Good Morning,

It's a pleasure to be able to provide the National Industrial Security Program (NISP) policy impacts from an industry perspective today. To say the least, it has been a busy and unpredictable year thus far. What hasn't changed is industry's active involvement monitoring all the moving parts of the NISP that may have an impact on the industrial base. Today I will provide a few of the topics being monitored, tracked, and worked by the Industry NISPPAC members, and industry associations.

Industry has encountered an enormous amount of change these past few years and we are noticing this is increasing at a much faster pace than anticipated, understandably due to the increased threats towards US interests. It's more important now than ever that industry and the United States Government (USG) gain fidelity on the costs of NISP implementation before additional reforms and policies are considered and implemented.

I will also add now is the time for industry to be united in our efforts in addressing our collective concerns for the benefit of the entire cleared industrial base. Together we are stronger, I ask that the NISPPAC industry members are utilized to the greatest extend possible to address industry's NISP concerns with the United States Government .

New legislation, development of policy, and the variances in which federal agencies interpret and implement has caused a strain to industry that could impact our ability to provide the needed services and products to assist the United States Government in maintaining its competitive our edge over our adversaries.

Industry is continuously tracking new legislation and policy changes that will have an overarching impact on industry's operations. Some are minor and have been anticipated while others will have a major impact to our way of doing business On the surface one section of legislation may not cause concern however, when combined in the collective with all the other new polices, it may have an administrative and resource strain on the industrial base. Industry must closely follow legislation/policy from development to implementation as often seen a well-intended policy is as only as good as it is implemented at the lowest level. In many cases, the way an agency or department interrupts a new policy sometimes has an even greater effect on industry, often adding unnecessary administrative burdens when not accompanied by strategic vision and communication. Through the NISPPAC we can better shed light on industry's challenges in a collaborative environment proactively.

While I don't have time in this forum to address all of industry's interests and concerns with legislative impacts, I will speak to a few key sections of National Defense Authorization Act for Fiscal Year 2019 that has our interest.

Section 889 prohibits the Federal Government from procuring or obtaining, or extending or renewing a contract to procure or obtain, "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." The prohibition takes effect August 13, 2020,

Considering the impacts of COVID-19, industry associations have recommended language to extend section 889 implementation.

While we understand the need to combat the national security and intellectual property threats that face the United States there is still a lot of unknown implications to this rule. More collaboration with USG is required to ensure no disruption to services or products provided and to better understand how federal agencies intend to implement and the processes they will put in place for cleared industry to ensure compliance. Industry is confident that NISP supply chain topics will be the focus for the foreseeable future. Industry recommends the creation of a NISPPAC supply chain working group so discussions like the impacts to proposed or approved legislation can be addressed and as a team we can find viable solutions to our shared concerns about the risk to supply chains.

National Interest Determinations (NIDs) timelines and processes are still perceived as an issue for those companies under foreign ownership, control or influence that have a requirement for a NID. Delays in the process affects the ability of contractors to meet contractual obligations . NDAA, Section 842 eliminates the NID requirement for covered National Technology and Industrial Base companies beginning on October 1, 2020. Industry is looking to the USG for additional clarity and guidance to all contracting activities. It is recommended at the next scheduled NID NISPPAC Working Group to discuss the current NID process, identify gaps and work to find efficiencies in the process to limit processing timelines. Currently NISPPAC Industry does not have a full listing of companies under a NID obligation to better understand the issue from an industry perspective Industry is working on a Freedom of Information Act request to obtain the information so that discussions could be started with affected companies to understand the impacts and areas of concerns. Industry continues to work with USG on the overall process to improve timelines on NID approvals.

While industry has expressed concerns about the USGs ability to share threat, adverse and insider threat information for decades there is still work to be done. Section 9403 of the NDAA, *Federal Policy on Sharing of Information Pertaining to Contractor Employees in the Trusted Workforce* is a first step to improving this gap. Until industry is treated as an equal partner in the full spectrum of information sharing, we are limited on our visibility of potential threats. Information sharing policies should take into consideration protections for cleared industry to share relevant threat information between cleared companies and the USG without the fear of reprisal.

There are many other sections in the NDAA that affect industry's involvement in the NISP. These will be tracked, and industry impacts collected through the NISPPAC Policy working group for discussion with our government partners. In the future, it is beneficial to industry and USG alike to understand and acknowledge impacts to operations early in the process and partner to find amenable solutions.

Industry has and wishes to continue to be active partners on working groups to provide expertise early in the planning process for all aspects of the NISP. With that said, industry would like to acknowledge their appreciation to many government partners over this past year. ODNI, OPM and PAC PMO have increased their collaboration with industry NISPPAC members on vital personnel security reform. We look forward to continued discussions as government develops and implements this reform.

Additionally, DoD and DCSA were quick to act and increase their collaboration with industry at the on-set of COVID-19 to better understand the impact to industry. Albeit, collaboration had already increased prior to COVID-19, it was appreciated the level of involvement and effort by DoD to get industry guidance on several operational impacts. Industry encourages this type of collaboration at all levels on a continuous basis and not just during a crisis.

Industry is closely monitoring the impacts of new legislation and policy; but we are also still focused on the CSA agencies efforts to provide oversight of the industrial base.

At the November 2019 NISPPAC meeting, I last spoke about the 2020 Industry's Key Efforts we were focused on. At that time, it was DoD Cybersecurity Maturity Model Certification (CMMC), Risk Management, Insider Threat and Personnel security reform. While CMMC is about to be implemented throughout the DoD's cleared contractor base, industry still has concerns about the level of the effort, duplication of oversight and how the roll out will impact industry over the next few years. As noted, previously, ODNI, OPM and PACPMO have been working with industry on personnel security reform. While there are still some implementation unknowns the transparent discussions throughout the process are appreciated. The NISPPAC Insider Threat Working Group meet after the last NISPPAC meeting and is working on updating job aides in anticipation of the updated

Industrial Security Letter. Industry is still closely monitoring DoD's effort to move the NISP from a compliance-based program to a more risk-based process. While industry understands the reasoning, there have been processes developed over the last 2 years and tested in certain segments of industry resulting in an administrative and financial burden for companies without an associated policy or contractual obligation. While that process appears to be on-hold for the moment, industry is still concerned about new processes for Tailored Security Plans, being developed under the name Standard Security Practices (SPP), development of a Security Rating Score and other oversight procedures with little industry engagement at the NISPPAC level. A strategic vision and communication strategy of efforts would be beneficial to industry and the government customers that DCSA provides oversight in support of.

As DoD has the predominance of the cleared companies in the NISP, industry still would be interested in being engaged early with all CSAs as new oversight processes are developed. There is always a continued need to improve strategic communication of efforts, transparency of the processes, consistency across the nation, and understanding of industry impacts. Together we can develop solutions to better protect the nations critical information.

One notable area that industry has been exerting an enormous amount of resources is managing all the government systems developed and utilized to manage the NISP. Many systems have come on-line and/or are under development at the same time. While looking at one system it might not seem to be of concern but when coupled with , lack of a strategic plan or communications issues are amplified when promulgating to industry, there are also system latency and data integrity issues. Without a full understanding of the impact for any new system, process or procedure, the role of the facility security officer or any other NISP security professional can quickly become riddled with administrative burdens that move them away from actually performing security functions and moving to a more risk-based approach.

Industry looks forward to assisting our government partners in understanding our challenges so that collectively we can work on viable solutions so that industry at large can meet NISP regulatory requirements, ensure our companies viability in the US and global markets, and maintain a viable secure supply chain so that we can get to a balanced approach to protecting our national security.

One administrative note before I end.

Industry NISPPAC has started the process on the nomination and selection process for two new industry NISPPAC members and will have proposed member nominations to the chair no later than September 1, 2020.

Thank you for your time and look forward to in-person meetings in the future.