PLENARY SESSION

Questions and Answers

- **U.S. EPA:** Wouldn't it sometimes be better to disconnect a part of critical infrastructure from the internet (instead of attempting to protect)?
    - **Nitin Natarajan, CISA**: Definitely. I think as we examine air-gapping systems, taking them off the internet is a safe way to go if we can. The challenge we have seen over the last several of years is the need for more remote operations and remote work. We are examining things like building the control systems. I came from the healthcare space, and when I was in my hospital, someone from engineering had to come into the building every time on the weekend when something happened. Now, we have remote mechanical systems and I think it is advantageous, but it also poses a risk. So, there is two folds to that, one is pre-COVID-19, where we transitioned to the need for more remote capabilities through internet and VPN. There is still that risk. The other part is that people have internet-facing devices and systems that they do not even realize are internet-facing. Our federal agencies are large machines with IT systems built over decades – do we even know what is connected to the internet and where? I totally agree that air-gapping is a way to go, if possible, but it needs to go hand-in-hand.
- **U.S. EPA:** What role do you see artificial intelligence (AI) playing in the future of cybersecurity?
    - **Nitin Natarajan, CISA**: We are having a lot of those discussions right now. For me, it is more about being able to identify the threats more immediately. When we examine the volume of the information we are tracking, things like potential risks from IP addresses, how do we make that differentiation between a threat and what is not a threat? A lot of that is still done manually. We use a certain amount of AI and machine learning currently, but we are not where we need to be, but I am excited to see what our partners in academia and other agencies are able to get done here. The sooner we can identify threats, the sooner we will be able to introduce mitigation. Using AI does introduce an additional vulnerability, though, and we need to prepare for that as well.
- **National Research Council of Canada:** Do you have any databases that tracks attacks on water distribution systems?
    - **Nitin Natarajan, CISA**: We are trying to get visibility on where and what type of attacks are happening, the frequency of attacks, and who the victims are. Many people who are attacked do not report it, and that is why we are trying to have better reporting systems so we can better understand what is out there. We are trying to do a better job of this and are working with federal partners in this space to improve. As we examine companies and governments advocating building in additional cybersecurity, we need to determine what resources we need to better enhance our cybersecurity posture. It is a different argument to say, 'I heard about an attack' versus 'we have seen X attacks over X amount of time that has resulted in this economic impact on our customers.'. Right now, we only have the information of the former and are trying to get the information to create the second bucket.
- **Air Force Institute of Technology:** What is the future of our budgetary needs?
    - **Nitin Natarajan, CISA**: There has always been a battle of how much we invest in cybersecurity versus physical security and how. To me, what we do not invest now is greatly outweighed by

the impacts of an attack. The savings that we gain are worth investing now, in terms of cost/benefit. But they money is not necessarily available. To me, it depends on that risk determination. Risk has 3 elements: risk identification (we spend a lot of time on this), risk mitigation (we spend a lot of time on this), and risk acceptance (stuff we identify but do not spend time on; we often forget this piece). We need to ask if we truly understand those risks that we are accepting. I think looking at that risk differently will help drive some of our resource investment strategies moving forward. However, we also have to realize that we will not be able to mitigate all risks.

- **U.S. EPA:** "ICS," used in the presentation to denote Industrial Control Systems, is also more commonly used to describe the Incident Command System for emergency management. Any concerns about confusion for the response community?
  - **Nitin Natarajan, CISA**: Possibly, but I think we try to abbreviate as best we can. I have had the privilege of working at three different federal departments, HHS, EPA, and now the Department of Homeland Security (DHS), and each time I had to learn and re-learn three different sets of acronyms. Each time there has been a lot of duplication across the federal inter-agency. We are going to try to de-duplicate acronyms as best we can but hopefully, in context, it will be clearer.
- **Booz Allen Hamilton:** Limited financial resources for cyber security is a challenge of drinking water systems. How can CISA assist in this area?
  - **Nitin Natarajan, CISA**: To me, it is about information-sharing and collaboration. I have been across the nation to water utilities (urban, suburban, and rural) and all of them need a different level of support – different tools/information/resources. CISA is never going to be in a position to fund everyone, so what I want to focus on is what we can do to benefit all sectors, particularly wastewater systems. Working collaboratively to understand risk, what can we provide with our work and collaborations to bring national tools and resources down to local levels? How do we partner with local associations and EPA so that utilities understand what is available? How do we help and inform elected officials so they are able to better provide support? It comes down to information-sharing and collaboration.
- **DSO National Laboratories:** With the current pandemic, holding online meetings is the current norm. How would you advise on securing such meetings?
  - **Nitin Natarajan, CISA**: Understand what software you are using! I speak at conferences using a lot of different platforms. We are seeing supply-chain impacts on resources but understanding supply-chain of your software is important, too. Are you using all the tools provided by the platform (e.g., multi-factor authentication)? Many of these platforms have capabilities that not everyone utilizes. So, it is understanding your platform and using the security and features they provide.
- **U.S. EPA:** What type of research is needed to support water utility cybersecurity? Do you envision using simulation and modeling tools to demonstrate consequences?
  - **Nitin Natarajan, CISA**: The research and development needs are vast. We want to make sure we are looking at the true risks and vulnerabilities in collaboration with our partners. CISA does not have a test bed. We can bring our cybersecurity knowledge to the issues other agencies are facing. We do not have decades of experience; we want to focus on collaboration to order to learn how to help. Sharing our ‘wish list’ with the research and development community – some of those have been tackled and some are still pending, so we have started there.
- **U.S. Air Force:** How much of the current infrastructure bill is allocated to cybersecurity?
  - **Nitin Natarajan, CISA**: I do not remember the exact number. What we are talking through now is how we get the most ‘bang for our buck’ with any investment we make. We want to make sure

what we do is not done in isolation and truly raises the bar and moves the needle forward. How do we build security in up front? As we use this infrastructure bill and build new systems, how do we build in cybersecurity into the front-end, which is easier than trying to retrofit later? We also want to look at building in this security into all the systems, not just those supported by this important bill.