integration of the WAN, in both civil agencies and in the Defense Department, will include more end-to-end network optimization, greater agency-wide aggregation in the acquisition of circuits and services and more enterprise-wide coordinated adoption of next generation WAN and cyber technologies to enable greater efficiency and automation of network and cyber operations.

The second big trend – the broader definition of the enterprise network - is occurring because an increasing number and a broader range of network-related services are being acquired at the enterprise level to reduce security risks, to ensure enterprise-wide interoperability, and to facilitate more consistent, rapid technology enhancements. The definition of enterprise networks is broadening from the pipes that carry terabytes of digital information to now include the services and tools that give value to this information.

The third trend involves the redefinition of the boundaries of the enterprise network. It's no longer limited to connections between points of penetration into offices, buildings, campuses or bases. It goes from keyboard to keyboard and from mobile device to mobile device. It's no longer confined to carrier or government-owned fiber links and electronics. The broader definition of the government enterprise network extends into the government cloud, the commercial cloud, the local area network, as well as the final LAN, Wi-Fi or Bluetooth connection. And if you tell me that this broader definition of the enterprise network begins to sound like the definition of the end-to-end IT ecosystem, my answer is, you're right. As we move into a world of Everything-Over-IP (EoIP), when federal and DoD users need to communicate, receive and send information securely from anywhere to anywhere, a narrowed definition of the enterprise network implies a narrowed definition of the attack surface, which is not

only absurd, it's dangerous. Likewise, in an era of accelerating migration to government and commercial clouds, our definitions of the network management and security management domains need to be broad enough to give us the ability to protect, monitor and restore the health of the network and network services regardless of where our data and applications reside and regardless of where we decide to move them. This extreme broadening of the definition of the network enterprise isn't a dream – it's a necessity. It's the only practical way to approach managing today's IT environment and to prepare for tomorrow's changes in commercial IT marketplace technology and services.

So how should industry and government respond to these three trends – the accelerating integration of the WAN, a broader definition of the enterprise network and a redefinition of the boundaries of the network? I'd like to begin answering this question with some statistics. The true size of the federal government workforce is around 5 million, according to New York University professor Paul Light, if you add together full time federal employees, active-duty military personnel, and Postal Service workers. If you add in contract and grant employees, which includes a large staff augmentation component, the total is closer to 9 million. Federal networks not only need to interconnect these workers, but also must link them to a broader community of state and local government workers and coalition partners who support federal and military missions. Likewise, as I mentioned earlier, federal networks are linked to more than 38,000 federal sites when you expand beyond GSA's sample and add in the sites for large, specialized federal organizations, such as the FAA and the Intelligence Community. The statistics tell the tale: *federal networks connect about twice the number of workers and more than the total number of locations when compared with the combined total number of workers and sites at the top ten corporations in the United States.*

My reason for taking this brief statistical detour is to highlight a fact that we sometimes tend to overlook: As a consumer of network services, the federal government is the biggest game in town. Our scale, in terms of the number of workers and locations connected to networks, is, by orders of magnitude, second to none. This gives us extraordinary clout in the marketplace. It underscores the importance of accelerating integration of the WAN as a mechanism not only to do a better job at defensive cyber operations and to optimize the delivery of services to our user communities, but as a way to aggregate demand that helps flex our muscles in the marketplace. Likewise, the broadening definition of the scope of technologies and services covered in the move to the enterprise and the redefinition of the boundaries of the network give the government greater clout in the acquisition of industry's latest terrestrial, mobile, satellite, video, cloud, and cyber offerings.

This greater marketplace clout associated with the government's move to the enterprise is not limited to the buyer side of the economic equation. Industry executives in the government segment can

leverage this growing clout to strengthen their company's competitive positioning when going after enterprise-scale federal opportunities. This includes improving the ability to leverage internal company management resources to get more competitive pricing and stronger technical/engineering resources for developing solutions that will beat the competition. It also includes the ability of bidders to hold up a federal enterprise sized carrot to influence feature/functions and product development roadmaps of their suppliers or team members. And we're not just talking bells and whistles here. The federal move to the enterprise puts federal requirements for basic network services like email and collaboration off the charts when compared with requirements of typical corporate enterprises. In effect, federal primes serve as the government's "muscle" to make sure that commercial IT will really perform, at scale, for huge federal institutions like the Defense Department. Federal prime contractors also serve as the government's "muscle" to push the envelope of industry's commercial off the shelf offerings to meet the government's enterprise-level cyber and operational requirements.

The growing marketplace clout associated with the move to the enterprise won't come automatically, and this is the cautionary note at the tail of this marketplace tale. The government needs to be careful to use their enterprise-level clout or they'll lose it. In recent years, we have been so focused on the need to speed next generation network solutions to the federal customer, so consumed by our inferiority complex when we compare the government's acquisition system with what we perceive as the faster, more flexible approaches used by Corporate America, that we don't pay enough attention to exercising our muscle in the IT marketplace.

Let's go back to Econ 101. The marketplace is, theoretically, a place where a willing buyer and a willing seller come together with perfect information to conduct an economic transaction – for example, to put out and respond to an RFP to replace an existing network contract. Now we all know that there's no such thing as perfect information, and behavioral economics has taught us all kinds of new strategies and tactics to incorporate an understanding of our primitive, irrational brains and our imperfect organizational structures to approximate this theoretically ideal environment. But when we compare and contrast the characteristics of the federal marketplace with the way Corporate America buys stuff, we should appreciate that, in many ways, the government comes closer to the ideal competitive environment for marketplace transactions than the typical American corporation. Just try to get pricing history for contract awards to American corporations. You can't. The government, on the other hand, has extensive, detailed information about how much they've paid for goods and services. Not perfect, not always accessible, but way better than what you get from any U.S. Corporation. Or consider barriers to entry. It certainly is a royal pain in the butt for a company to enter the federal marketplace, but once they've figured it out, they can get information in exquisite detail about what the government needs, when they need it, what are the government's technical requirements, who are the contact points on

the buying side, who is likely to be the competition, and on and on. Likewise, the bidder who is willing to invest in understanding the Federal Acquisition Regulations and related documents can get a clear understanding of the rules of the road in the selling process. Consider, even, the hated bid protest process. Yes, it introduces delay in government acquisitions. Yes, it ties up government resources. Yes, sometimes companies protest for the wrong reasons – to delay the end of an incumbent contract, to poke a finger in the eye of the competition, or even to blame the unfairness of the government acquisition for what was the real problem – the failure to assess the competition correctly, the failure to read the customer environment correctly, or the failure to put together a good proposal. But you can also think of bid protests as validation that we have an open marketplace, that there are well defined rules of the road, and that there are effective ways to deal with those who violate the rules. Think of protests as the price we pay for having a more open, more transparent marketplace with clearer rules than most American Corporations.

So let's appreciate what we have in the federal marketplace, and let's not throw out the baby with the bathwater. On the government side, we need to take care with how we use mechanisms like the Defense Department's Other Transaction Authority or OTA. Yes, the OTA may speed our ability to buy IT, but it can also undercut the very opportunities to increase the government's clout in the marketplace that we've been talking about. Sure, let's figure out better ways to deliver innovative technology to our users, but let's consider carefully before we give up the opportunity to achieve the benefits of full and open competition, which allow us to aggregate demand, maximize the number of bidders, keep standards high, and achieve consistency across the enterprise. Likewise, let's continue to watch out for the interests of small and minority businesses to give them a fair shot at federal opportunities, but let's not take deals that are best addressed by leveraging the clout of the largest, most powerful players in our marketplace – the ones best positioned to act as government's "muscle" – and set them aside for small companies that can't deliver the results that the government needs because they don't have the technical breadth, the financial depth, or the experience to design and deliver large next generation enterprise network solutions at the right scale and the right price.

Let's also remember that getting results in a segment as complex and dynamic as today's federal network marketplace is as much an art as a science for government and industry. In a marketplace moving to SDN, 5G, AI/ML, Zero Trust, and white box technologies, acquisition strategies can't be applied mechanically. Commercial, off-the-shelf, out-of-the-box solutions are an illusion. The government's acquisition and program professionals are understaffed and overworked, but their acquisitions for next generation federal networks can't be approached as cut-and-paste jobs using documents issued years ago. The government must also pick acquisition vehicles that fit requirements for complex enterprise network and cyber technology, not vehicles designed and priced for low end

labor performing routine tasks. There's an art to putting together an RFP for next generation federal networks, and we need to take enough time to make sure we get inputs from program personnel, acquisition professionals and industry to get it right.

On the industry side, risk-taking and innovative thinking are as important as capture strategies and proposal plans. The winners in industry will be the players who master the integration challenges associated with the broader technical scope of next generation federal networks and the warp speed of network technology evolution. They're the ones who make an early, consistent commitment to engineering and solution development, even when government RFP release dates slip to the right. They're the ones who will take full advantage of the information-rich federal marketplace environment to set winning prices despite the many risks connected with next generation network technologies and customer behavior. They're the ones who will show that they really know how to implement complex federal networks by treating their proposals as thorough, credible plans for action, that don't sweep real risks under the rug, but address them with a combination of clear eyes and an entrepreneurial spirit.

A final note. Both government and industry need to target the sweet spot at the intersection between what the federal customer needs and what the commercial IT marketplace can deliver. This doesn't mean buying into the illusion that commercial off the shelf products and services will deliver next generation network technology out of the box. It does mean that the federal government is a big enough force to help shape the evolution of commercial network technologies. Yes, the government is no longer inventing next generation technologies as we did in the early days of the computer and the internet, but we are very large-scale early adopters with the clout to shape the direction of the largest network service and technology providers. We can get better prices and better solutions by packaging the government's heavy-duty requirements in ways that will provide an incentive for industry to improve the features, functions, and cyber protections needed in other important market segments including banking, finance, healthcare, education and state and local governments. By recognizing our power in the marketplace and playing our cards right, we will, together, be a shaper of markets at the same time that we do a better job supporting the important missions of our nation's civil and military agencies.

Thank you.

Warren Suss is President of Suss Consulting, Inc., headquartered in Jenkintown, Pennsylvania. The company has been delivering results for leading corporations and agencies in the federal government information technology community for over 38 years.