SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
"Nominations of Max Vekich, to be a Commissioner of the Federal Maritime Commission; Christopher Coes, to be Assistant Secretary for Transportation Policy, DOT; and Laurie E. Locascio, to be Under Secretary of Commerce for Standards and Technology, DOC"
253 Russell Senate Office Building
10:00 AM, October 20, 2021

Questions for the Record from Chair Maria Cantwell to Dr. Locascio

Supply Chain**.** The nation is experiencing considerable supply chain disruptions, including shortages in semiconductors. PACCAR, a truck manufacturer based in Bellevue, Washington, reported 9,000 unfinished trucks parked in lots waiting for semiconductors to be available. This is just the tip of the iceberg in the auto industry – it is estimated that there will be a production shortfall of almost 8 million vehicles by the end of this year. The United States Innovation and Competition Act ("USICA") would appropriate funds towards the CHIPS for America Fund, directing $39 billion to the Department of Commerce to help alleviate long-term issues with the semiconductor supply chain and $11 billion specifically to NIST for research that will strengthen the U.S. semiconductor ecosystem. USICA would also increase funding for the NIST Manufacturing Extension Partnership, which, among other responsibilities, helps small manufacturers understand and manage supply chain risks.

Question. What steps will you take as NIST Director to help protect the nation's supply chains and to ensure that CHIPS for America appropriations, and other funds dedicated to supply chain resiliency, are efficiently executed, well spent, based on national need, and free of political interference?

Answer.
The microchip shortage is an urgent concern across many sectors, and legislation like the CHIPS Act and USICA reflects the need to address this issue in a serious manner. If confirmed, I commit to meeting with leaders from across the semiconductor industry, representative trade groups and associations, and leaders from impacted industries including the automotive industry in Washington State, to hear firsthand about the challenges and threats they are facing, and to engage them in a dialog about the best possible solutions to meet the demands of the U.S. economy and national security. To solve these problems, we must work together in partnership – government and industry – for the benefit of the nation.

If confirmed, my top priority will be put into place the people, processes and partnerships necessary to implement the strategic efforts outlined in the CHIPS Act and USICA. I commit to working to establish robust programs that incentivize competitive U.S. semiconductor manufacturing and contribute to U.S. economic security through a domestic supply chain with measurable deliverables and timelines. I will work to grow the internal laboratory programs to meet the needs of the semiconductor community, building on the strengths of a longstanding research program in semiconductor electronics and in partnership with experts in industry, academia and other federal agencies. And I commit to support the NIST MEP program to work closely with the states to assess regional and national supply chains to address national shortages that we see across many sectors that are important to each state. If confirmed, and if this funding is appropriated by Congress and entrusted to NIST, I will ensure that the process for managing these dollars will be managed with the highest level of integrity, transparency, and accountability.

Diversity, Equity, and Inclusion. In March, NIST published the results of an internal survey on diversity and inclusion. The survey produced some troubling conclusions. More women than men reported being interrupted in meetings, not receiving credit for their ideas, and, "[B]elieve they have to work harder, wait longer for promotion and opportunities for leadership." Other surveys have shown that women and minorities are less likely to be promoted than their peers. Your résumé demonstrates a commitment to nurturing diversity and diversifying the STEM community.

Question. As NIST Director, how will you ensure that NIST recruits and maintains a welcoming environment for women and underrepresented minorities?

Answer.
Diversity, equity, and inclusion in STEM are topics that I am very passionate about, and I have been an advocate for a diverse workforce and diversification of leadership for my entire career. I understand the importance and responsibility of being a good role model for others and take that role very seriously.

My approach to this topic has always included:

- setting expectations of a respectful and inclusive workplace as the organizational leader;
- putting equitable processes in place so that all employees feel that they have the opportunity to be their best at work;
- engaging everyone in helping to develop an inclusive culture through compassionate and open dialog;
- actively mentoring and supporting women and underrepresented minorities;
- intentionally recruiting and creating pipelines by partnering with women and minority-based STEM organizations as well as universities that have strong STEM minority development programs; and
- educating the workforce about the benefits of diversity.

If confirmed, I will use my past experiences, and invite others to the table so that I can learn from them, so that together we can build solutions. The organization that does this right is the place that people will want to be a part of now and in the future. My goal is that NIST will be that place.

Questions for the Record from Senator Klobuchar to Dr. Laurie E. Locascio, to be Under Secretary of Commerce for Standards and Technology, U.S. Department of Commerce

Research on Algorithms at NIST. As you know, artificial intelligence and algorithms are everywhere. They decide which apartments we're allowed to rent, which jobs we get interviews for, and which food items go on sale at our local grocery store.

Question 1.
In your testimony, you discussed NIST's role in developing standards that are trusted worldwide. If confirmed, how will you lead NIST in developing standards to ensure artificial intelligence technologies are transparent and accountable to consumers?

Answer.
NIST activities in the field of AI are very important to the future of AI technology development and deployment. In order to achieve broader adoption and acceptance of AI in all sectors from banking to transportation to medicine, we need to have confidence that the AI systems are secure, explainable, and unbiased. NIST is developing an Artificial Intelligence Risk Management Framework with stakeholders from across the world and has fundamental and applied AI research programs. My understanding is that NIST staff, through this work, is dedicated toward cultivating trust in AI. This trust will ensure we can realize the full potential of AI, and I look forward to working with you to strengthen NIST's role in this area.

Additionally, I understand that discussions are already underway with the EU and other like-minded government counterparts to promote global cooperation in AI. If confirmed, I commit to supporting the Secretary of Commerce in engagements with our counterparts in these discussions. I will also ensure that NIST's AI experts are at the table meeting with their technical counterparts in standards bodies and in bilateral and multilateral meetings to address the issues of transparency and accountability to consumers.

Question 2.
Algorithms are powered by data — often massive amounts of data. In your view, what is the relationship between algorithms and data privacy?

Answer.
In order to promote the development of reliable and trustworthy AI, there must be access to reliable data upon which to train the algorithms. Of utmost importance in accessing that data, is protecting the privacy of those whose data is being used.

In January 2020, NIST released the NIST Privacy Framework and is actively working with stakeholders to promote its voluntary adoption. If confirmed, I will work with this committee and with NIST's ongoing activities to continue to promote its adoption and to assess whether there are gaps that need to be filled to address the committee's concerns.

Speaking to my own background, I have extensive experience in managing privacy of individuals' data as I manage the human subjects protections program at the University of

Maryland. There are robust checks and balances that are put into place that are required by law in order to ensure that we protect the privacy of human subjects involved in research.

Voluntary Voting System Guidelines. In February, the Election Assistance Commission (EAC) approved updated guidelines for voting systems known as the Voluntary Voting System Guidelines (VVSG) 2.0. The National Institute of Science and Technology (NIST) is charged with providing support to the EAC in developing the VVSG, producing testing methodologies in accordance with the VVSG, and with accrediting laboratories to test voting systems. The current guidelines (VVSG 1.0) were approved nearly 16 years ago, so it is critical that all components of VVSG 2.0 are finalized quickly and that voting system manufacturers can begin submitting new equipment for testing.

Question.
If you are confirmed, do you commit to ensuring NIST provides the resources necessary to make VVSG 2.0 operational as soon as possible and to fully support the EAC in accordance with NIST's responsibilities?

Answer.
At this point in time, when many have lost their trust in U.S. elections, it is critical that we are able to instill confidence in the integrity of our voting systems. It is not an overstatement to say that democracy is at stake, and the American people must believe that they can trust that their votes are counted and recorded accurately. If confirmed, I commit to working with this committee and with the EAC to identify and address its cybersecurity priorities for election systems. This will include that NIST has the resources needed to make VVSG 2.0 operational and to support the EAC in accordance with NIST's clear responsibilities.

Questions for the Record from Senator Sinema to Dr. Locascio

Semiconductors. A global semiconductor shortage has affected the supply of many goods that American families and businesses rely on. The U.S. Innovation and Competition Act (USICA) builds on my CHIPS for America Act by allocating over $50 billion in investments for our domestic semiconductor industry. The National Institute of Standards and Technology will likely have a role in distributing these funds through an incentive program for domestic semiconductor manufacturers.

Question 1.
If USICA becomes law and you are confirmed, how will you ensure NIST makes prudent investments in the semiconductor industry that ensure our federal dollars provide maximum benefit for domestic manufacturing?

Answer.
The microchip shortage is an urgent concern across many sectors, and legislation like the CHIPS Act and USICA reflects the need to address this issue in a serious manner. If confirmed, I commit to meeting with leaders from across the semiconductor industry, as well as representative trade groups and associations, and leaders from impacted industries to hear firsthand about the challenges and threats they are facing, and to engage them in a dialog about the best possible solutions to meet the demands of the U.S. economy and national security. To solve these problems, we must work together in partnership – government and industry – for the benefit of the nation.

If confirmed my top priority will be put into place the people, processes and partnerships necessary to implement the strategic efforts outlined in the CHIPS Act. I commit to working to establish robust programs that incentivize competitive U.S. semiconductor manufacturing and contribute to U.S. economic security through a domestic supply chain with measurable deliverables and timelines. If confirmed, and if this funding is entrusted to NIST, I will ensure that the process for managing these dollars will be managed with the highest level of integrity, transparency, and accountability.

Question 2.
How will these investments make our nation less dependent on other countries for new semiconductor chips?

Answer.
Investments to increase U.S. manufacturing and production, including packaging, of semiconductor chips to a level that is commensurate with U.S. demand (~30% of global demand) will decrease reliance on other countries for supply and decrease vulnerabilities in our supply chain for key sectors of the economy. Additionally, investments in cutting edge semiconductor research through the National Semiconductor Technology Center should increase our ability to innovate past current technologies and provide the bridge to manufacturing for next generation electronics in this country. These are both part of a long-term strategy which is necessary given the state of semiconductor manufacturing in the world today with the U.S.'s global position shrinking significantly in the last 30 years.

If confirmed, my position at NIST will be focused on planning and implementation of the programs established by the CHIPS Act, if funded.

Additionally, I will do what I can to support the Secretary of Commerce in her efforts to address short term supply chain issues through outreach to foreign governments and foreign semiconductor companies.

Manufacturing. NIST operates the Manufacturing USA program to bring together academics, manufacturers of varies sizes, and state and local partners to collaborate on manufacturing research. In addition, NIST's Hollings Manufacturing Extension Partnership provides consultations to small- and medium-sized manufacturers through state-based centers.

Question.
What actions will you take to ensure Arizona small business continue to have access to these NIST programs?

Answer.
The Manufacturing USA Program and its network of 16 institutes, supported by NIST, the Department of Defense, and the Department of Energy, are a critical part of America's overall goal to bring manufacturing back and strengthen U.S. competitiveness and innovation. Nearly 2,000 companies, universities, and non-profit organizations from across the U.S. participate in these institutes which serve as innovation hubs for manufacturing, providing real value to U.S. industry. These hubs will position the U.S. to compete globally in existing and emerging critical technologies. These hubs benefit the public by outreach to local K–12 students and teachers, stimulating workforce development in new technical fields, and providing for improved job opportunities.

Another important component in the U.S. efforts to bring back manufacturing is the NIST MEP program. I believe the MEP, working in every state in close partnership with local and regional assets, is critical to building a more healthy and vibrant manufacturing base across all of the U.S. If confirmed, I commit to support the MEP program and its extension in Arizona in partnership with the Arizona Commerce Authority. If confirmed, I would look forward to working with you in the continued growth and acceleration of manufacturing for the Nation.

Cybersecurity. The National Institute of Standards and Technology (NIST) plays an important role in developing cybersecurity and privacy standards, best practices, and technology to protect federal government and private sector networks. Over the past year, several new laws, the President's Executive Order 14028 "Improving the Nation's Cybersecurity", and new policies have tasked NIST with carrying out numerous cybersecurity-related requirements and with increasing collaboration with public and private sector entities.

Question.

What challenges does NIST face in meeting these new requirements? Are there other cybersecurity best practices, standards or technology that NIST wish it could pursue if it had the appropriate resources?

Answer.

In May 2021, the President's Executive Order on Improving the Nation's Cybersecurity (EO 14028), issued in response to the SolarWinds hack, charges multiple agencies – including NIST – with enhancing the security of the software supply chain. In July 2021, the President's National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, issued in response to the Colonial Pipeline attack, directs DHS to work with the Department of Commerce (and NIST as the Department's lead on cybersecurity) in developing cybersecurity performance goals. And in August 2021, at the White House Cybersecurity Summit, it was announced that NIST will collaborate with industry and other partners to develop a new framework to improve the security and integrity of the technology supply chain.

In my experience, NIST prioritizes its efforts effectively in order to meet critical deadlines. NIST is also an incredibly collaborative organization with private and public sector stakeholders and works effectively through partnership. That said, these are critically important and highly visible tasks that NIST has been assigned. The challenge NIST faces is it must manage these assignments while continuing to perform cutting edge cybersecurity research that can lead to future standards and guidelines. Cybersecurity is a high priority for NIST and we must not get behind. If confirmed, I will work with the committee and the Department of Commerce to ensure NIST's cybersecurity efforts are adequately resourced to help address the nation's critical cybersecurity needs.

Cyberspace Workforce. The FY 2021 National Defense Authorization Act (P.L. 116-283, Section 9402) enhanced NIST's ability to "identify and develop standards and guidelines for improving the cybersecurity workforce for an agency as part of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework." Originally, the NICE program was created as part of the Obama Administration's Cyberspace Policy Review (2009) and Comprehensive National Cybersecurity Initiative.

Question 1.

What are some of NIST's short- and long-term priorities in carrying out this responsibility and what are its plans in taking on the central lead to coordinate the efforts and outcomes for numerous educators and agencies with their own independent cyber education initiatives? What role will the new Office of the National Cyber Director play in these efforts?

Answer.

The NDAA tasks NIST with identifying career pathways for cyber security positions in the public and private sectors, establishing cooperative agreements between the National Initiative for Cybersecurity Education (NICE) and regional alliances, initiating national cybersecurity challenges, and carrying out programs to award competitive prizes, among other assignments. If I am confirmed as the next NIST Director, I would prioritize cybersecurity workforce development and support the use of all possible tools for attracting talent and building a robust cybersecurity pipeline. If confirmed, I would also support the development of cooperative agreements between NICE and regional alliances to develop training and assessment of the cybersecurity workforce around the Nation. I look forward to working with the committee on this important goal.

Question 2.
In your testimony, you mentioned having a family member take part in a reskilling program to become a cybersecurity expert. Are there any lessons you witnessed from this that would help inform reskilling efforts within NIST to ensure it has the skilled workforce it needs for the future?

Answer.
My son worked for several years in another field and was attracted into the cybersecurity workforce by the promise of potential career growth, flexibility, mobility, opportunity for remote work, and a stable high-paying job to support his young family. His initial retraining was a 6-month online program and not through a 4-year university. On the job, he now has opportunities for further retraining. From this experience, I see that it is important to have incredibly robust outreach activities to show people what is available, what the future opportunities are for growth, and how to retrain and upskill without a 4-year educational commitment. During the pandemic, we have lost millions of people from the workforce. I believe that cybersecurity jobs could be an attractor to pull some of these people back into the workforce.

Questions for the Record from Senator Hickenlooper to Dr. Laurie Locascio

Cyberattacks. Cyberattacks continue to impact small businesses, hospital networks, and other critical infrastructure throughout the nation. As Governor of Colorado, I helped establish *The National Cybersecurity Center* in Colorado Springs as an organization dedicated to cyber innovation and awareness that serves both public and private organizations and individuals through training, education, and research. If confirmed, I would like to invite you to the NCC to see the great work underway there. At the federal level, NIST plays an important role in cybersecurity by defining standards and best practices for organizations to build effective cyber defenses and mitigation plans.

Question.
How do clear definitions and standards produced by NIST help us measure and track cyber-related incidents so we can develop effective policies and protections? How can market solutions, such as cyber insurance, align incentives and remove barriers to help businesses of all sizes successfully adopt NIST's cybersecurity guidance?

Answer.
Thank you for the invitation to visit the National Cybersecurity Center (NCC) in Colorado Springs. If confirmed, I would be delighted to visit. It sounds like a wonderful model to shore up cybersecurity for public and private entities in your state. I would look forward to seeing how NIST might engage with the NCC.

Guidance, standards, and definitions produced by NIST in collaboration with public and private stakeholders can help to build an understanding and agreement of the appropriate metrics by which to gauge the effectiveness of our national cybersecurity efforts. In order to remove barriers to adoption of the Framework, NIST should continue to develop partnerships with potential stakeholders, conduct educational outreach, and work through the MEP program to reach small and medium sized manufacturers. A comprehensive approach to increasing adoption could include potential market solutions to incentivize adoption and increase awareness even further. If confirmed, I would prioritize NIST's cybersecurity programs and look forward to working with you and the committee on these issues.

Questions for the Record from Senator Warnock to Dr. Locascio

Regional Supply Chain. As one of his first acts in office, President Biden gave an executive order for a 100-day review of all American supply chains, including identifying risks for material sourcing, reviewing transportation needs, and assessing workforce skill matching. I was happy for NIST to be a part of the Biden Administration's supply chain review. However, the needs and challenges facing a small business manufacturer in Valdosta or Rome, Georgia are simply not the same as one in California, Indiana, or New York.

Question.
Dr. Locascio, do you believe that NIST should conduct a supply chain review that addresses regional supply chain differences in the country and provides localized findings and recommendations?

Answer.
The NIST MEP program and the Manufacturing USA program worked closely with the states during the pandemic to assess regional supply chain issues and it is my understanding that this information was passed back through the national network to assist manufacturers in locating parts and services across the national landscape. It is clear that we need an understanding of local, regional, and statewide supply chain issues to address the national shortages that we see across many sectors that are important to each state. To compete in this global economy and to ensure our quality of life, we must engage all states and regions in the U.S.

Cybersecurity. Every day, Georgians rely on digital and online networks for school, work, and health, to just name a few applications. However, security gaps in these networks can make it easier for bad actors to exploit vulnerabilities and cause long-lasting damage in our communities, including by accessing personal data and attacking critical infrastructure. I've heard from Georgia's Manufacturing Extension Partnership, based out of Georgia Tech, that smaller manufacturers across the state struggle to implement cybersecurity best practices because they lack the resources of larger corporations.

Question 1.
Dr. Locascio, if confirmed, would you commit to prioritizing cybersecurity issues at NIST, including through increased local and regional outreach by Manufacturing Extension Partnerships?

Answer.
The NIST Manufacturing Extension Partnership can be a powerful mechanism by which to promote cybersecurity efforts within small and medium sized manufacturers. The MEP can work to help those with fewer resources become familiar with the NIST Cybersecurity Framework, and can also assist those manufacturers with its implementation. NIST can also

work to ensure that its cybersecurity resources are produced in formats that are more practical and actionable for small businesses. If confirmed, I will commit to prioritizing cybersecurity issues at NIST, including outreach to Georgia manufacturers through the GaMEP in partnership with Georgia Tech.

Question 2. What steps would you take to encourage industry to implement NIST's cybersecurity framework?

Answer.
In order to remove barriers to adoption of the Cybersecurity Framework, NIST should continue to develop partnerships with potential stakeholders, conduct educational outreach, and work through the MEP program to reach small and medium sized manufacturers. If confirmed, I would prioritize NIST's cybersecurity programs and look forward to working with you and the committee to discuss further incentivization to increase adoption of the Framework.