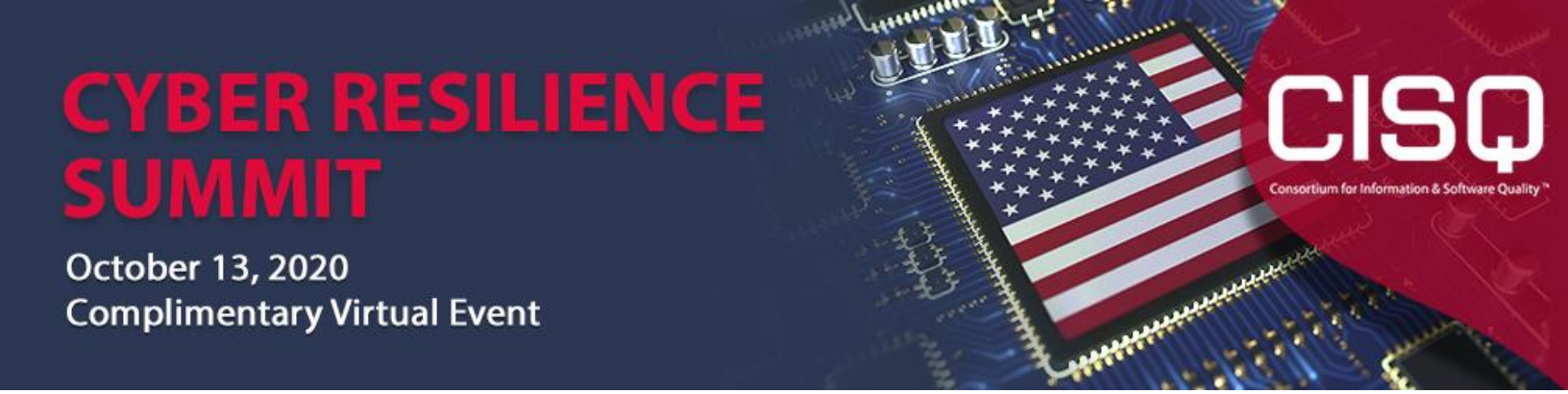

This "Titans of Cyber" closing discussion with Mr. Tony Scott, former Federal CIO and member of the Cyber Resilience Summit program committee, and Karen Evans, CIO of the Department of Homeland Security, will summarize key points made during the Summit and provide insights on the path forward. This discussion was moderated by Luke McCormack.

Tony Scott's remarks

- We talked about the notion of technical debt - issues left in code that you need to fix, architectural debt - the way things are put together, and security debt - things that haven't been done that should have been done. We must constantly remind ourselves about this debt.
- We tied into cost. Cheap sometimes results in higher costs. A lot of procurement activity has been based on lowest cost, technically acceptable.
- There has been a ton of progress on Software Bill of Materials (SBOM) in the last year. We should expand beyond software to a comprehensive BOM for hardware, software, and suppliers. Be mindful of the fact that whatever we put in place tends to be there for years. The biggest surface area is not necessarily where things come from, but what happens once things get installed. The operation of software and systems is very important. Bad stuff happens in that space. There are challenges in the operational supply chain.
- There is a continuous movement toward zero trust and narrowing the aperture of surface area where things can go wrong. We need progress on managing zero trust at scale.
- Final thought - depending upon your organization, your concerns and focus areas might vary somewhat. How do we bring organizational context into models and technologies? Remember who the client or customer is because you cannot do everything. Mission makes a huge difference.

Open discussion Karen Evans, Tony Scott, and Luke McCormack

- Karen Evans shared her perspective from being at OMB preparing guidance and now as DHS CIO implementing guidance. It is helpful to understand how OMB intends for circulars to be used together. That insight helps improve processes at DHS.
- DHS is very closely partnered with CISA. It is exciting to show other departments and agencies this collaboration and to be able to implement and demonstrate capabilities.
- OMB is focused on 2022 budget and guidance for fiscal year 2023. There are some gaps we can fill in preparation to make sure we are prepared. Artificial intelligence, for example, is one area. We are looking at AI from a resource perspective, cybersecurity perspective, and resilience perspective.
- Onto cyber workforce and the Cyber Talent Management System (CTMS) initiative. CTMS is a way for us to be competitive with private industry when hiring cyber talent, says Karen. It maps to the NICE Framework and skillsets map to competencies. It maps to private industry salaries, so

we are competitive when hiring cyber talent. It also determines additional training, career paths, and how to progress for career development. A pilot will run in May. Outstanding progress!

- Luke McCormack: Budget execution. As budgets take a haircut, IT budgets are inside of the CIO's organization. What is the best way to manage that situation, for security and cyber?
- Tony Scott: Big lesson I have learned as CIO is you have lots of tools at your disposal. There are easy things to cut, and then there are the right things to cut. Let us do cuts that are sustainable and will not boomerang back on us. It can be new application development budgets or capabilities that you prioritize... But what are the sustainable, wasteful things that will make us better and will not result in problems down the road? Sometimes it is an upgrade of existing technology. Talk with big tech companies.
- Karen: At the department, one of the challenges is this 2021 fiscal year the working capital fund has gone away. Depending on funding streams, we're going through an exercise of zero-base budgeting. Knowing the operational cost of services gives you the ability to gain efficiencies. We analyze contracts and partner with CPO. Working with CFO and Congress to reinvest those savings. Network modernization, cloud first, data center consolidation have real meaning now as we moved into a virtual environment.
- Luke: Cut, keep, and reinvest capability is important.
- Luke: Audience question about zero trust. Zero trust is not just one widget, it is a constellation of activities and technologies, like 5G. What is zero trust and what are those products and capabilities? Where are we on the zero trust journey?
- Tony: Still early days. We have done a great job of making things interoperable. Plug and play. But what we did not do in terms of designing interoperable architectures is answer the question: Should we interface, should we connect, is this a legitimate thing? Is it safe? A known quantity? Is it performing in the way it should? Zero trust is built up on couple of ideas - known *good* things and banning everything else. It is hard to scale this and manage it. It is a challenge today. You cannot do it manually today.
- Luke: Need machine-to-machine brains in the middle of this.
- Karen: DHS has some use cases under way. We are really talking about balancing risk tolerance to manage assets. IoT has blown up everything. As you try to establish the perimeter, the edge changes every day. We are living it today.
- Luke: We are living in a virtual world. Does the world stay virtual? What does that look like?
- Karen: Distributed infrastructure. The environment we are in demonstrates the need for resiliency. How apropos for the *Cyber Resilience Summit*.
- Tony: For every big wave that happens, there are aftershocks and waves over time. Once we get past the current COVID-19 crisis, whenever that is, we will see a reversion in some cases. People like to be with other people. Following is another reversion, hey, I do not have to be here 100% of the time. I can use this great networking technology to connect. We will see some really exciting things happen. The technology is getting better and better. Three years ago, we could not have done this like we can today.