Mind the Gap: Federal Cybersecurity Workforce Initiatives

Featuring Jason Barke, Kristy Daphnis, Seeyew Mo, and RADM (Ret.) Mark Montgomery; moderated by Natalie Alms
Opening remarks by Camille Stewart Gloster
Introductory remarks by Cliff May

MAY: Well, good afternoon, everyone, and welcome, and thank you for joining us at the Foundation for Defense of Democracies for a discussion on the federal cyber workforce. It's Monday, November 6th. I'm Cliff May, I am FDD's founder and president. And on behalf of FDD, we're happy to welcome those here in person and those tuning in live and listening on podcast platforms for an event cohosted with CSC 2.0, which preserves the legacy and continues the work of the Cyberspace Solarium Commission, and that was established to develop a consensus on a strategic approach defending the United States and cyberspace against cyberattacks of significant consequence.

About a year and a half ago, FDD and CSC 2.0 released a report on the federal cyber workforce, and we hosted an event with then-Director Chris Inglis. Since that time, our experts have had the honor of working closely with the Office of the National Cyber Director as the ONCD developed the National Cyber Workforce and Education Strategy, a robust strategy that sets out ambitious goals to equip Americans with foundational cyber skills, transfer cyber – transform cyber education, expand the national cyber workforce, and strengthen the federal cyber workforce, as well.

We're here today to discuss the fourth pillar and are pleased to have on stage with us Seeyew Mo – thank you – assistant national cyber director for workforce education and awareness, and Jason Barke, the deputy associate director for the strategic workforce planning at the Office of Personnel Management, and Kristy Daphnis, a senior executive in the Office of Performance and Personnel Management at the Office of Management and Budget, and of course, our own Rear Admiral Mark Montgomery, senior director of FDD's Center on Cyber and Technology Innovation and CSC 2.0 executive director.

Now, before I turn it over to Natalie Alms, staff reporter at, to moderate our discussion today, I'm pleased to introduce Camille Stewart Gloster, deputy national cyber director of technology and ecosystem security. We at FDD like to say that we knew Camille, when? We have had the privilege of working with her for, what is it, five, six years? I lose track of these things – since you first participated in FDD's national security program for mid-career professionals. She led initiatives at our Transformative Cyber Innovation Lab, uncovering how Beijing, the Chinese Communist Party of China, is exploiting the U.S. bankruptcy courts to acquire sensitive technology, and then identifying critical gaps in the policy community's understanding of cybersecurity behavior and individual identity.

Camille will set the stage for our important discussion today. She's a passionate advocate for expanding the national cyber workforce and brought this commitment to the development of the National Cyber Workforce and Education Strategy. I have no doubt that her determination will serve the nation well as the Office of the National Cyber Director leads the implementation of this strategy.

OK, one last thing before we dive in, just a word about FDD. For more than 20 years now, about 22, I guess it is, FDD has operated as a fiercely independent, nonpartisan research institute exclusively focused on national security and foreign policy. As a point of pride and principle, we do not accept foreign government fundings, we never have, we never will. For more on our work, visit our website, FDD.org, follow us on Twitter, @FDD. And that's more than enough for me.

Welcome, Camille.

(APPLAUSE)

STEWART GLOSTER: All right. Thank you for that warm welcome. It's such a pleasure to be here today to talk about the federal workforce. I think a lot of the conversation we've had to date has really focused on the expanse of the national cyber workforce.

I want to start by thanking Mark, FDD, CSC 2.0 for hosting this conversation today, for my colleagues for being on the stage, for Natalie for hosting the conversation.

This work is not new. The federal government, the cyber community, the tech community have been struggling with how to build out a capable workforce for some time now. You have seen federal workforce strategies, federal workforce reports. You've seen commitments to invest in this area. You've seen – many of the strategies you'll probably hear today are things that you have seen explored, seen evangelized, seen put forward as solutions to the challenges we face.

The National Cyber Workforce and Education Strategy, the coming together of the Office of the National Cyber Director, the evolution of the national cyber ecosystem, such that we have public-private collaboration as a core tenet of the work that we are doing, not public-private partnerships, which was that threat indicator sharing that kind of frustrated many of us, but true collaboration that means that the ideation, the execution, the policy development, the implementation has been a group project of sorts, right? We are collaborating on all of that – means that we are at a moment where we actually can see a lot of this move forward.

So we started with a summit where we brought all of us together and have a conversation about, where do we need to invent – invest? What are the challenges? What are the opportunities? Where do we, as the practitioners in this space, as the experts on cyber workforce, on cyber education, on the – cyber ecosystem as a whole, see opportunity and need?

And that catalyzed a series of engagements that landed in the National Cyber Workforce and Education Strategy, which I'm going to assume you all read very thoroughly, so I won't recap the strategy too much, but what I will say is that strategy is very bold in its thinking because it looks across all of the different players in the ecosystem.

We're focused on how we touch every American and what their role is and the skills that they need to be functioning members of society, but also to have the building blocks to be able to move into a cyber career. We focused on the education and training apparatus that supports the agility and the ability for us to meet the changing dynamism of our technological landscape.

This strategy is purposefully technology agnostic because we recognize that the skills that we need today are not the skills that we'll need tomorrow, that they will change, people will need to adapt. And so we want to really focus in on the skills that people need to be able to meet that changing environment, to be able to be proficient in the industry. We focused on the broad national cyber workforce, and then of course, the unique needs of the federal cyber workforce, which we'll discuss today.

One of the things that I want to highlight is the fact that we focused really heavily on implementation, on making sure that not only did we work with you to cultivate a strategy that really identified the challenges and opportunities and the work that needed to be done, that really called upon all of the players in this space to then lead on that work, because to be frank, maybe 40, 50 percent of that is the federal government's work. Some of it – quite a bit of it is from private sector, nonprofit, academia, state and local, or other partners, to make investments in implementation.

But we made sure we had the infrastructure to be able to support the longevity of this work, the investment. We stood up the National Cyber Workforce Coordination Group, which brings together at the assistant secretary level or higher, all of the players across HR, the mission space, finance, to be able to look across all of the work being done at a national level.

But we said that wasn't enough. We also need the same thing on the federal side. How do we make sure that we are really honing in on making the investments that we have all been talking about for some time, as well as the new ones that we identified?

And the best way to do that is to have all of the right players at the table, and to create an environment for collaboration.

You'll see around this room there are a number of players from the –federal government, from different agencies. And on the stage, you will see the ONCD [Office of the National Cyber Director], OMB [Office of Management and Budget], and OPM [Office of Personnel Management] are together leading this work to ensure that all of the right stakeholders, all of the right leaders, all of the right authorities, are brought to bear on these challenges.

And so what I hope that you all see from this discussion, even if you've heard the immediate task before, even if you've seen similar investments, will recognize that we are in a unique moment where that coming together of factors, the right organizations, the public-private partnerships, the clear orientation, the holistic view across the entire national ecosystem, is something we have not seen before and makes for ripe conditions for us to be successful.

So with that, I will turn it over to the illustrious panelists, and to Natalie, to take us away on a deeper dive. Thank you.

(APPLAUSE)

ALMS: Awesome. Thank you so much for articulating the Office of the National Cyber Director's view on why national cyber resilience demands both a robust cyber workforce as well as a general population educated and engaged on these issues. And also, thank you to the Foundation and to CSC 2.0 for having me here to moderate.

And with that, let's dive right in. So as we kick off this discussion, Seeyew, I'm hoping you'll do some level-setting for us a bit. Pillar 4 of this strategy focuses on the federal cyber workforce specifically. So I was hoping you could walk us through sort of in what way the challenges for the federal workforce mirror our broader trends and challenges nationally.

And besides salary, which always comes up, I'm curious what is unique about the challenges in the federal space when it comes to building out that robust cyber workforce?

MO: Thank you so much, Natalie.

I think when we think about people, I think we all – of us are here today because we know that, like, workforce is an important issue. But if you look at the private sector and public sector, by and large sometimes workforce is still an afterthought, right? We care a lot about the next emergency, both companies and the government. We care a lot about somebody is, like, launching new initiatives.

But by and large, when we think about, like, do we – no one is usually, like, you know, at the top, sort of asking the question, “hey, do we have the people to do the work? Do we have people to actually, like – are we building up a plan to make sure that we have enough people to do the work in the long run?" So I think that is a big similarity between – whether it's private sector or public sector, right?

Workforce is important but it's always never the number one issue, which is why it is so important for all three of us to be here today, OPM, OMB, and ONCD, is because we're trying to kind of make sure that the people component is still number one priority in the work that we do. So that's a similarity, right?

But as we all know, the U.S. government is a big government. There are a lot of challenges. You know, some of the stuff that I don't think private sector companies face is the fact that we have all sorts of different authorities and flexibilities that are –either created through guidance's, rulemaking, or by law.

So I think just navigating that in an environment in which technology changes faster than we can train people, in which the skills are constantly changing, I think that's a unique challenge that our federal workforce face in trying to recruit people, right?

And one thing that, you know, you mentioned – the last thing I would say is this. You mentioned that yeah, the money part is, you know, a thing, but, you know, some agencies are able to pay more, right? They have those authorities.

And I would say that a lot of times, we can talk about money or we can talk about mission. I think it's important for us to highlight that some jobs are only available in the federal government. There's huge impact when someone works in the federal government, right? Any decisions that you make can affect hundreds of thousands to millions of people.

So I think, as a federal government, we shouldn't be underselling ourselves by always thinking that, like, money is the component that all the candidates are looking for. I think mission and impact are equally as important, and that is both a unique – that's a unique thing that we have that the private sector might not have.

ALMS: Sure. Yeah.

Mark, let's bring you in. You know, the first white paper you guys did at CSC 2.0 after launching was actually on the federal cyber workforce. So before we get into too many details, I'm curious why you guys started with that issue, despite, as Seeyew said it, not often being the first people – thing that people think about?

MONTGOMERY: Well, thanks, Natalie, and I agree with everything Seeyew said.

The reason we did this is that when we look at cybersecurity, I think most of us understand it's a mix of technology, policy and processes, and people. Inside the federal government, there's been a lot of spending on technology. You know, the DOD [Department of Defense] gets about $13 billion for cybersecurity, non–DOD about $13.4 billion. I mean, that's real money every year.

There's been a slew of policy, whether it's legislative, executive orders, OMB or OPM rulemaking, you know, that has really helped get things smoother.

The one area where I think that there is an opportunity for movement is in personnel, and one other interesting thing is when you think about technology, the private sector is helpful in technology. They develop their own technology that we some – that we buy and bring into our systems.

I don't always find them helpful in personnel. I think they meet with our quality people at meetings and poach NSA, active-duty military, DOD, and .gov workers on occasion. So it's about – that was clearly a place to fix.

And one of the things that really struck us was that – well, I think we have the right group here with Kristy and Jason and Seeyew. This is the group that would –that has a focus on this issue, on the federal cyber workforce.

But the reality is the 101 federal agencies do not prioritize cybersecurity workforce. And you know, my anecdotal statement would be that you know, if the Department of Agriculture had the opportunity to hire a food inspector or an IT administrator and they had money left for one, the Secretary of Agriculture is going to say, "get me that food inspector so I don't have mad cow disease and end up on the front page of the Washington Post," whereas he just – I just think in general, they had this lack of prioritization than those other federal agencies.

So Senator King and Representative Gallagher, when we rack and stack the first five or six issues we're going to attack, put workforce number one.

ALMS: Sure. Yeah, let's bring Kristy in here.

So one more level-setting question, if you guys will humor me, but I'm curious. Obviously, the administration has a focus on workforce issues writ large. So how does the cyber workforce fit into this broader focus? How is it distinct? How is it similar?

DAPHNIS: Absolutely. So as you all have probably read, the President's Management Agenda includes workforce as the number one priority.

Underneath the President's Management Agenda, we have a few different strategies, and the first two strategies in the workforce priority include hiring for simplification purposes, hiring and employee engagement. Those are sort of the first two strategies under there.

We have been working very closely, both OMB and OPM, with ONCD, as Camille had sort of mentioned in her opening remarks, to ensure that this initiative here with ONCD and with the broader federal cyber community really nests alongside those PMA [President's Management Agenda] priorities.

We are a part of the federal workforce. The PMA is broader. The cyber workforce initiative is expansive. And we are thinking about it in terms of how can we get the right people in the room to think about strategic workforce management.

And Jason here leads strategic workforce management with OPM. They're a very strong partner. And we think about how do we get to the point where, as a government, we can think through some of those strategic workforce management issues to really best understand how to use those resources, as Mark mentioned, to do mission delivery?

And cyber and a lot of the occupations within it are mission-critical occupations, and those are the types of occupations that we need to prioritize, that we need to think through, like, how do we put our resources toward that? How do we do pipeline development? How do we get people in the door of the government? So that's sort of how it fits together.

And one of the most important things in sort of the context changing pieces about this Federal Cyber Workforce Working Group and some of the activities that we're prioritizing under it, is to get the right people in the room.

Previously, on a lot of these cyber workforce initiatives or IT workforce initiatives, you might have a group of CIOs [Chief Information Officers], and CISOs [Chief Information Security Officers] talking about it, you know, the Workforce Development Committee of the CIO Council, but you didn't have the CICOs [Chief Information Compliance Officers] in the room and you didn't have the CFOs [Chief Financial Officers] in the room.

So when we went down this path, we got together and we said, "those are – all of these people are important. All of these different angles are important in ensuring that we're aligning on what our priorities are and how do we actually carry them through, how do we actually implement."

So that's kind of how we see it fitting together. So hopefully that helps -

ALMS: That is very helpful.

DAPHNIS: - set the stage..

ALMS: Yeah – yeah. OK.

We're going to go back to Seeyew, and then Jason, I haven't forgotten about you, I promise.

So Seeyew, Kristy was mentioning this working group. So as the strategy outlines, it's in charge of coordinating government-wide efforts. So I'm hoping you could give us a little bit about the implementation efforts. What are some highlights as far as what this group has done so far? And what is coming down the pike?

MO: Yeah, so the Federal Cyber Workforce Working Group, or FCWWG for short, it's a collection of …

ALMS: Sort of for short.

(LAUGHTER)

MO: Yeah, sort of for short. It's a collection of 34 agencies and departments that have equities in federal hiring. And what we have done so far is that we have reviewed an OPM legislation that will be sent to Congress or, you know, in the process of getting done so, but – and also, like, approving the strategy and whatnot.

But the main thing here is to get everyone on the same page and approving things and setting up that infrastructure that Camille was mentioning, right?

The difference between what – look, we're talking about federal personnel 10, 20 years, whatever. The difference now is that are we setting, like, long–lasting infrastructure that can actually make changes? Are we – are you – are we getting everyone together to kind of prioritize some of these initiatives?

That's what the goal of the FCWWG is, and that is to raise the importance of workforce because everyone who is meeting cares about workforce here, and then also have – drive federal cohesion so that we are not just running around doing our own projects, right?

Like, one of the – just to give you a few examples of, like, what FCWWG has done, is that as part of the implementation process, the group is now – we are doing a joint prioritization of one of the initiatives that we want to do in the next year or so, so that when we are signing on, everyone is moving towards, like, the same vision and same target.

We have been supportive of OPM in the Tech to Gov Initiative, right? One of the line of efforts in Pillar 4 is to facilitate transition between public and private sector for workers. Like, how do we make it – how do we make sure that we can kind of make progress on that front?

Now, Tech to Gov, it's a project led by OPM. They have sort of, like, a broader mandate, but we're able to kind of work together with OPM in that process to be supportive of their effort, right? We have subject matter expert – we help recruit subject matter experts for OPM so that they can actually run the Tech to Gov process.

And then our hope is, through those Tech to Gov events that OPM is running, we can figure out eventual long-term process changes that can facilitate more private–public folks who are transitioning from the private sector to the public sector, right?

So that's just an example of how we are supporting the effort for OPM, making progress today, but at the same time, use it as a body to drive long-term changes in a strategic and measured way.

DAPHNIS: If I might just add …

MO: Yes.

DAPHNIS: ... one thing, just about Tech to Gov specifically, this is another good example of sort of where the PMA strategies and the Federal Cyber Workforce Working Group strategies sort of touch, right?

We've been talking a lot in the broader federal space about using tools like pooled hiring and shared certificates which we had gotten approved by Congress several years ago, and how do we make that more the norm when it comes to federal hiring?

And this Tech to Gov is a great example of us encouraging agencies to use it because what it really is, is it's agencies getting together on a few really, really key occupations and working together to do some of that recruitment and to do some of that hiring.

ALMS: Awesome.

Jason, how does OPM fit into this? Curious if you could give me your top sort of lines of effort on cyber workforce?

BARKE: Yeah, I think it's really been – you know, as everybody stated, a great partnership between ONCD and OMB as we start looking at, you know, what a National Cyber Strategy would look like and what roles do we play and you know, how do we impact this kind of – you know, this landscape across the cyber workforce, right?

So we know that, you know, everybody's kind of working towards these goals, and how do we hire cyber people and how do we get the right skills, and how's AI [Artificial Intelligence] fit into this, and what is kind of the long-term, and where are we going?

And so, you know, as we've worked with the ONCD working group and with OMB, we've kind of, you know, helped kind of shape and frame that strategy on where we want to go, you know, and start looking at, you know, well, what is the data telling us? You know, where are we going across there? How do we create kind of this equity across the federal government for, you know, everybody kind of on this level playing field, so that as we start – you know, we're not really competing against each other, maybe we're competing against private sector, but we're able to bring in that talent that we need.

And some of the initiatives that – you know, that have already been mentioned I think are key factors when we start thinking about that and we start thinking about the future and where are we going and you know – and we kind of glossed – you know, Kristy brought up kind of the hiring and the pooled certs and, you know, the efficiency of government and these things that are, like, top on mind for us when we start thinking about, like, skills-based assessments, you know? How are we going out? How are we trying to get the right people in the jobs?

So often we see people that just – you know, JOAs [Job Opportunities Announcement] that have this – these kind of self assessments, go in, and self assess, and then we see thousands of applications coming in and it's a huge burden on our HR specialists.

So how do we start thinking about that next level to really get the targeted quality people in, you know, that have the qualifications into these positions? And how do we start using things like multi–hurdle assessments to take it to that next level?

So we're really focused on kind of that hiring area and how do we improve efficiencies in supporting the initiatives?

ALMS: Awesome. Yeah.

Seeyew mentioned in the strategy there's a commitment for the administration to work with Congress, right, on similar hiring, pay, talent management authorities, as to DOD and DHS [Department of Homeland Security]. So I wouldn't be a good journalist if I didn't ask you, my editor would be extremely mad if I didn't ask if there's any details you'd be willing to share.

I know I talked to the OPM Director last week who said that, you know, this is moving along and we should expect something soon.

BARKE: No, it is. We're really excited. We've been working closely with the cyber community, with our partners at ONCD and OMB, to really think about, you know, where can we make inroads? You know, what would a legislative package look like? And we kind of, like, tackled each area that maybe, you know, separates a little bit of CTMS (Cyber Talent Management Systems) and CES (Cyber Excepted Service), and you know, VA's [U.S. Veterans Affairs Department] got the PACT Act.

And so we're starting to see kind of across the organization where there are special hiring authorities, special incentives. And so we wanted to look at a package that makes sense government-wide so we don't have more pop–up legislation, we don't have more independent, we have one kind of system that fits across government.

And so we feel that this – you know, this package is – really kind of does that, answers a lot of those questions. And so we're excited to kind of see it move forward.

MONTGOMERY: So Natalie, if I could jump in on that?

ALMS: Yeah.

MONTGOMERY: First, I'm excited that OPM is doing this. I think, you know, if you – you know, we had a lot of minor recommendations in our paper, like the FCCWG [sic, FCWWG]and other – a few other acronyms like that – the NCWES – but for us, the Cyber Excepted – a version of a Cyber Excepted Service for the .gov was critical.

You can't have, you know, a hundred federal agencies materially or 80 federal agencies materially disadvantaged versus the other five or six where the congressional committees have taken action.

I was on the Senate Armed Services Committee when we did the Cyber Excepted Service. We thought about it for a long time. It's taken a while. DOD didn't – the workforce didn't flock to it initially. Over time now, it's become much more popular.

And, you know, CTMS was a seven–year pilot program – I would just say seven years to take – if your plane takes seven years to take off from the runway, you'd be a little disturbed, but, you know, it's taken a while. But I think, you know, through patience or just because it took us a while to get here, we're now at that point where we can create these conditions.

And I think there'll be – I think we really need the appropriate federal agency – congressional committees, Oversight in the House and Homeland Security, Government Affairs in the Senate, to take leadership on this and say there will not be 67 solutions from 67 separate subcommittees in Congress. There'll be one solution that embraces the OPM plan if it's appropriate or adjust it if they feel they need to, and gets it across the finish line, because I think that will make it easier for OMB and the appropriators to see how to do this.

And the final thing I'll say is not every federal cyber employee is underpaid, right? It is really, you know, entry level versus mid–career versus senior. It's a different answer at every stage. The skill sets you have, you know, whether you're a cyber-enabled lawyer in that – and there's probably a lot of money. We have to – that's going to cost us a little bit.

On the other hand, some of the basic IT administrators are especially when they're inside the D.C. area and getting a D.C. compensation, are reasonably compensated.

So it is a complex answer to what is – usually seems like a straightforward question.

ALMS: Sure. Yeah?

DAPHNIS: May I offer a bit of perspective on this?

This is one of the reasons why having the Federal Cyber Workforce Working Group has been very helpful, right, because OPM has been working on this legislative package for quite some time.

The typical process would be OPM develops the legislative package, and then they send it to OMB for review, and then it's, like, done. And you might have some equities that are not always fully reflected or worked out as that process goes through.

With this particular piece of legislation, we took a slightly different approach and we spent a few months actually having conversations amongst those 34 agencies to try to come to better consensus before it even got to the point of formal interagency review.

So the hope there is that we were creating a package that, when it does go up to the Hill and – there's buy in from all of the agencies and there isn't as much of a clamoring for those special authorities in different places.

Now, what I will also say is that, like anything else, it's a process and it will take some time to get to a point where this is useful. I mean, it has to get passed, it's a law, right? And it has to be – there has to be regulations to implement it.

So, like, these are parts of the process that we can't necessarily cut off because they're very important to the process. But your point being well taken, that there are things we need to do now – again, another point where some of this interagency collaboration and communication can be helpful because there are a lot of authorities that are already out there that are not always necessarily being fully utilized.

MO: And I would say one thing too. I think based on those experiences of CES and CTMS, I think what we need people to understand is that, like, unlike – it's – unlike introducing technology, I feel like when you're introducing, like, policy that affect people, you know, there's this, like, here's the policy now and then there's rules and then you kind of have to do, like, a round of training of all of the people who are involved.

And you know – so I think there's this lag time, per se, in personnel policy that – you know, that happens when we're talking about people and – and whatnot. I think we kind of have to acknowledge that, knowing full well we're still pushing really hard to make sure that things are implemented as quickly as possible but there is always that lag because when you are, in this case, affecting someone's livelihood, we want to make sure that we are crossing the T's, dotting the I's, and ensure that we can implement the policy in an equitable and sound way.

(CROSSTALK)

DAPHNIS: ... definitely some ways we can fill in those gaps using some of the existing authorities that we already have.

MONTGOMERY: Unstated in that was that the thing that kills a lot of OMB – White House legislation are federal agencies going behind their back to the congressional committees of concern and saying don't do this. So that's why you need the FCWWG and other acronyms to come together and agree that this is reasonably ...

DAPHNIS: We should have thought the acronyms through a little better.

(LAUGHTER)

MONTGOMERY: Yeah, it's OK. I think ours was worse. It was like six letters instead of five. But, you know, the – my point is that you have to get everybody on board because if you don't, you know, particularly – I won't name names – but I mean, there are federal agencies that are very effective in using their committees of jurisdiction to kill legislation.

ALMS: Sure.

(CROSSTALK)

BARKE: Well we were excited about that, you know, as we did and we worked with the group and we started getting, you know, some informal comments and some formal comments, we were able to kind of really adjudicate those and really have some conversations with some of those more powerful agencies that I think – that have very specifics and said, well, what does this mean and how do we – how are we going to implement this? And we were able to craft some legislation, I think, that really made sense for the majority of government and for the majority of those agencies. I would say that it was a very smooth process and a good process as we went through this, so.

ALMS: Great. One follow–up before we move on to something else. Mark alluded to sort of the struggles DOD and DHS had with these similar excepted service capabilities getting off the ground. Is that something on y'all's radar? And, like, why are we doing this, even though those had some struggles? I'm sure you have an answer. So, yeah.

DAPHNIS: Absolutely. I think we saw those other systems and the process around them as a real learning opportunity. And I know that as OPM was crafting this package, they were looking at how some of that played out. I mean, OPM has been a phenomenal partner with all agencies in thinking about how do you bridge some of that more technical HR stuff with the strategic needs of the government?

And they were really looking at it through that lens to say, OK, here's what worked in CTMS, here's what didn't. Here's what we could do better. You know, here's how this looks in a manner that, you know, can scale across government. Like, those sorts of things.

ALMS: Awesome. Fair enough.

I wanted to ask about another bigger idea in the ether here. Mark, CSC 2.0 proposed a federal cyber development institute a while back. That appeared in the strategy as well. So I wanted to start with you, asking why you suggested that at CSC 2.0, and then go to Seeyew to ask where we are on that idea?

MONTGOMERY: Thanks. So originally, when we were thinking of it, Laura Bate and I –and other people have thought of this, we're not the only ones.

ALMS: Yeah.

MONTGOMERY: We were thinking about a mid–career development institute. In other words, how do we help people who were hired on as GS [General Schedule] 6s or 7s with a certain certification and now they're – want to compete for a GS 10 or 11 or mid–career job.

And what we found is – and even publicly, federal citizens would say “my best hiring approach is to meet a talented person at another federal agency and poach him.” I think the Commerce one said it out loud in in a panel. And that's obviously not the best thing for the federal government.

And a – I'm all for movement between federal agencies, which is a whole separate issue that we ought to discuss, but for – we needed something for mid–career management development. But then, when we went to the precursor group, to the WWNCG [sic, FCWWG], whatever it is, which was a group of federal CISOs, HR people kind of talking together, they mentioned, “hey, we also need a front-end piece to kind of, like, help recruit, help make sure that we get –the new employee is baselined and right sized. Also, help us get a more diverse workforce by being able to offer some of the initial certification and training at the front end.”

DOD has used this and NSA have used it very specifically. But our idea was like a two–to–three–month federal onboarding, basically, in cyber that would – you'd have a guaranteed job at the back end but you'd get that – the certification, some experience, get your placement, and then later in career, four or five years later, you could come back for mid-career development, that next level certification.

And the government would be involved in you getting it, whether it's like in the military, where there's a commitment after we help, you know, pay for your certification, but a lot of this could be online delivered. You could also be doing your interim secret clearance during it, which would shorten that timeframe as well, you know, in that four or five-month process.

And then finally, the aspect that we got in, and it was from talking to people and watching a couple of HR hiring processes, which were very eye-opening, that was at the HR people, the human relations, talent management people – federal agencies are not all cyber experts. I mean, that would be generous. And it's frankly – at a small agency, they're probably really good at their small agency specialty. They were. They were not so good as they broke open the nice NIST list. That's the nice is actually a word, now not an acronym, but from the National Institute of Standards and Technology is a list of 57 jobs, but each one has 15 or 17 specialty codes aligned to that job.

Well, knowing which one was really important, which one wasn't. There's a whole psychology into how people respond to questions on this, that also knocked down diversity – so – in the federal workforce.

So the idea of training talent management people, just a one-week class within this institute – so the idea is if there's an institute, I think OPM is the natural home for it. There's legislation out there now for OPM to do this. You know, it's moving it's not on the floor yet of the House or Senate but there's – in a very bipartisan way, people's – you know, Republicans like Senator Mike Rounds, and then Democrats like Representative Ro Khanna, so a pretty good split there.

But both seeing the value and having OPM lead this kind of effort to, like, you know, better recruit, kind of right size, develop, and then retain the federal cybersecurity workforce, I think this is an idea that has value, but OPM is going to have to be the one that turns an idea into a process that works.

ALMS: Sure. Seeyew?

MO: I would just jump ...

ALMS: Yeah, tell me.

MO: I think that that's the status, right? The status is it requires legislation. And, you know, it's working through the process.

I would say that, you know, when we were developing the strategy, we thought that the Federal Cyber Workforce Development Institute, it's a good approach, one of the good approach, that we will – we can use to respond to the demand for a highly skilled cyber workforce in the federal government.

I think in the meantime, the – we – ONCD, through the working group, is looking for ways to actually fill the gaps right now. So recently, like, almost every week now, we have about an hour of training on HR professionals to kind of prep somebody's HR professional to support the Tech to Gov Initiative, right?

So, we are – we're actively, essentially, without a program structure, because that's sort of – like, you know, requires legislation, but we are supporting a lot of the ideas behind it, is that, like, you know, how do we make sure that HR professionals know to hire cyber folks so that – and we're providing training through OPM's coordination, to kind of support that as a trial run. It's where we're at right now.

DAPHNIS: Yeah, the other thing – the other thing I would add to that is not only are we trying to think about how do we train up some of our HR folks, we're also trying to think about things like how do we assess candidates …

MO: Yeah.

DAPHNIS: … right? And that's not even – when you get to the HR professionals, it's like do we have the right assessment tools that lead to the right kind of outcomes and what are – what do those assessment tools look like? Whether they be, like, human-based or whether they be more automated, because you can take a lot of those concepts in integrated into some of the assessment of candidates.

Also, the other thing that we have done through the PMA and elsewhere is created agency talent teams. Now, those talent teams are used in different ways, in different agencies, but that's another place where we see some agencies using those talent teams to help shore up some of those mission-critical needs, like IT workforce and cyber workforce.

MONTGOMERY: And I'm glad you mentioned assessment because that's one of the most – if we had a development institute, there's a minimum skills assessment to get into it, but what you would find is people who were in a good STEM high school program are probably going to be artificially higher on that. But after two months of this, if you – when you redo the assessment and see where a young woman or man stands at that point, they may well be able to get into a different, higher job.

And you can – two or three months of government training, this is what we've learned in the military and – what are called C Schools and A Schools, the way we train military personnel – is that we – the military can uncover the skill, you know, the quality of the woman or man who's a worker in an area, in a way that just a high school degree doesn't or a GED does – it doesn't.

And so I think this really will give us a more diverse workforce in the harder – in the harder to get jobs. And you know, when you look at the 57 jobs in the NIST list, or the 73 jobs in DOD's Cyber Workforce Framework, you know, you want to have a distribution across that as well of women and men and, you know, across all aspects of diversity.

So I really think there's opportunity in this and it's going to give us a better workforce over time.

DAPHNIS: Absolutely. And I did not mean to suggest that the assessments would replace something like that, but just more thinking through, like, how do we get the right kind of candidates in the door?

BARKE: Oh, you know, we've definitely been supportive of that. You know, we just recently released, you know, some guidance on skills-based assessments, and how do we do that and how do we work through that?

And I think there's still some challenges out there and I think agencies are still trying to figure out the best way to develop skills assessments, and then how do we implement those, and then how do we validate those and how do we make sure that they're rigorous and we're getting the candidates that we need?

But I think as a community – and this is something, you know, that ONCD has been working on, as their workgroup – is how do we think of this as a community? Is there a way to share assessments? Is there a way to create repositories of assessments, where we're looking at the same work roles, the same occupations, and we're assessing the same way?

But I think that, you know, we need to continue to develop that, we need to continue to move forward. We're seeing some agencies are piloting this in very limited fashions. But as a whole, I think, you know, from an ONCD – from – sorry, not an ONCD – but from a cyber standpoint, we really need to figure out how we could do this on an economy of scale, at an enterprise-wide level, to really be efficient and really figure out how do we develop these assessments? Who's developing them? And then how do we create this repository?

MO: And that's – I would jump in, right, sort of, like, to pull in all this conversation together, which is what makes this work exciting for me, is that we're really looking into this as like a pipeline of people, right?

So we've – if you look at all this conversation, we're attacking – essentially, it's a pipeline question. We're attacking it from different angles, right? We're attacking it from, like, the assessment angle, we're talking about, like, how do you broaden the funnel so that more people can come in? How do we assess? How do we train? You know, there is, you know, work around, like, even, like, position description. How do we make sure that, like, position descriptions are shareable among all the interagency so that we have – we use the same common position description that is friendlier and whatnot, right?

ALMS: Yeah.

MO: So you essentially then sort of – now you kind of sort of see, like, with all of this conversation, we're really talking about broadening the pathways, getting more people through the pipeline, and then eventually, like, learning the jobs that we need them to be, which I think – you know, unfortunately there's no one silver bullet, you have to kind of fix a lot of small, little things along this pipeline, which is why we need – kind of need everyone together to kind of work, and we – as we triage and fix, triage, and fix all these different parts of the process.

MONTGOMERY: I'm so glad that Seeyew's excited about this because he doesn't know that cyber workforce is the one issue the rest of the White House said, "Not it," you know, when they were giving – when they were handing out jobs. So I'm glad you're excited, Seeyew.

(LAUGHTER)

ALMS: Yeah. You guys are skirting around one of my questions, which means that I have good questions.

Jason, it seems to me you guys are talking a lot about skills–based hiring, right? So could we make sure for anyone uninitiated in the room or online that they know what that is? And then could you give us sort of the lowdown on what OPM is doing overall on this? And I guess it's particularly relevant for cyber, so.

BARKE: Yeah, I mean, I think we've talked a lot about today.

ALMS: Yeah, we have.

BARKE: … you know, it's – you know, so kind of how I started earlier, right? We want to have – we want to be able to have assessments that are testing the skills of people, right? So if we're going out and we want to be able to hire and we want to be able to reach people that have those skills, may not have the college degree, and may not have the work experience, but have those skills that they can come in and they can contribute right away, and they can do the job, how do we do that?

How do we do that beyond what I mentioned earlier, just a JOA that is a self-assessment, right, where somebody goes in and self-assesses themselves, and now you have thousands of applicants and the HR specialist has to try to go through – has to try to decipher who really has those skills that can do the job. Then – now we start having an assessment that goes to that next level.

OK, maybe that is the first hurdle – we go in, we do our self-assessment, but now we've kind of, like you know, reviewed, gotten that down to maybe more of a manageable number, and now we have a second assessment that has very specific – could be technical questions around the job, how do you do it, then now starts narrowing it to a very small, highly qualified group so that a manager now that gets that knows that everybody on that list can do that job, is qualified, and allows them to really get more targeted on who they're hiring.

And so that's our vision. That's what we've been working towards. That's – you know, I mentioned the guidance that came out. A lot of the Tech to Gov stuff's been already mentioned and how we're doing that, the pooled search, the shared certs, bringing in SMEs [Subject Matter Experts] to kind of do this work and help us with this work.

I think, you know, the next step is – you know, what – we were just having that discussion – is a more wider, broader, or – skills-based assessments that are out there that agencies can use, and how do they do that? How do they develop that?

You know, it's – we also know it's limited resources, right? Agencies are, you know, trying to figure out how they're using their resources, and how do we build assessments? And maybe, you know, a broader step is a pool of assessments somewhere that is funded that we could use that we know are certified or are qualified, and then we can start bringing people in.

But we know that there's – you know, I've been talking to a bunch of agencies – you know, CISA, VA, some of the other agencies – that are starting to do these kind of assessments and they're having good results from them and it's really working for them and they're being able to share, and now they've done an assessment, now they can share through pooled certs or through shared certs qualified applicants amongst either their agency or amongst other agencies.

So we're really starting to become much more efficient on how we're hiring.

ALMS: Cool.

MO: I'll jump in. I think, like, I'll I'm not going to talk about the technical detail part that Jason covered. I would just say, like, from ONCD's standpoint, skill-based hiring, skill-based assessment is sort of like ingrained strategy itself, right? If you think about the three imperatives that we have for the strategy, the first imperative is we have too small of a pool of people right now who can do the job, and we keep hiring them away from each other.

So the first thing that we need to do is we need to dramatically expand the people who would want to do the job, right? So if you think about it that way, as, like, "OK, so now we have a bunch of people, then what do we do with them next?"

The next thing is, "Well, let's train them with skills." So, that's why the – that is the second imperative, is to make sure that cyber skills are accessible to everyone that we're bringing in, regardless of where they are in their career.

If they're K–12 students, great, there's some way to do it. If they're post–secondary situation in their learning either college or community college, or they want to do certifications in boot camp, what can we do? If they're like a mid–career transition person, if they're a veteran, what do we do, right?

So I feel like the skills component part is the part that was, like, "Hey, we get all these people, we get them with skills, and then finally, we have the last imperative." And that is the – what we call the public–private collaboration, which is the ecosystem approach.

In this case, is that what we're asking the question is – I actually don't know whether training doctors in cyber or getting a cyber person to work in, like, healthcare is the solution, but I feel like the sector itself, the ecosystem itself, would understand that.

So I think in this case, the through thread of all these three imperatives is the idea of, like, skills, right? Getting people to learn – getting people to want to learn new skills, getting people to learn the skills eventually, and then, like, getting folks to actually accept those skills as sort of, like, the currency.

So, you know, I think that's sort of, like, a basic principle that we have in our strategy, and I truly believe that if we do it right, the federal government, because of our scale, if we do skill–based hiring right, we can really send a good signal to the private sector of how to go about it, because we have the scale to make the changes that others just have to follow.

ALMS: Awesome. OK.

Kristy, I wanted to ask you, you know, someone here mentioned budget. I feel like that's an eternal panel question. So I'm curious, you know, how that looks here. You know, how is it working to align budget proposals with the things that cost money in this workforce strategy?

DAPHNIS: Yeah, I mean, I think the elephant in the room is that agency budgets are very tight. And in all of our conversations, both within our Cyber Workforce Working Group, as well as within the broader budget ecosystems, recognize that agencies have to really prioritize and make sometimes very difficult decisions.

I think what we encourage agencies to do is to be very thoughtful about those decisions. The example that Mark mentioned about do we want a food inspector or do we want an IT specialist? I mean, I think those are things that agencies have to work through as they develop their budget submissions to OMB, as they develop their own budget, and as they figure out, you know, how are they going to spend the resources that they have.

And that's where it becomes critically, critically important around the workforce to be doing this strategic workforce management and to have a very, very strong human capital operating plan, to make sure that agency leadership is really well informed and well aligned on what some of the needs are, and the real realities of what it means if we don't have the cyber workforce or the IT workforce that we need.

I think, in general, across the government, we have to get better about communicating that and not in a “Oh, my gosh, the sky is falling” sort of way but in a real way, where we're linking these types of positions, which are very expansive to the mission delivery.

So that's – I know it's a little bit of a non–answer answer but it's truly the way that we need to think about it, right? We have to think about, like, how do we build this in to what we're doing and how do we make that the norm as we think about our broader workforce?

MONTGOMERY: So I'll jump in and try to – from outside the government, I can be more answerable.

(LAUGHTER)

The – I'll say the – first, I would say I suspect if I looked at the 100 federal agencies' budgets over the last 20 years, 2,000 budgets, very few have been kicked back for lack of cybersecurity investment if the name of the federal agency didn't include “cyber” in it, like Cyber Command or CISA, Cyber Infrastructure Security Agency.

I think two things are going to help improve that. One, OMB Director Shalanda Young and Chris Inglis at the time, the National Cyber Director, signed a deal where the ONC – the – one of the Deputy ONCDs is a dual–hatted – Chris DeRusha, the federal CISO.

The second is the decision – as – ONCD, in fact, it's in the law that they'd have – you know, that they would do budget – that they would look at the budget and work with OMB on it, and the selection of Drenan Dudley to be the Deputy National Cyber Director leading that. She comes from the Senate Appropriations Committee, working with Ms. Young, you know, able to – has a very good understanding of federal budgets.

Now, look, that's the big budget issue of all 101 federal agencies, but the workforce is a part of that. And I'm comfortable that, in the first review pass back that happens this year with that system set up, there'll be a few federal agencies to get a bell ringer, that “hey, you didn't put enough into this,” and some of that might be workforce, some of it will be other presidential priorities where the President said do something and the – you know, the CFO of the federal agency decided that the Cabinet member had a higher priority, you know, and it gets resolved by OMB in the right way.

So I – I'm – but I actually – I hope the second year, the FY '26 pass back, the majority of federal agencies get a bell ringer, that you're not spending enough on cybersecurity in these areas, or you're not meeting the President's goal on this initiative in cybersecurity. And there, I really hope workforce comes home.

So to me, I think there's two positive trend lines that are going to drive success. But I do have to look back on 20 years of consistent not success – and you can interpret that word another way if you want – to say we need to watch this carefully.

DAPHNIS: Well – and, you know, it's the communication of, like, this isn't just about, you know, do you have, I don't know, some technical cyber system thing installed on your = systems, but how are you integrating some of the workforce conversation into that broader investment strategy, right?

And that's why it's critically, critically important to have not just CIOs and CISOs in the room, but also CICOs and CFOs right, because then you can start to pull that together to think about, OK, where is the technical investment most important, and then where do we need to kind of amp up our look around – you know, what kind of people we need, what kind of skills we need? And, you know, how do you sort of integrate that within the rest of the – essentially, what is the agency's, you know, operating budget and not their, you know, capital kind of investment?

MO: And we're still doing the annual memo. OMB, ONCD is still doing the annual memo. We did the second year this time around earlier this year, and then it will continue forward. It's my understanding, so.

ALMS: Sure. Yeah, I'd imagine data is part of this. You're talking about, like, making a case for your needs and stuff.

Jason, I know at OPM, you guys have built out a cyber workforce data dashboard. I've looked at it. So I'm curious, you know, if you could tell us about it, what it's meant to do, and is it having the effects that you were hoping it would?

BARKE: Yeah, thank you. We're really excited about that. Hopefully, everybody's out there seen it – opm.gov\data, our data portal. So I'll just – a little plug out there. But we have a number of dashboards out there and we really feel that this is kind of the direction that we want to go to be able to kind of be transparent in our data.

We know that under the commission's report, you know, they asked us to be more transparent about data. We've been working with the community and ONCD on how do we provide this data? We've been collecting this data back under the Federal Cyber Workforce Accountability Assessment Act. We had to go through. We coded all of our occupations.

So all of the occupations had been coded at cyber. So they feed into those dashboards, those two dashboards. There's a public-facing dashboard that's out on the site I just mentioned, it's really more high – level, aggregate view. People can go in and they can kind of get an understanding of what the cyber workforce looks like, where we are.

And then there's more of a agency look that only agencies have access to that gets much more granular look that really talks about how we're doing in these certain areas with each work role, with occupations. Where's the – where are the work roles? What occupations are they in? Who's doing it? What is our hiring look like? What does our separations look like? What's our retirement look like? What is our demographics like? So all this kind of workforce data that we look at, that really has not been available previously on the cyber workforce.

And so we've really gotten some, I think, good feedback from the agencies on the importance of this data. We're continuing to kind of update the dashboard as we get more feedback, but I think there's been a lot of use.

There's always been an interest in comparing and benchmarking and how many, you know, work roles do you have in certain areas? How many do we have similar missions, similar occupations? How are we doing? How is your sessions? How is your time to hire going on some of these things? So that they're able to collaborate, they're able to work together, maybe on like positions – we talked about shared certs – maybe there's a work role that's out there, you know, that we're looking at a shared cert under the Tech to Gov? How do we kind of come together and use this data to really inform our build our workforce planning?

So that was really an intent. I think that it's meeting that intent. We're excited about it. And so far, the response has been good.

MONTGOMERY: You know, I'd say, you know, we looked at data. It's one of the three Ds for us – there's a lack of data, lack of diversity and lack of dough, you know, kind of …

(LAUGHTER)

And, you know, this data one hurts. Look, we had a Federal Cybersecurity Workforce Assessment Act, as – as Jason mentioned, 2015. I would say agencies were non-compliant, would be the right word. A handful did – you know, place like VA, DOD – well, DOD exempts itself from everything – but VA, a few others would play along.

But the reality is many didn't, you know, a handful gave good data, handful gave bad data, and a lot gave no data. There was not good congressional oversight. I think OPM probably missed some opportunities there for oversight. And as a result, we didn't have it. And in fact, the act expired last December, December '22.

And, you know, we – so we think we need to get this back. We need good data. You know, I think senators Hassan and Cornyn have a federal work – everything's almost the same name – Cyber Workforce Expansion Act. And the very, very last line is just adjust 2022 to 2027 on that Assessment Act.

ALMS: Sure.

MONTGOMERY: You know, probably more could be done to that bill, although that's – that kind of minimum – minimalist approach is good.

One thing I'd say about data is that without good data, it's very hard. And I questioned some of the federal agencies. I think if they have 60 – if they're short 60 of a certain type of IT administrator, they will not advertise 60 jobs simultaneously. I think we all know that there's a reason, in terms of what they have to set aside and budget and other things, that they wouldn't do that. As a result, we kind of have a false sense.

I would bet that if I went to OPM and said, how short are we in the federal cybersecurity workforce, I might get an answer, like, five or seven percent, but if I went to the actual cybersecurity workforce and said, how short are we, they'd say, hey, like the rest of the country, between 25 and 33 percent.

That delta is driven by the fact that we can't have this high–quality data without going directly to open jobs, which is a hard thing for the federal agencies to get around. And I understand why, you know, the strictures of policy and budgeting make that. But without good data, it's very hard to get great solutions.

ALMS: Jason ...

MO: But ONCD, as a response to that – like, you know, that's – it's line of – line of effort 3.1.2 in a strategy for those who are tracking. We are, because of how important having good data is, we – ONCD is hosting a workshop tomorrow with public and private sector experts to kind of brainstorm a path forward and how to get better data.

It's the first step, I know, just yet another meeting, but it is trying – we're trying to elevate the topic and the issue, we're trying to make sure that it's socialized so that it's in the collective consciousness that we need better data.

So we are hosting an event tomorrow at the White House to talk about cyber workforce data to ...

ALMS: There you go. Yeah.

MO: In response to all of this request for better data, yeah.

(CROSS–TALK)

ALMS: Jason, you're either lucky or unlucky that it's time for a question and answer. So if anyone in the audience has burning questions that I'm not asking, I know we have a mic and we would love to hear them.

I think we have one over there.

WATERMAN: Yeah. Shaun Waterman from *Newsweek*. What is the – what are the consequences if we fail at this? What – and what – what's happening now because it's not being – it's not been done yet? And what are the – what would the consequences be if we fail at it?

And how do you sort of frame it in terms of a – you know, the global kind of competition around technology leadership that the US is currently sort of locked into?

MONTGOMERY: I'll take a first whack just because I'm outside the government. I'd say the consequences are really serious. First, look, I get DOD is the number one thing under attack. And we've kind of not talked a lot about them, because I think they're in a slightly better position. But don't worry, the .gov is right behind them.

I mean, SolarWinds was a 15–month ass-kicking of the .gov, right, by the Russian SVR Intelligence Group. Part of that is not – if you don't have the right technology, the right policies and processes, and the right people, all three of them working in an integrated fashion – just having one or two of them is not enough, you have to have all three – you are vulnerable.

And look, there are bad guys coming after our systems – Russian, Chinese, North Korean, Iranian, nation states, but also a lot of criminal activity. Almost – you know, a good percentage of us in the – in this room had our data stolen by the Chinese and – between 2014 and 2015, our personal data, our fingerprints, polygraph results, things like that. I mean, it was a bad day for the government, or a bad year and a half for the government in that case.

Not having enough people on site, not having enough people setting compliance standards, not having enough people do assessments of systems, leaves you more vulnerable, and vulnerability leads to loss.

And so the answer is it's a very significant national security issue. That's why cybersecurity has not escaped the national security oversight and why the workforce inside cybersecurity is an integral part of that.

MO: The only thing I would add, without going into the scary stuff that Mark just mentioned, is that I think we need to remember, like, the people deliver federal services, right? Like, you know, Americans benefit from federal services when American – federal workers deliver them.

So if you can get – if we can't train the workers or if you don't have the workers, then we can't deliver the services that we promised the American people.

So, you know, like, there's all this “attack” stuff, but there's also, like, stuff to just make things work. And then we always ought to remember, like, this is also an opportunity for a lot more Americans to actually, like, benefit from these jobs that are, like, you know, well paying, and many of them, according to cybercareers.gov, do not require college degrees right now.

MONTGOMERY: And one other thing I'd mentioned is cybersecurity is also about preventing fraud on government networks.

MO: Yeah.

MONTGOMERY: And there's a – we've learned from the PPP (Paycheck Protection Program) money that went out that there's fraud. We see it in Medicare and – and other programs, and there is a percentage of fraud. The IRS has a kick ass clawback team that's out there.

I mean, there are a surprising number of cybersecurity-enabled programs that are out there protecting our taxpayer funds, and we need to make sure – you know, that's an equally important part of this, as well as the day-to-day maintenance of the .gov and the federal networks.

ALMS: All right, if ...

BARKE: No, go ahead.

ALMS: All right. Any other questions out there?

LIVESAY: So Seeyew, you talked about how skills-based hiring within the federal government can send signals to the private sector about how to do that effectively. Given that this is also sort of a competitive process with the private sector, I'm curious if you could elaborate more on how that relationship works?

MO: Well, I think it's through – like, you know, we are one of the biggest employers in the country, right? So I'm thinking in terms of, like, federal contracting, if we are making a lot of changes to the contracting process, to make sure that, you know, folks without four–year college degrees but with the skills are able to kind of, like, you know, do those jobs, or if we are hiring a lot of this talent that is currently not being utilized by the private sector, then we kind of get a competitive advantage at getting some of these people.

So I think the private sector will have to respond because we can hire that many more people as a single employer. I think that's how I think, like, the market of skill, the economics of scale is what is the difference here, is the number of people that we can kind of compete and hire.

MONTGOMERY: I also think the government is good for establishing – for helping baseline properly, what is the percentage of, like, your cybersecurity workforce that has to be college educated? I think the government is sitting in about the right number on 26 percent and – somewhere – if I could – I think that's what I got from your strategy. I think private sector is more in the 40 percent thing.

We heard it a little bit – our DFARS [Defense Federal Acquisition Regulation Supplement] contract – our defense contracting, push it, you know, has some old stale language in it …

MO: Yeah.

MONTGOMERY: … or is interpreted that way that causes defense contractors to require graduate – undergrad to graduate degrees for their workforce, supporting a government job that may, in fact, be managed by a non–college degree person. So there's things there.

And then the other thing we do that we, the federal government, does well is, like, there's programs like Scholarship for Service and the Cybersecurity Scholarship Program at DOD that build – and the NSA Center of Excellence program – that builds cybersecurity programs at – between which program I talked about – 100 and 400 universities, the cybersecurity programs that become the baseline that other – you – that the private sector sends their kids through – or their men and women go through as well to get their degrees.

So I think the government can be a great partner to the private sector in this. But one of the ones is the private sector probably needs to take a good look at what percentage of cybersecurity professionals need that college degree versus needing, as was mentioned, by Kristy and Jason, skills-based requirements, driven by standards for us or NICE/NIST or DOD Cyber Workforce Framework, but could be something else in the private sector.

ALMS: Anything else to add panelists? If not, we'll – all right. Other questions? We have one in the front here. Thanks.

ROBERTI: Thank you. So we've talked a lot about the human and – importantly. So is there – well, we talked very briefly about AI at the beginning. But are there – where do you see – and this is for any of the panelists – leveraging emerging AI tools to be able to bridge some of the gaps that you have in the government side for workers? And then separately is, you know, to what extent does that eliminate the need for certain workers? Thank you.

MO: I – I'll just jump in and say – I will just take the first crack at this, and then you guys can jump in.

So I think the – when we develop – developed the National Cyber Workforce and Education Strategy, we thought about that question. And that's why to – sort of the outcome that we want is a – like, a dynamic workforce, right?

It's, like, a – that's why we focused on foundational cyber skills, that's why we kind of focus on, like, hey, we can't quite predict what cyber job would be five years, 10 years from now. So what can we do to make sure that folks are equipped with the skills to do the jobs of the future?

One particular example that I have seen, and this is early days, is that I've known some companies that are trying out using generative AI to help sort of, like, entry level analysts to ask better questions and take the next steps.

So I think I see more of it as how do we actually, in this case, like, increase productivity, using it as a – more like a training tool, like a companion tool, to actually get all these entry level folks trained up faster and get them deployed quicker.

It's one exciting way that I thought would be good for the industry as a whole because now we are both deploying a new technology and also getting people trained quicker and getting them some guidance so that we sort of, like, rapidly scale up the workforce.

MONTGOMERY: So I – I'd say on that I think machine learning has already – in the anomalous activity detection, already had that impact over the last five to seven years, and driven that.

So we've seen some that impact. I think generative AI may have some, but I think because machine learning was there already allowing you to develop anomalous activity detection tools that were faster than, you know, the kid working around the network on his own, looking for something unusual, and the speed of the adversary is such that – because they're operating in an automated environment, that I think we already experienced some of that likely reduction or savings. AI may provide a little more on top of that, but lots of AI have been around in this area for 10 and 15 years – not the same as generative AI, which I think, you know, hit us all in the face last November.

But, you know – so from my perspective, I don't know that it's going to create a lot of jobs savings, but I do love the idea of building better training products, building support products for the workforce. I think there's a lot to be said with that.

ALMS: All right. Well, unfortunately, we're nearing the end of our discussion. So, I want to give each of you guys a second for a last closing thought. How about we just go down the line. Jason, any final thoughts?

BARKE: I really appreciate the conversation that we had today. Really some good perspectives. I think, you know, when we think about it at the end, it's how do we attract, recruit, hire, retain the cyber people that we need?

There's been a lot of talk about a lot of different strategies, a lot of different ways that we're doing this. But at the end of the day, I mean, the first question that came is, you know, what does this mean? What's the consequences, right? We need to be able to protect our infrastructures, we need to be able to protect our systems, we need to be able to protect against everything that Mark and Seeyew and Kristy talked about.

And to do that, we need to get the right people in place and we need to use everything – all the tools and resources that are available to us. We need to have good data, we need to think about the resources, the skills-based hiring. We need to think about the pilots like Tech to Gov, where we're really seeing an interest in the federal government. How do we become that employer of choice? How do we bring people to the federal government? We know there's an interest.

And I think that we need to, as a community, continue to do that, continue to think about how we move this forward, and how we make sure that we have all those processes and the people and everything in place to continue this work.

DAPHNIS: Yeah, I would ditto what Jason just said. I would also offer, you know, in some cases, we just need to get it – get out of our own way, right? We need to use what's there and just do it.

(APPLAUSE)

DAPHNIS: Right? So I think we – there's a lot of work to do. We have a lot of progress that needs to be made. But the conditions right now are right, as Camille sort of alluded to in her opening remarks. So now we just got to do it.

MO: Yeah. I guess I'll add to that. In front of my boss, Camille, here, I would say we're going to focus on implementation, right? And that might not be the sexiest or most exciting announcement of big programs or whatever but we are focused on implementation. It's a lot of, like, small things that we have to fix along the way to actually, like, increase the bandwidth, and that's what we're going to do.

And I appreciate the opportunity to share some of the ideas that we're thinking about. And I encourage you, if you have any ideas, let us know. If you work for an agency in departments, make sure that they understand that workforce is important and increase the priority of – join the FCWWG. We're always looking for more people to help us do the work.

MONTGOMERY: Well, thanks. I – you know, I really appreciate that Acting National Cyber Director Kemba Walden, Camille, Seeyew, have been working as hard. I mean, this is what Senator King and Representative Langevin thought would happen with ONCD on this sort of issue. And I appreciate that Kristy and Jason represented offices that are going to have to work to get this done.

I do think the big things we mentioned though today – development institute, data collection, required data collection, a cyber excepted service outside of the .mil, whatever we end up calling it exactly – those will require congressional support.

And Congress is going to have to look at this, and as they normally do in a bipartisan way, not confuse this with some problem they have with disinformation in CISA or something like that, and understand that these issues have to be addressed, they have to be corrected. And if they make – if they pass a law today, OPM will be affecting it two years from now and we'll be experiencing the benefit three to four years from now.

So every day that they delay after today, you're extending that solution – that possible solution from three or four years from now to sometime even farther in the distance. So incremental things are great, we've got to push them, but we need to get those substantive measures done over this legislative cycle.

ALMS: All right. Well, as much as I think at least I could talk about this all day, I think we're at time. So thank you to Camille for her remarks, for her leadership on this stuff. Thank you to our panelists, as well, for sharing your expertise and your time this afternoon.

And finally, thank you to everyone in this room, watching online for joining us for the conversation.

Take care, everyone.

(APPLAUSE)

END