**December 1, 2020 in Washington D.C.**

**ATARC interview with Jim Sheire, Branch Chief of Quality Services Management Office (QSMO) at Cybersecurity and Infrastructure Security Agency (CISA) and Vincent Sritapan, Cyber QSMO Acting Section Chief, CISA to look back on the first year of activities, discuss lessons learned and accomplishments made.**

**Tom Suder, ATARC:** Thank you for joining us today, my name is Tom Suder and I'm the founder of the Advanced Technology Academic Research Center. And we have a couple special guests today.

One of them is Jim Sheire, who's the Branch Chief for Cybersecurity at the Quality Services Management Office, or QSMO for short over at CISA in the Department of Homeland Security. We also have with us Vincent Sritapan, who's the Cyber QSMO Acting Section Chief over at CISA.

And my first question is for Jim: since the formal OMB designation of CISA as the Cyber QSMO in April of 2020, what have been the major initiatives, achievements, and challenges in performing its mission.

**Jim Sheire, CISA:** Thanks Tom, and thanks for having us here today. Really, really appreciate this opportunity to talk about CISA’s work in this area and advancing this key initiative.

So yes, so we were pleased to receive our formal designation this year.

Our major initiatives really have focused on the three service areas that OMB designated us for. So, we work on cyber broadly, of course, as a key system mission. But OMB designated us for three areas: a vulnerability disclosure platform service, a new protective DNS resolver service, and security operations centers, including SOC [Security Operations Center] as a service – so a managed service offering. And so that's really where our main focus has been: is going out and executing on that designation and developing solutions that we can bring to our agencies as shared services so that they can leverage those solutions that are centrally developed and procured and managed, instead of going out and procuring on their own or building from scratch. And you know we're leading to really substantial cost savings and more effective service delivery.

So, briefly, what we've been able to accomplish there is on VDP [Vulnerability Disclosure Platform] – so this is a platform that supports a Binding Operational Directive (BOD) that CISA issued around accepting reports that third party researchers submit to CISA on potential vulnerabilities they find on externally facing government systems. The agencies are required to set this up under the BOD, so our first service is a central platform where researchers can come and submit the vulnerabilities against agency systems where they’re centrally listed and handled. And the agencies, then, can leverage our service instead of building their own, in a centralized. We finished that procurement up at the end of September, so that is underway. And so, we're going through final procurement steps and then looking to stand that up and in 2021 and go live.

The second one on protective DNS resolver – we did some market research this summer. So that's moving through the acquisition lifecycle as well. We're looking to do a request for proposals later this year or early next year.

Lastly, security operation centers, that's been a really interesting one. So, there – instead of acquiring, one of the jobs of the QSMO is to partner with agencies that are currently offering cyber security shared services to other agencies – we call them federal shared service providers. And there, we early on knew that the Department of Justice offered a great service for security operations center, so the QSMO is partnering with DOJ where we're assessing their service, which is great. They have a number of existing customers. We want to support them and better making their service available to agencies connecting, where CISA identifies gaps in maturity or needs from our customers – can we connect them with DOJ and other providers. So, we are finalizing that partnership, and so DOJ will be (when it's all said and done) a QSMO approved federal shared service provider for security operations centers. And there too, we hope to wrap that up by the end of the year.

So those are really the three main initiatives we've rolled out on, and as you can tell, we've underlined that our acquisition strategies and research, we've had to work with our standards development lead – a separate office in CISA; we've partnered with other agencies; we've stood up the governance, the program management office for all the activities and build that out in our just our first year. So really this got started last summer with our first five-year implementation plan submission. The shared services governance board (that's the government-wide board that oversees this process) gave us great feedback on areas we needed to build out and make sure to cover. One key area that they called out was making sure we really built in a strong voice of customer functions. So, we built out a customer experience section that they really want to get the feedback from the agencies, not only from what their needs are, and services, but through our procurement, and execution, and eventually delivery. We want that strong feedback loop that brings those valuable insights back to us and it really guides everything we do through the life cycle.

And then, lastly, we're working on our first marketplace. So that's going to be kind of our storefront of our services. I mentioned earlier, really the key piece of QSMO is we want to create that marketplace of solutions that we've vetted, that we've done the work, so that agencies can go in and know that they're acquiring good high quality service to meet their mission need. So, we're going to build that out, and then look at potentially pursuing other designated service areas and see where that leads. So, yes, I'd say it’s been a great first year really with those three services, and those will be the focus in 2021 – finishing those up, and moving on to other areas.

**Suder:** Yes, that's fantastic. I know how hard it is to get other agencies on board. It sounds like you've done a really good job to bring these other agencies in it, so they're definitely seeing some early value.

How do you align with other CISA initiatives like CDM [Continuous Diagnostics and Mitigation] and trusted internet connection (TIC) that are kind of in your organization?

**Sheire:** So, CDM, likewise in execution of its mission is delivering tools and solutions to agencies, so we both sit in the same part of CISA. We closely align on kind of looking at what agency needs and gaps and support needs are. We really work closely together in looking at where is agency capacity? How can we help build it? What are the gaps, we can fill?

So, we're really well aligned there in our engagement strategy and it's great, of course, to be in the same piece of CISA with CDM, so that we can get the strategies closely aligned. We’ll be looking to build that out, even cooperate in certain areas going forward.

TIC – trusted internet connection – it's an emerging initiative, very interesting – what the implications and opportunities there are for services. So, I think – TBD. But there too, we sit in a similar part of the building, so we will of course support that key initiative in any way we can.

**Suder:** Great! Jim, I know it's only been a year, but it seems like you've made a lot of progress.

But what have been some of the key findings in the QSMO work to identify common technology services to meet the agency cyber security needs?

**Sheire:** Well, I'd say key finding, actually probably one of the major findings is – in trying to build out a solution that can meet a variety of mission needs and unique scenarios across government, an interesting part of our work is developing government wide standards and requirements that can capture that broad landscape. Because we often go in and find different needs, different delivery model requirements, different funding models, so that work of trying to find common solutions is very interesting.

Fortunately, I'll say – in looking at standards and requirements (by the way, by standards and requirements, I mean common cyber security standards and requirements based on underlying policy authorities. And of course, NIST standards themselves – NIST being the authoritative holder of IT standards), so we base a lot of our work there. Importantly, the QSMO actually partners with another entity in CISA, called the cybersecurity Standards Area Lead, or SAL for short. So, if you read the OMB and memo, and the governance around how sharing quality services is governed, the standards area lead is a distinct function separate from the QSMO. The QSMO focused more on the marketplace, the Federal providers, the acquisition strategies for solutions. The standards area lead – their job is to work with the cross agency community to develop that common set of standards and requirements and needs that we can then leverage in going out and partnering with a provider that meets those needs. So that's what we assess them against in setting up new acquisitions.

So, yes, that that key finding of that broad variety of needs and requirements. But then, you know, fortunate to work with that great group and the standards area lead to bring the community together to arrive on a common set of standards and requirements for that area.

And really, it's so important there too, again, to bring in the customers on developing those standards and requirements, because we need that voice of customer to better understand what that is. I'd say that that's been a key finding.

**Suder:** Absolutely.

Another question: how does the QSMO plan on leveraging innovative strategies of acquisition approaches to enable more procurement of cyber tools and solutions? Of course, we're in the Federal government – that's always one of the first questions. How do I get to this technology?

**Sheire:** Well, yes, it's a good question. You know, cybersecurity, of course, is a rapidly evolving field. We want to make sure we're looking at the latest and best solutions from the great community of solution providers, so we work closely with acquisition entities within CISA to look at what vehicles are available and what solutions.

For our first two services, we work with GSA on acquisitions and the VDP service, I mentioned. Productive DNS working there as well. But I know that our acquisition folks are looking at a number of new innovative, agile, other methods as we look at future solution tools, so I guess the answer there is – we will leverage the best tools we have to make sure that we're bringing innovative solutions in as part of our marketplace.

**Suder:** Great. Great.

Vincent, I've got a question for you: as a long time mobile security expert, what initiatives are you looking to promote in the cyber QSMO?

**Vincent Sritapan, CISA:** So, within cyber QSMO (and we have a variety of initiatives, as you mentioned), one of the first things that I'm looking at is leveraging existing capabilities across CISA and what does that mean for mobile and how can that be brought in? Whether as a centralized service or as a sort of a contract offering that leverages this standardization, cost savings, different economies of scale, including security language within the contract. One thing that I did look at right off the bat – if we are talking about protective DNS, as an example – how does that actually work within not just server laptop type of scenarios, but what does that mean for the mobile ecosystem – for iOS and Android.

If you think about the architecture, the API access, all that is very different than what you would normally get on the traditional platforms of Windows, Linux, and Mac OS. So, definitely, that's where I'm starting to look at first. There are definitely areas where we look to propose different types of centralized services, which I can't say too much about. But definitely, we do have plans for it. Even capabilities – you think about what was tried and true and proven with partnerships with NSA and others within the science and technology side of things that have already gone through test and evaluation. These are things that we're looking to bring forward, I’ll definitely say. But the platform with things like the federal mobility group – bringing that over honestly gives us a voice of people who own and operate mobile programs within government and how can they best leverage cyber QSMO.

I will say, in coming over, it is a very big step in trying to look at all the different aspects of mobile security and how that protects federal departments and agencies networks.

**Suder:** Thank you for that. And that's all the time we have today. Thank you, Jim and Vincent, for letting us know a lot about QSMO. And look forward to hearing what we come up with in the next year. Thank you very much.

**Sheire:** Thanks, Tom.

**Sritapan:** Thanks.