Ramona Schindelheim, WorkingNation editor-in-chief:

You are listening to Work in Progress. I'm Ramona Schindelheim, editor-in-chief of WorkingNation. Work in Progress explores the rapidly changing workplace through conversations with innovators, educators and decision-makers, people with solutions to today's workforce challenges.

For companies and government agencies across the country, the demand for AI and cybersecurity skills is insatiable. US employers posted nearly 200,000 jobs requiring AI skills in the past 12 months and the World Economic Forum predicts demand for AI and machine learning specialists will grow 40% worldwide over the next five years. The demand for roles in cybersecurity is even stronger with more than 400,000 jobs posted. Both these areas point to employers need for talent that can analyze data. This week at the ASU+GSV Summit, Google Cloud announced two new certificate courses in cybersecurity and data analytics and a course in generative AI to help connect talent to in-demand tech jobs across industries and sectors.

This curriculum is designed to prepare learners for in-demand cloud roles in data analytics, cybersecurity software development, systems operations and more. It was developed through a public-private partnership between Google and the US Department of Treasury. I spoke with two of the leaders behind this venture, Todd Conklin with the Treasury Cybersecurity Office and MK Palmore, chief information security officer for Google Cloud. Palmore says these new certificates are offered free of charge to give more people a pathway to enter this field, including career changers and those without a college degree.

MK Palmore, Google Cloud chief information security officer:

Generative AI is dominating topic today among technologists and cybersecurity practitioners, so that's the leading cert that's come out, but we also have a complementary cybersecurity and data analytics cert along with those, and it's a growing field in terms of certifications that we've weighed into because we realize the value of providing certifications to folks as a bit of a, not just a pathway, but a shortened pathway in some ways. But at the same time, it provides substantive guidance, advice and skill levels that will help people at least initially enter these growing fields of technology and explore the possibility of a career there.

It tells the potential employer a couple of things, and I know this from my own practical experience. So I've been now in the cybersecurity field for better than a decade. I did not get my undergraduate degree in cybersecurity or computer science, but what I did at the time that I was employed by the federal government was that I was one of the individuals who sort of weighed into this territory and my employer, quite frankly, through certifications, provided a certain level of training and opportunity to me through the certification process.

And when you couple certifications along with practical experience, you are stating to an employer that not only can you grasp the academic portion of the work, but that you've shown the ability to then apply that work in a real state and that is as good in some cases as any degree, especially if you can show a significant amount of practical experience along with those certifications. I'm a big believer in the certification pathway and capability because I use it myself and I tell folks that as long as you are willing to do the work, in other words, apply yourself, the certifications will give you that starting point.

But when you look for post-certification, how do you leverage this new capability or knowledge that you have? You have to get some application, you have to apply it, and then when you combine the two of those, it makes you a pretty formidable candidate.

Ramona Schindelheim, WorkingNation editor-in-chief:

Last year, the Biden administration issued an executive order outlining a broad vision for the AI and cybersecurity workforce, then started the process to create new pipelines for government agencies to recruit new talent. Conklin explains why there's such an urgent need for AI, cybersecurity and data analytics professionals now, especially in the government.

Todd Conklin, U.S. Department of the Treasury chief AI officer & deputy assistant secretary of cyber:

Part of what I tried to do at Treasury going back seven or eight years ago was begin our first modernization effort, which included a heavy cloud footprint and that led us to Google AWS and Microsoft of course. And now we run a multi-hybrid cloud environment that required a workforce that had specific cloud expertise, which our historic workforce obviously because we didn't run cloud systems, so that was an obvious gap there. And to me, the foundation of AI development for most organizations, there's some exceptions, is really cloud. So once you get the cloud place down, you put your data in particular data lake structures and you're able to really innovate from there.

And that's really at a really high elementary level. That's been the treasury model over the last 10 years and we try to upskill our workforce that we already had. I think the difference with this, especially the Google partnership, is it offers us a new pipeline that enables us to be a little bit more competitive with the Silicon Valley type enterprises. And I think if you're on the West Coast, if you're in the Midwest, I think you gravitate towards probably the technology firms more so than the public sector and US government agencies.

And I want to leverage this as an opportunity to present the reality that you can have a really great career in public service and also work on innovative things like cloud and AI. And I think that message gets lost. We are a great opportunity if you want to be innovative. We have nearly a hundred AI use cases in development right now across Treasury alone. So it's a really exciting time to be in the government and you can have both public service and be passionate about what you're doing in your day-to-day job.

So it's not a bureaucratic position. Historically, the thought was you had to take a step backwards technologically if you wanted to go into the government. Now the opposite's true. A lot of great innovation is happening in the government and it's an opportunity for you to actually serve as fuel for your career if you wanted to. So many of my staff are going on to private sector positions at a very senior level, and it's part of that process of being able to be innovative within the government. So pretty exciting time.

Ramona Schindelheim, WorkingNation editor-in-chief:

Conklin explains why he hopes the US government will benefit from new cybersecurity talent created through this partnership.

Todd Conklin, U.S. Department of the Treasury chief AI officer & deputy assistant secretary of cyber:

People I don't think realize this, but Treasury ultimately serves as the bank for the US government and we process a significant amount of payments on behalf of US citizens on a daily basis, which rivals our largest financial institution. So effectively, Treasury itself and there's infrastructure parts of it, operate as a global bank to some degree. So there's that aspect. In addition to the broader national security Treasury mission, which I historically was part of where we do anti-money laundering, we do sanctions work, a lot of enforcement activities, all of that is done under the Treasury, IT enterprise umbrella.

Which if you do join us, if you go through, for example, this Google program where we try to match your skills, we created two specific courses that are oriented towards what we're trying to do at Treasury. If you go through those programs and if that qualifies you for at least an interview with us, then it's an opportunity for you to really open up the doors of the national security apparatus to you in a more direct way. And we're trying to get access to a much more diverse pool of employees and then also geographically diverse pool of employees. I want to break us out of the cycle of recruiting just from inside the beltway, as we call it in DC.

It's a broad range of opportunities at Treasury in the cyberspace. So we have general policy specialists that are more on the cyber policy, more kind of academic side that focus a lot on how do we bolster standards. Then you have a regulatory oversight side of Treasury that is an opportunity to actually help in the process of evaluating financial sector systems and promoting best practice for the sector. And then you actually have the hands-on IT, potential track of actually being a person who is the first line of defense from a cybersecurity specialist perspective.

And then you also then have the more advanced data analytics cadre, which is where a lot of our AI use cases are coming out of. So there's a whole range in spectrum that we're trying to have a diverse enough workforce that could bounce across all of those spectrums to have a really robust background. It almost kind of trains them for a chief risk officer type position, even more so than just a cyber hands-on keyboard. But anyway, to focus on the exact effort with Google, we're prioritizing cloud security skills and focusing on in the initial courses, three specific areas around typical gaps that you see in firewall protection.

In general, gaps in how you would scan for vulnerabilities across your whole enterprise, and then also within the data buckets themselves, how you architect around potential issues and vulnerabilities. So those are the three core areas that we're focusing on in the first two modules, just to get sensitized to, first of all, what the NIST risk management framework looks like, how that then correlates with Google's security portals and offerings, and then how you actually apply that in a hands-on way. So we're trying to blend that high-level policy of risk management framework with actually how you implement it in the Google Cloud system. So it's pretty neat course.

Ramona Schindelheim, WorkingNation editor-in-chief:

That certification curriculum according to Palmore, gives new professionals or even career changers practical skills they'll need in the field.

MK Palmore, Google Cloud chief information security officer:

So what you learn in any of the certs that we provide are the skills necessary to get you that baseline entry into a field. Everything in technology has foundational core components and elements. What we try and do in the certification space is infuse those foundational capabilities and skills into the cert so that at the end of that process, person gaining the certification has at least the foundational skills to get started in any one particular area. Our cybersecurity cert, which we launched quite some time ago. Essentially readies a person for entry-level cybersecurity jobs as a potential security operations analyst.

Security operations is the core fabric or content, I call it the heartbeat of any functioning security apparatus. So you literally learn the skills necessary to triage alerts. You may learn some simple coding associated with conducting queries or searches of datasets, compiling information, putting it in a structured way so that you can then relay its importance and impact to the enterprise to others who might be interested in that kind of information. And you're giving some level of ability to assess the information yourself because that's a key component of any functioning cybersecurity apparatus as well.

So it varies from cert to cert. In the generative AI certification, you have to assume that the information that's going to be provided isn't necessarily going to propel you into capabilities of say, developing through coding your own generative AI models, but you got to start with the basics. Generative AI is a new versioning field, although Google has done a lot of the deep innovative work here, there's still a need to level set everyone on exactly what this technology is, expose you to some of the use cases that we've seen across the board, and then as an individual you get to think about, how can I deploy?

How could I leverage this technology into making the enterprise that I'm working for better? Individual exploration into it in terms of determining how it might impact your life. It's always about providing those foundational skills and then subsequently applying those skills in practice so that you can then... The canvas then opens up exponentially in terms of what you have available to you.

Ramona Schindelheim, WorkingNation editor-in-chief:

Both Conklin and Palmore explain this public-private partnership might work to close the skills gap and meet the growing need for cybersecurity in the US Treasury Department and Homeland Security.

MK Palmore, Google Cloud chief information security officer:

There's the outward solicitation to the government, "Hey, we need your help in doing this." The government certainly recognizes the problem, they did when I was an executive in the government. They recognize that there's an issue, and I think this is one of those areas like some of the other critical problems we faced as a society that only public and private partnerships can really bring together the necessary resources and provide those resources to a potential workforce so that we can then welcome them and provide them with an entryway into the workforce in a solid fashion.

So it seems like a natural mesh to me because again, if you look back historically, all of the major problems that we faced as a society, when you put together the resources of the private sector and you bring the immense resources of the US federal government to bear on those problems along with the private sector, there's no problem that we can't solve, but it takes that intentionality to do that.

Todd Conklin, U.S. Department of the Treasury chief AI officer & deputy assistant secretary of cyber:

I would say it's the mission that would attract people, so people who want to help support national security, people who want to be part of the public good, who want to use their skills and their brain power and their experience to promote US national security and the strength and health of the US economy. So that's kind of track one of the typical type of profile of a person who may be even be interested in Treasury. But what I'm trying to do is expand beyond that into what's historically been the tech track of people who would go towards Silicon Valley, who are more attracted to innovation and entrepreneurial spirit type organizations.

We're trying to make it clear that you can have that attitude and mentality and be successful and have a good career that you'll enjoy at Treasury because we're offering a lot of entrepreneurial opportunities for employees at the entry level coming in the door. So can you sustain your family? Definitely, yes. So I think we've been mindful within the cybersecurity space over the last decade to try as much as possible, obviously with limitations, to try to close that income gap that exists between us and the broader Silicon Valley.

Ultimately, we're not going to completely match obviously dollar for dollar, but then you factor in the ability to be entrepreneurial and then also support national security. It is a really compelling package that I think is ultimately competitive when you start to factor in those other things that just go beyond purely compensation and maybe stock offerings.

Ramona Schindelheim, WorkingNation editor-in-chief:

These jobs are not just nine to five and people who choose to go to work for the US government don't have to do so in Washington DC.

Todd Conklin, U.S. Department of the Treasury chief AI officer & deputy assistant secretary of cyber:

With my specific part of Treasury, we pushed out remote first positions and one of the first hires that we brought in under that program is actually someone who lives in California. He visits us maybe twice a year for meetings on the East Coast. I think that's a great example of exactly the target base that we're going after is people across the country from Midwest to West coast who historically thought, "Well, I don't want to move my whole family across the country. Can I access these jobs?" The answer is yes now, which I think is a great opportunity for not just in prospective employees across the country, but for the US government and US Treasury.

I've been trying to be forward leaning in that approach to make sure that we do spread out our workforce, and frankly, it helps us. From a cybersecurity perspective, the adversary doesn't turn the lights out at 6:00 PM when we all walk out of the building. It's always 9:00 PM on Friday that the worst things happen. So having people across the time zones is actually extremely helpful from an incident response perspective, and that's something we've been very purposeful to do. Obviously we can't move our whole entire staff across the country. That's not going to happen.

There's still going to be a core nucleus that has to operate from DC and that's for logical reasons, but there is a significant benefit to being remote.

Ramona Schindelheim, WorkingNation editor-in-chief:

Both Conklin and Palmore emphasized that the skills taught in this certification course are not only for government jobs, they can translate to companies with a need for cybersecurity, which is in fact just about any company.

MK Palmore, Google Cloud chief information security officer:

Every business today, especially global businesses with a technology footprint, all have a cybersecurity apparatus. If they don't have one internally in the organization, they outsource those capabilities to some other organization because at the end of the day, they have to protect their digital assets. The cybersecurity workforce challenge fluctuates year to year, but the numbers have always been enormous. There have been years in the past decade where globally the workforce challenge and the gap in cybersecurity professionals has been as much as a million and a half people.

The numbers here in the US fluctuate anywhere from 450,000 to one year there were 750,000 open positions in terms of cybersecurity. And so when you think about numbers of that immense size, again, public-private partnerships, providing people with the technology piece, providing people with the connectivity to potential employers, giving them practical skill sets that they can use and leverage in order to gain entry with those employers. It's all part of a recipe for success, but everybody has to be playing in this.

Again, Google's part in this is to, with our deep bench of cybersecurity leaders, practitioners, our generative AI leaders and specialists, we can pull together some pretty impressive training and capabilities and we want to be in a position to deliver that widely. Especially and of course to the available workforce, but also we want to bring folks into this who maybe don't have a natural path into cybersecurity and technology. And so in that manner, we're talking about a much more diverse workforce where we're bringing in women, underserved communities, of course the veteran population.

Everybody has an opportunity to get in here and to learn and then to prepare themselves for potential career in the technology space.

Todd Conklin, U.S. Department of the Treasury chief AI officer & deputy assistant secretary of cyber:

We are trying to broaden the pool. We can help equip you with the tools you need through this program to come in the door and be successful that go beyond the typical college career track education. And we could train a broad group of people who have an interest in these areas and a passion and a work ethic. We could give them the tools and skills by being innovative through these types of programs that will help them get in the door. So it is another avenue to help get in the door, at least for an interview, and discussion. It's not going to guarantee a job, but it offers a nice competitive balance for someone who's on the outside who maybe doesn't have a specific degree.

Or for people who are trying to move across various functions who do have a degree in something maybe unrelated, who maybe is just a little bit scared because they're not an engineer, so they don't think they could do the cyber world. And that's the beauty of some of the first courses we curated. They really walk you step by step so that you can do this. Everyone can do this. We're trying to demystify the cybersecurity workforce, but we still have a significant gap in the number of jobs that are available versus the number of people who either have an interest or are qualified to do those.

Ramona Schindelheim, WorkingNation editor-in-chief:

For people who do have an interest in these jobs. Palmore explains how they can learn more about the Google Certificate program.

MK Palmore, Google Cloud chief information security officer:

Grow with Google has an externally facing website. They can Google the term Grow with Google's certificates, and they will certainly be taken to the area that will take them down the pathway to apply to take these certificates. We are also, by the way, partnering with a numerous amount of nonprofits in the cybersecurity workforce space, and there are a number of ways that folks ultimately will have access to this kind of material.

The nonprofits also act as an additional arm in terms of being able to deliver these capabilities, and we are quite open to working with employers, as you know that there's a consortium of employers who will now look at these certificate graduates as possible employees. So there's a whole system and ecosystem that has been curated to support this ongoing effort.

Ramona Schindelheim, WorkingNation editor-in-chief:

That was MK Palmore, Chief Information Security Officer at Google Cloud and Todd Conklin, Deputy Assistant Secretary for the US Treasury's Office of Cybersecurity and Critical Infrastructure Protection. They spoke with me about the new Google Certificate courses in cybersecurity and data analytics and training in generative AI. A project launched with the US government to help develop talent for in-demand tech jobs across all sectors. I'm Ramona Schindelheim, editor-in-chief of WorkingNation. Thank you for listening.