GRANTS OFFICE
empowering communities

Fortify Your Frontlines: Funding Cybersecurity with the State and Local Cybersecurity Grant Program and Beyond

Webinar Transcript • May 6, 2025

Presented by Michael Paddock, Amanda Day, and Sam Rawdon (Grants Office) • With Matt Singleton and Debbi Blyth (CrowdStrike)

Sponsored by CrowdStrike • Grants Office, LLC

Welcome and Introductions

Michael Paddock:

Hello, everyone, and welcome to "Fortify Your Frontlines: Funding Cybersecurity with the State and Local Cybersecurity Grant Program, or SLCGP, and Beyond." I'm Michael Paddock, CEO of Grants Office, and I want to welcome everyone to today's session. We've got a great session for you today on the increasingly talked-about topic of cybersecurity, and we're very happy to have our sponsor CrowdStrike with us today. Thanks to CrowdStrike for making it possible for us to bring you this information, and we've also got some great presenters from CrowdStrike, as we'll talk about.

Housekeeping

Michael Paddock:

Before we get started, we've got a few housekeeping items for you. First of all, as many of you know, you can listen hands-free over your computer speakers or headphones. There's no need to dial in by phone, but if you do become disconnected from your speakers or headphones, you can always go to the audio and video menu at the top of your screen. If you're not seeing the audio and video menu at the top of your screen, look for the show menu bar — that should bring up the audio and video menu to find alternative ways to connect to the audio portion of today's session.

If you miss big portions of it, don't worry. The session is being recorded, and the replay will be available, ostensibly where you registered for today's session, but also Kate will be putting into the chat the location where you can find the replay and the slides and other helpful resources as you're beginning your cybersecurity funding journey. So all of that will be available to you.

You can ask questions at any time using the question and answer interface at the bottom right-hand corner of your screen. Again, if you don't have a question and answer interface there, go to the three dots at the very bottom right and click on Q&A — that should open the window for questions and

answers. Send in as many questions as you'd like, and we'll get to as many as we can again at the end of today's session.

Today's Speakers and Agenda

Michael Paddock:
We're talking about funding cybersecurity with the SLCGP program and beyond. We're going to talk about a CrowdStrike cybersecurity threat report, so we'll get a sense of what is the landscape that we're looking at. We'll talk about cybersecurity funding — what exactly are we securing ourselves against? And then we'll talk about the cybersecurity funding landscape: funding for local and tribal governments, for K-12, some thoughts on justifying your cybersecurity needs. And then we'll talk more about CrowdStrike solutions to a lot of these issues before we get into the Q&A.

To talk about all these things, I'm joined by a fantastic panel of knowledgeable experts. We've got Matt Singleton, Executive Strategist for CrowdStrike, Debbi Blyth, Executive Strategist for CrowdStrike. We've also got Amanda Day, Grants Development Consultant here at Grants Office, and Sam Rawdon, Grants Development Associate here at Grants Office. So I couldn't imagine a better panel to really shed light on both the issue of cybersecurity as well as some of the funding opportunities that are available to support your cybersecurity initiatives. With that, let's start with the CrowdStrike global threat report. I'm going to turn it over to Matt Singleton. Matt?

The CrowdStrike Global Threat Landscape

Matt Singleton:
Awesome. Thank you, Michael. Really appreciate you having us on today. We're going to hit just a few things to orient us around the threat landscape before we dive into the grants conversation. I've got just a few slides — I promise I'm not going to geek completely out on you, but I do want to walk through what we're seeing.

The Cost of a Data Breach

Matt Singleton:
This first slide is a data point that I used quite a bit prior to joining CrowdStrike, when I was the Chief Information Security Officer for the State of Oklahoma. I used the Ponemon report, which transitioned to the IBM report, around the cost of a data breach quite often in that role, and it's one of the reports that I stay on top of even after my transition to CrowdStrike. This is an interesting thing to use for kind of building that burning platform around cybersecurity, but it also gives you some great visibility into the primary attack vector.

You can see it there in the purple banner — we're up to 292 days for a dwell time based off of stolen credentials, which has become the primary attack vector that the Ponemon and IBM Institutes have identified in their 2024 report. The other thing I'll call out here is the average cost per record. It's $173 per record breached. I call this out specifically because this is something that I used as I was negotiating third-party contracts at the state. A lot of times you had to try to identify some sort of a common metric that could be used, and most organizations agreed that the Ponemon and IBM reports get you in the ballpark to understand what the liability might need to be for individual contracts.

The 2024 Global Threat Report: The Enterprising Adversary

Matt Singleton:
As we transition over to the 2024 Global Threat Report from CrowdStrike, you all know that this is one we've been publishing every single year, and 2025 is no different. This is the premier threat intelligence report in the industry, and every year the report has a theme. This year's theme is the enterprising adversary, and we chose this based off of what we're seeing our adversaries doing. Over the last few years, organizations have gotten really good at protecting their core enterprise assets, really managing those assets and getting better visibility on them. Our adversaries are having to come up with new and enterprising avenues to achieve their endeavors. So this seemed like an appropriate theme for this year's report.

Voice Phishing, Access Brokers, and Breakout Time

Matt Singleton:
Jumping into the next slide, we'll start looking at actual metrics. I'll take a really high-level view of the global threat report. The very last slide we have in my section is a QR code to download the report directly. I encourage you to do that. I know it's always weird when you're talking to cybersecurity folks about using QR codes — I promise this one's safe. You can also obviously google it and find a direct link yourself, but I encourage you to dig into it because we're just going to scratch the surface today.

Year over year, we've seen a 442% increase in voice phishing activities. This takes the form of what you've probably heard about in terms of bad actors contacting the help desk and impersonating individuals with elevated privileges, convincing the help desk to reset passwords and MFA tokens. But there's also the other side of that coin where the help desk is calling in users. There are some interesting case studies in the global threat report — I encourage you to look specifically around Curly Spider, where we actually observed an adversary who identified the target and did what we call spam bombing, where they sent hundreds of spam emails to that individual's inbox in a short amount of time, and then contacted them by phone shortly thereafter and said, “Hey, I noticed there's something weird going on with your account. We probably need to do something about that.” And basic human nature — the individual said, “Yep, let's fix this. I've seen what you're talking about, can't keep this going on, so let's fix

it.” The adversary convinced the user to give them access remotely, they downloaded some malware, started creating credentials. All of this happened within the span of about four minutes. Again, our adversaries are moving very quickly.

We've also seen a 50% increase in access broker activity. Those of you who have been tracking the report for a while now — the access brokers are those individuals who specialize in breaching usernames and credentials and posting those on the dark web for sale. We've been tracking individual unique advertisements and have seen a 50% increase year over year.

The last thing I'll call out is lateral movement. Breakout time is something we've tracked for years. In 2018, the time from when an adversary would get access to your environment to the time they would do bad things was almost 10 hours. Every year since then we've seen significant decreases in the breakout time. You can see on the screen here, 51 seconds is the fastest that we've seen last year, but the average is just under 48 minutes now. Again, our adversaries are moving very quickly and improving their sophistication.

Social Engineering and Generative AI

Matt Singleton:
On the next slide, we'll dive a little bit deeper into the social engineering aspects. There are some really interesting things happening around the impersonation of IT support — as I mentioned, Curly Spider — but then also using MFA resets to access single sign-on and cloud applications. Adversaries are really moving quickly using social engineering capabilities and actually incorporating generative AI into their exploits.

On the next slide, you'll see what we're talking about with generative AI. You probably heard about the extortion, the transfer of $25.6 million. We had an adversary in Western Africa who actually used generative AI to create a deepfake conference call with a financial firm CEO and convinced — or as the CEO — convinced a financial associate in that firm to actually transfer that money voluntarily. So generative AI is continuing to be something that we're tracking very closely. We're also being able to identify phishing emails that have been created by generative AI versus humans. You can see the stats there looking at the click-through rates: generative AI has gotten pretty good at these phishing emails. 54% are being clicked through, as opposed to 12% offered by humans.

The last thing I'll talk about in terms of generative AI — you may have seen a case study we published the latter half of last year, actually around our Fal.Con event, on Famous Chollima, where a North Korean adversary group has started actually placing human assets within U.S.-based companies. The generative AI portion of this is, as the investigation has continued, we've been able to identify that they're using generative AI capabilities to build out their LinkedIn profiles, to assist them in responding to interview questions. There are some really interesting and scary videos out on the CrowdStrike

website of the actual Zoom interviews for these adversaries interacting with the HR specialists in these companies. You can see how this all plays out.

Chinese Nexus Adversaries

Matt Singleton:
On the next slide, we'll talk a little bit about the expansion of our Chinese nexus adversaries. A 150% across-the-board increase in exploits from China, but specific industries are seeing between 200 and 300% increases. China's gotten very good over the last couple of decades. They've significantly invested in their cyber capabilities, and they're now on par with most of the leading nation cybersecurity capabilities. So something to definitely keep an eye on. They've also gotten to where they're actually specializing. There are adversary groups that are focused on specific industries and doing things like using forward operating bases within the cyber realm to actually launch their attacks, so it's harder to identify where it's coming from.

Cloud-Conscious Adversaries

Matt Singleton:
On the next slide, you'll see that we're talking about cloud-conscious adversaries. This is another one where, a few years ago, our adversaries would kind of stumble into an environment and fumble around a little bit while they figured out what they had and what they could do. Our adversaries have gotten much more specific and much more deliberate in their cloud exploits, so we're seeing a significant increase in cloud-conscious adversary activity — 25% increase just in cloud intrusions overall. But again, identity continues to be a thing. If you remember from the very first slide from the Ponemon Institute, identity is the number one attack vector. 35% of cloud intrusions are using valid credentials now, folks. So it's really important that in addition to securing your identities for on-premise systems, you think about it in terms of your cloud environments as well, and how those interact with your on-premise solutions.

We're also starting to see more cloud-conscious adversaries exploiting the new generative AI and large language model environments that organizations are starting to embrace. If an adversary is looking for intellectual property, these are really interesting targets, because in order to train these models, organizations are uploading a ton of their proprietary information into these cloud environments. Our adversaries are identifying those primarily through the cloud control panel. It's a great one-stop-shop — makes reconnaissance super easy and super fast — and our adversaries are taking advantage of that wherever they can.

Vulnerability Exploits

Matt Singleton:
The next slide: one of the other main things we've seen is vulnerability exploits, and this is nothing new. Most organizations know you need to patch your vulnerabilities. But what we're starting to see is our adversaries are using generative AI to help with reconnaissance and to identify specific targets they should pursue. They're also using it to collect information around vulnerabilities, pointing them to the publicly accessible databases to pull down which tools have vulnerabilities and how to exploit them, and building out new capabilities for their adversary groups as a result.

The other thing they've started doing is — they know that most organizations are prioritizing patching based off of CVSS scores. So a lot of organizations have a policy that says if it's a score of nine or above, I've got to get that patch installed within the next 24 hours; if it's seven or above, maybe it's two weeks. Our adversaries have figured out that if they can daisy-chain a couple of lower priority CVSS scores together, they can accomplish a lot of the same things. So if I take a CVSS score of three for remote access and a CVSS score of four for privilege escalation, all of a sudden I'm off to the races. It's really important that organizations start prioritizing patching based off of what's actively being exploited.

Software-as-a-Service Misconfigurations

Matt Singleton:
The last thing I'll talk about is around software-as-a-service. A lot of organizations think, hey, it's a SaaS offering — I should be good to go, security is taken care of. That's partially true. Part of cybersecurity is understanding the configuration and ensuring that you have the proper controls in place at all times. Our adversaries are starting to identify — really, Office 365, Microsoft 365 environments — they're frequently targeted, and misconfigurations there, especially around the security controls, are making it really easy for our adversaries to get in and do bad things. What we're seeing is a lot of the misconfiguration is done by the administrators for those environments. Maybe they're trying to make it easier to get through, get some of their work done quickly. Maybe they've disabled multi-factor authentication or something along those lines. Our adversaries are absolutely jumping on that. So stronger MFA is essential for software-as-a-service solutions.

That gives you just a quick orientation of the threat landscape as it stands today. I'd encourage you again to go out and download this threat report. I saw Debbi dropped a link to it in the chat as well. Take some time, read through it — a lot of great information here, and know that CrowdStrike is here to help you work through whatever strategies you might need to better secure your environment. Michael, I'll hand it back to you.

The Cybersecurity Funding Landscape

Michael Paddock:
Great, thanks very much, Matt. You handled it pretty fast, but that was a great overview of cybersecurity threats generally and for specific types of platforms. Really appreciate that overview. Now I'm going to turn it over to Amanda Day to start us off talking about the cybersecurity funding landscape. Amanda?

Amanda Day:
Thank you, Michael, and welcome, everybody. Thanks for coming. With these types of threats continuing to rise, it's necessary to implement those cybersecurity measures now, and grants are a great way to help with the cost of those solutions. So we'll start off today with a bit of general cybersecurity funding information, and then I'll get into some specifics of how cybersecurity technology is being funded through state and federal grants, and then Sam will cover a K-12 overview of that grant landscape.

Three Main Sources of Funding

Amanda Day:
Where are these funds coming from? There are three main sources of funding when we talk about grant funding. First, we have money coming straight from the federal government in the form of competitive programs, where applications are submitted directly through the federal government, or as formula grants where funds are directly awarded to states, cities, or counties based on certain criteria like population.

Second are pass-through programs. With these, states are awarded funding that comes from the federal government, and then those funds are passed down to local applicants. Often with these grants, states are able to keep a certain percentage. For example, in SLCGP, states are keeping 20% and passing down 80%. It just depends on the grant program. The state agencies can keep some of that funding for their own cybersecurity needs essentially.

And then the third type is a state-level grant. Think of these as budgets allocated to state-level programs. For example, New York State has its own cybersecurity grant program. Florida had its own cybersecurity grant program. Those funds came right out of the state budget, with revenues coming in from income tax or general taxes on things like cigarettes and gasoline. Those are the three types of funding that are generally available.

Cybersecurity-Focused vs. Cybersecurity-Friendly Grants

Amanda Day:
Within those three types of grants, cybersecurity funding can be split into two distinct categories. First is cybersecurity-focused grants that are specifically targeted at cybersecurity initiatives and provide

financial support to organizations aimed at enhancing cybersecurity measures, resilience, and capabilities. But far more common are grants that are considered technology-friendly or cybersecurity-friendly, meaning the funding agency is motivated to award funds for your project based on a complete and comprehensive idea rather than that specific technology or cybersecurity solution. Think about a Homeland Security project, a public safety project, or a transportation initiative where cybersecurity is a necessary component of that larger goal. Sam will get into a little bit more of the weeds on these two types of grants later, but that's just a general overview.

In the first type — cybersecurity-focused grants — there are limited amounts, but there are funds out there. These grants are created specifically to address cybersecurity needs. At the federal level, as you can see on the slide, the Tribal Cybersecurity Grant Program was created to assist tribal governments with their cybersecurity needs, and the Rural and Municipal Utility Advanced Cybersecurity Grant provides funding to rural electric utility providers to help combat cyber threats in the electric grid. An example of pass-through funding would be the State and Local Cybersecurity Grant Program, which I'll dig deeper into later with information on where that program is and where it's going. This grant is the biggest and most important cybersecurity grant to come from the federal government. It was created in 2021 and has been funded for four years so far. It provides funds to state and local governments for cybersecurity planning, cybersecurity hardware and software, and workforce training, which is really important. Most of the grants you'll see for cybersecurity include workforce training in some manner. Like Matt was saying, a lot of these things are human error — clicking on links or giving credentials away — so workforce training is a big part of these grants.

In addition to those two types, we have state-level programs. Some states have chosen to fund their own. New York and Massachusetts have their own, and South Dakota is in the initial stages of creating its own program. They're setting aside $7 million for local governments to purchase cybersecurity solutions. It's in the beginning stages, so I'm not surely where they're headed with that, but that's something to consider if you're in South Dakota. Hopefully this is a trend that may continue as federal funding is up in the air, so states may take the initiative to start their own programs as well as taking advantage of those federal funds.

As far as cybersecurity-friendly funding, there are several agencies that include cybersecurity in their grant guidance. The top three by funding amounts are listed here: the Department of Transportation, the Federal Emergency Management Agency, and the Bureau of Justice Assistance, all include cybersecurity as an eligible expense in their guidelines. In addition to those three major funders, there's also supplementary funding allocated for various purposes like election security, water and sewer infrastructure investments, transportation, and broadband initiatives. Really, cybersecurity is part of every sector. So while there are a limited number of cybersecurity-focused grants, there are many grants out there that will fund cybersecurity as part of that larger project.

Building Comprehensive Projects

Amanda Day:
That being said, we have to think about building that more comprehensive, not just cybersecurity-focused project. So what does that look like? The goal is to think about how your cybersecurity needs fit in with that larger project or mission goal. Your organization has a mission-driven effort, so how does cybersecurity fit in with that when you're applying for grants? Technology-friendly grants will absolutely fund cybersecurity as long as you're able to connect the dots back to how cybersecurity is just another tool to help you accomplish your goal of improving your community.

Some examples of the types of projects might be a Homeland Security project — anti-terrorism, emergency management preparedness — election security funds, law enforcement programs like body-worn cameras or ruggedized laptops or in-car cameras. All of these need cybersecurity protections, as sensitive information is at risk from hackers and cybercriminals. Water and sewer infrastructure is now being targeted heavily by hackers and ransomware. They receive funding to improve cybersecurity through grants, and as these systems become increasingly connected through digital technologies, they'll become potential targets for cyberattacks. This is a sector that's becoming increasingly vulnerable to attack.

And finally, public healthcare is another at-risk sector. If you think about this one, we're talking about lives being at risk. Cybersecurity is critical in protecting sensitive patient information, but it's more critical in protecting facilities from ransomware attacks that can result in shutdowns and endanger lives. There are many other areas where cybersecurity is grant-fundable, but these are just a few examples.

Deep Dive: The State and Local Cybersecurity Grant Program (SLCGP)

Amanda Day:

Program Background

Amanda Day:
I want to dig deeper into the State and Local Cybersecurity Grant Program. I'll give a little background of what the program is for those who don't know, and then let you know where we stand and where we're headed. This program was created as part of the Infrastructure Investment and Jobs Act in 2021 under the Biden administration, and it is administered through the Department of Homeland Security and FEMA, in partnership with the Cybersecurity and Infrastructure Security Agency, or CISA. They're overseeing the application process for this program. So if you click on their website, they'll have a lot of good information about the program.

Funding is slated to run four years — fiscal year 2022 through 2025 — but our hope is that this will become a cyclical grant like the other FEMA and DHS grants and will be funded in future years. I really am optimistic that this will be a continuing program, as cybersecurity is not something that is going away or is a one-and-done funding opportunity. As part of the application process, states developed a cybersecurity planning committee, and those committees created a cybersecurity plan for each state. That plan was submitted to CISA for approval, and after the plan was approved in that first year of funding, the state was allocated their funds for fiscal year 2022 and they were able to open their own programs.

Each state has opened its own program in its own time, and as states received their share of the grant money, it's up to them to further divide it at the state and local levels. As I said before, the state can keep up to 20% at the state level for state agencies, and then 80% is passed down to local agencies.

How States Disperse the Funds

Amanda Day:
As far as how those funds are dispersed, there are a few separate ways that each state has chosen to do that. First, actual grant monies can be provided for the applicant to choose and purchase their own cybersecurity provider and products. North Carolina, California, and Kansas have all chosen to go that route. Second, purchases can be made at the state level, and then the state will provide those cybersecurity solutions to eligible applicants. Some states felt that this was a better use of the money, as if you look at it as a bulk purchase, they were able to provide services and training to local governments. States like Colorado, Indiana, and New Jersey all selected CrowdStrike as their partner, providing Falcon Complete and other solutions to local applicants. And the final option is a hybrid model, meaning they could do a combination of both — some grant awards and then products to other applicants based on the technology needs. New Mexico is one of the states that has chosen that hybrid method.

As far as deadlines go, it's all over the map. Each state runs its program completely differently, so some have opened and closed all three years of funding — North Carolina, Kentucky — while others are just now opening up the first year of applications. So it's really just a matter of checking your state's progress to find out where the state is in the process, what the deadlines are, and how to apply. At this point, almost every state has a website dedicated to this program. There are a few that don't have a publicly accessible website, and it's a matter of contacting the state administering agency to see how those funds are accessed.

The Tribal Cybersecurity Grant Program (TCGP)

Amanda Day:
As part of that program, a certain percentage of the State and Local Cybersecurity Grant Program funds were used to create the Tribal Cybersecurity Grant Program that I mentioned earlier. This is a separate

grant, but again it uses funds from SLCGP, so it's generally the same guidance, but specifically created for tribal governments. The availability of funding is based on population size of each tribe, and that is listed in the guidance. There are four separate buckets based on population size.

One thing I do want to note about this program: tribes can apply at their state-level SLCGP program and apply for TCGP, but not for the same project. They can apply for both, but they cannot receive grant funds from both programs for the same project. They would have to choose one award over the other. They can apply for both grants for different projects and keep those award monies for those separate projects. As far as deadlines for this one, tribes applied for funding last January. They combined the first two years of funding for $18.2 million, and this third year they have not announced an application window for this yet, but you can check the FEMA website or the CISA website for deadline information. I don't have a date to give you, so it's just a matter of keeping your ear to the ground and checking those websites regularly.

Where Is the Program Going?

Amanda Day:
We are in the final year, so states will apply for their fiscal year 2025 funds later this year. I'm thinking late summer, early fall. But as I said before, our hope is that this program will continue to be funded through the federal budget in subsequent years. In early April, the U.S. House subcommittee led by Representative Andrew Garbarino held a review of the program with representatives across several areas from the private sector. There was a representative from Utah on the panel. Panelists testified about the program and pointed out what has worked well in their state and what they think could use some improvement, and they answered a lot of questions from lawmakers trying to get a better idea of how well this program has worked and what they could do to improve it. It's a positive sign that the program is being brought to the attention of lawmakers — that gives me hope that this is not going to be ending in 2025. So hopefully we'll find results of this subcommittee in the coming months. I included a link to the meeting recording. It's rather long, but it really did provide a lot of great information and great feedback from those panelists. So if you do get a chance, take a listen. It's a little long, but it's quite interesting.

Other Grants That Fund Cybersecurity

Amanda Day:

Department of Homeland Security Programs

Amanda Day:
While there are a limited number of cybersecurity-focused grants, I did want to highlight some other grants that include cybersecurity funding opportunities in their guidance. It's pretty obvious that the

Department of Homeland Security would be a major funding source, as most of these grants focus on anti-terrorism, emergency preparedness measures, and things like that. So on the right, you'll see a list of all the DHS grants that have that cybersecurity focus on them. The series of Homeland Security grants — the State Homeland Security Program, Tribal Homeland Security Program, Urban Area Security Initiative, Operation Stonegarden, and the Transit Security Program — all fund projects that focus on creating a secure and resilient nation, and that includes cybersecurity in their guidance. Cybersecurity is called out as one of the national priority areas for these grants. So it's definitely an option to look at a Homeland Security project to get cybersecurity funding, and it's a really great resource.

Election Security Grants

Amanda Day:
Next, election security grants. The State Homeland Security Grant actually sets aside 3% of its funds for election security, so that's an option as well. But the HAVA Election Security Grants are formula grants, meaning they are passed directly to states. They were first appropriated in 2018 to enhance election technologies and make election security improvements, and this includes cybersecurity as part of that election security improvement. Funds can be used for cybersecurity improvements as well as physical upgrades such as cameras or door locks. Typically, this is a biannual grant, so every two years funds are allocated to each state, but a total of $15 million was made available this year in the continuing resolution. In most states, the grant is overseen by the Secretary of State or a state elections division. It's just a matter of finding out in your state who is administering these funds and how local applicants can access them.

Utilities, Transportation, and Criminal Justice

Amanda Day:
There's cybersecurity in every area, but some of the main concerns are that it's necessary in transportation, criminal justice, and utilities. If you think about it, it's fundable with any grant that funds technology, because cybersecurity is a necessary component to protect digital systems, networks, and data. Utilities encompasses broadband, water and sewer, the electric grid, and so on. It's critically important for utilities because these systems are foundational to national infrastructure. Utilities like electric, water, gas, and telecommunications form the backbone of modern society. A cyberattack on these services can cause widespread disruption, economic damage, and even loss of life. So cybercriminals are continuously targeting utilities as a possible target for ransomware or just taking over systems to cause harm.

I'll give a quick aside of an example of a potentially harmful attack that I had personal experience with. In Oldsmar, Florida a few years ago, a plant operator saw his cursor being moved around on his computer screen, going to different functions and opening various functions on his computer, and this

hacker boosted the level of sodium hydroxide — which is essentially lye — to a hundred times the normal level. The operator immediately reduced the level back to normal because he was sitting at his desk, but had he not been there, these levels could have caused serious health damage to the public. The state of Florida noted this attack and really took action. They created a state-level cybersecurity grant program in 2022 and 2023 to help combat that type of threat. So this is a perfect example of the kind of damage that can be done if systems are not protected from hackers.

In modern transportation systems, these systems rely heavily on digital technologies that, if compromised, can cause widespread disruption, financial loss, or even endanger lives. Cybersecurity is vital for safety of passengers and operators of these systems and to ensure system integrity and reliability. So the Department of Transportation and the Federal Highway Administration are including a lot of smart technologies into grants, and cybersecurity again is an essential component to some of these grants.

Finally, cybersecurity is also crucial for the justice system because it safeguards the integrity, confidentiality, and availability of sensitive legal processes. Law enforcement and correctional facilities, in addition to judicial systems, often share data. There are a lot of networks that are connected, so a breach in any one part of this can compromise a whole network, making coordinated cybersecurity vital in the criminal justice sector. So I've spoken a lot about what is available for state and local governments and tribal governments, how they can apply for funding for cybersecurity, and how to fit that cybersecurity into that larger project. At this point, I'm going to pass things over to Sam to cover funding for educational institutions and to provide some additional cybersecurity grant guidance. Take it away, Sam.

Cybersecurity Funding for K-12 Schools

Sam Rawdon:
Thank you, Amanda. So with a better understanding of cybersecurity funding as a whole, I would like to shift into cybersecurity funding for the K-12 sector specifically, where over the course of several years it has become crucial for protecting student data, securing district networks, as well as preventing cyberattacks. Luckily, some of the programs Amanda touched on earlier can also assist K-12 schools in strengthening their cyber posture and helping them become more resilient to cyber threats.

The FCC Schools and Libraries Cybersecurity Pilot

Sam Rawdon:
If you live in the K-12 space, many of you are probably familiar with the FCC's Schools and Libraries Cybersecurity Pilot, which leverages about $200 million in unused E-Rate funding specifically for improving network security postures, not only for K-12 schools but libraries as well as consortiums of

both types of agencies. This program is still in its pilot phase, with selected participants announced back in January, but it is designed to explore how Universal Service Fund money, which also funds E-Rate, can support cybersecurity for schools and libraries. The FCC will determine after this three-year pilot period if they will continue to fund this initiative to help cover the costs for many types of cyber solutions and services.

Other Federal Programs for K-12

Sam Rawdon:
K-12 schools can also take advantage of SLCGP to improve their cyber posture as well. Amanda just covered SLCGP quite extensively, so I won't go into too much detail here, but K-12 school districts are most certainly eligible to apply. Programs like the State Homeland Security Program, or SHSP, as well as the Emergency Management Performance Grant, or EMPG, both support efforts to prepare for all kinds of emergencies, which can include cyber threats. Schools can qualify for funding under both of these programs mainly through partnerships with local emergency management agencies or homeland security offices. Both programs can especially be useful if the school is part of a broader regional or city-wide cybersecurity initiative centered on activities like training, planning, and even running simulated cyberattacks or incident responses. The Nonprofit Security Grant Program, or NSGP, can help private or faith-based K-12 schools that are designated as 501(c)(3) tax-exempt by the IRS to enhance their cyber posture against potential threats. So K-12 isn't entirely left out in the cold when it does come to state and federal funding sources.

Mission-Driven Projects, Not Just Tech Upgrades

Sam Rawdon:
When we do talk about cybersecurity in K-12, it's important to point out that cybersecurity isn't solely a technology issue. It's also a mission-driven priority — part of which Amanda sort of touched on — that can affect student learning as well as their online safety. First, it has to be part of the mission-driven project. It's important to remember that grants are not just funding the hardware or software for the sake of it, but rather approaching it more strategically. So it's important to ask: what are the project's needs and goals? Are you trying to protect student devices for remote learning, or protecting sensitive student information, or even trying to modernize your infrastructure?

Think of how these needs and goals came about, then ask yourself how cybersecurity will support those goals. For example, if you're expanding on one-to-one device initiatives or shifting toward a hybrid or fully online learning environment, cybersecurity is going to be important in making those efforts safe. It's also important to determine the school's current cybersecurity status. Are there firewalls? Are systems being consistently monitored for threats? Are staff and faculty properly trained? Think of how cybersecurity is already utilized in the school's ecosystem to determine needs and goals. And finally,

what are the risks? Conducting a vulnerability assessment is going to be key here in determining what specific risks are currently being faced.

The other side of that coin focuses on how cybersecurity can benefit student learning, because in K-12 it's not solely about the protection — it's also about enabling a safe digital learning environment for students. Cybersecurity concepts can be integrated into the existing curriculum as an innovative way to teach modern skills like problem-solving or critical thinking. Cybersecurity can also promote digital literacy for your remote or hybrid learners through digital citizenship programs, or even increase the scope of teaching and learning efforts to more under-resourced communities. A strong case can also be made centering on the creation of a career pathway in cybersecurity, since it has become such a booming industry. Initiating a career and technical education program or a club centered around cybersecurity can spark interest and lead to true career opportunities. And finally, it can even potentially support dual enrollment initiatives if students are taking college-level courses online in a CTE-related field like cybersecurity or computer science. The bottom line is that cybersecurity for a school is not just about the tech upgrade — it's also about the educational mission. So it is important to ensure that cybersecurity ties into your broader goals, as Amanda mentioned, as well as addressing student outcomes.

K-12 Funding Examples Where Cybersecurity Applies

Sam Rawdon:
With those key points in mind, here are some K-12-specific funding examples where cybersecurity can most certainly apply. Starting with the Distance Learning and Telemedicine Program, or DLT — this program is designed to support rural K-12 schools by expanding distance learning opportunities, often in partnership with colleges or universities. The important part here is that cybersecurity is a critical component of delivering those online learning services safely. So if your school is using DLT funding to support things like virtual classrooms or teleconferencing with partner institutions, you can also include cybersecurity tools and training in your request, because now protecting students and educators who are learning and teaching online has become a fundamental need.

Another example is 21st Century Community Learning Centers, which supports extended learning time opportunities for students attending low-income and low-performing schools, such as implementing after-school or summer programs. These programs can certainly include technology education programs with a cybersecurity focus. So if you want to start an after-school cybersecurity club or incorporate cybersecurity into existing STEM enrichment to reinforce what students are learning during the school day, this program can really help make that happen if it contributes to student learning in those extended-time settings.

Another example is Title V Perkins Career and Technical Education. This program supports building career pathways. So if you're thinking about implementing or expanding a cybersecurity pathway in a high school CTE offering, this funding can be used for things like the technology, but also curriculum, certifications, and even teacher training. Because the focus here is on workforce readiness, investments in cyber infrastructure or instruction can be justified as helping students gain industry-aligned skills. While it won't protect the entire school's network, it does provide students with a separate network to explore and learn on without disrupting regular cyber systems — so it's essentially giving them like a sandbox to play around in. Through these programs, cybersecurity can be supported when it aligns with an education-driven mission like distance learning, extended education, or workforce development.

Justifying Cybersecurity Needs in Grant Applications

Sam Rawdon:
Regardless of whether you're a municipality, a state or local government agency, or a K-12 district, the biggest thing when it comes to cybersecurity funding is being able to justify those needs in an application. Going back to what Amanda spoke to earlier, it's important to remember the two distinct types of cybersecurity grant funding that's out there: those grants that are cyber-focused and then those that are cyber-friendly.

Cyber-focused grants, as Amanda said, are those specifically intended to support initiatives that strengthen an organization's cyber posture. These programs are designed exclusively to facilitate the purchase and implementation of cyber technology — many of which Debbi will get into a little bit later — as well as training programs that build the skills and awareness of personnel responsible for managing or interacting with these technologies. The overarching goal of these grants is to help organizations proactively prevent, detect, and respond to cyber threats by enabling a comprehensive and sustainable cyber strategy. Think of a program like SLCGP. We would consider this grant to be a cyber-focused grant since its main objective is to fund the technology and services necessary to improve an organization's resilience to cyber threats.

Cyber-friendly grants, on the other hand, are those that, while not exclusively focused on cybersecurity, allow for cyber-related expenses to be included as part of a broader project. These grants typically support multifaceted initiatives like infrastructure upgrades, digital modernization, or emergency preparedness, where cybersecurity can be an essential supporting component. In these cases, organizations can use part of the grant for cyber measures like securing new systems or protecting sensitive data. But effectively leveraging these grants requires showing how cybersecurity is going to align with and enhance the overall objectives of a larger project. Thinking of programs like DLT or Perkins that I just mentioned, we would consider these to be cyber-friendly grants, since the technology required plays a role in a much larger mission-driven project that benefits student learning. So while

similar in nature, it is important to clarify these differences, because depending on your project's needs and goals, this will ultimately be a deciding factor as to which sort of grant you would like to pursue.

Grants Fund Comprehensive Projects, Not Just Products

Sam Rawdon:
Keep in mind, ultimately, it's about how the CrowdStrike solution you may be considering aligns with the overall mission of the cyber grant itself and how well it integrates with other elements of the project. Grants typically support comprehensive projects, not just the individual products themselves. This pie chart illustrates how a typical cybersecurity grant budget might be distributed among various components. So while the CrowdStrike technology that you're looking into will be a key part of it, a well-rounded project will also include other necessary parts such as hiring project managers, cybersecurity consultants, or providing training for IT staff or system administrators to effectively implement and manage the solutions.

Tips for Justifying Cybersecurity in Grant Applications

Sam Rawdon:
Before passing things over to Debbi, I'd like to wrap up by focusing on some tips to justify cybersecurity in grants. If you are considering a particularly technology-rich grant such as SLCGP, it's important to keep that bigger picture in mind and not lose the forest through the trees. One of the most important elements of any grant application is presenting a well-articulated needs statement. Simply saying that your organization lacks the modern technology is usually not enough to justify the funding. Instead, funders really want to understand the why, as Amanda touched on before — specifically the societal benefit that that technology will bring. So focus on how cybersecurity is going to help address that underlying challenge. For example, rather than saying our IT staff needs improved endpoint protection, a stronger justification would be: “To strengthen our ability to prevent, detect, and respond to cyber threats targeting sensitive data, we are requesting funding for the deployment of CrowdStrike's endpoint protection and response platform.” This type of needs assessment does more than just request the stuff or the things — it also shows how technology is supporting your goals.

Also consider what additional elements outside of the cybersecurity itself you may need to ensure project success. This might include staff training or consulting services, all of which can be funded together or in tandem with the technology itself. Equally important is involving both the IT team as well as solution vendors like CrowdStrike early and often in the planning process. Their input is going to help ensure the technical accuracy of a grant application as well as increase the likelihood of a successful project. When preparing an application, be sure to save formal quotes from CrowdStrike and any other technology providers. These quotes are often required as attachments and can also help validate your budget estimates. Your IT team and vendor contacts can even help translate technical jargon into clear

and compelling language for your budget narrative, which is something many of us really don't speak fluently. With that, I'm now going to turn things over to Debbi to talk about CrowdStrike solutions. Debbi?

CrowdStrike Solutions

Debbi Blyth:
Alright, very good. Thank you so much for that helpful information. So Gartner says that most organizations have 45 or more security tools, and these siloed security tools really create two major problems. First of all, we see adversaries exploiting security gaps, and they're able to easily hide between disjointed tools like AD, Entra ID, EDR, cloud versus on-prem, and even SaaS apps, as you heard Matt talk about earlier, and all the other tools in your environment. And security teams really struggle with inefficiency. They've got too many tools, too many alerts, too many consoles, perhaps different teams responsible for each tool, and of course manual correlation slows response. CrowdStrike really solves all of this with a unified platform — one platform, one agent, and one console for all capabilities, leaving adversaries with nowhere to hide.

The Falcon Platform

Debbi Blyth:
As a modern endpoint security leader, CrowdStrike is here to help you outpace and outsmart the adversary by giving you complete visibility, allowing you to track the adversary at every step of the way. It also provides AI-powered prevention and detection, which is built into the core of the sensor, and it allows you to detect and stop attacks based on AI and adversary behavior operating in the cloud and locally. It allows you to conduct unified investigations, automatically building a complete picture of an attack with full context and intelligence, with incredibly elegant search for efficient investigations to find stealthy adversaries. And it provides integrated response, allowing you to respond quicker and more intelligently across your entire enterprise with integrated response.

There is also an aspect of precision. You can fine-tune responses with scripts and deploy to individual machines or groups of them, and interact directly with individual machines. And lastly, it's super easy to deploy and operate. The Falcon platform is delivered with a single lightweight agent. It is easy to deploy rapidly, and it's all in the cloud — there is no on-premise infrastructure to maintain.

Unified EDR and XDR

Debbi Blyth:
Most of you know CrowdStrike because of our more than a decade of expertise building the world's most advanced EDR offering, but CrowdStrike continues to innovate and evolve, and that means a

paradigm shift to a completely unified EDR and XDR offering. You can start at the endpoint and then easily activate extended capabilities through XDR to extend visibility and control across all key attack surfaces, unlocking cross-domain detection, investigation, and response across your entire enterprise. This simply allows you to see more, to know more, and to do more across all key domains in one easy-to-use unified command console.

Falcon Insight XDR customers now get 10 GB per day of free third-party data ingestion, with over a hundred one-click connectors with parsers to jumpstart their cross-domain investigations. In addition to supporting native XDR use cases with first-party Falcon data across all CrowdStrike modules, customers can also leverage their existing best-of-breed technologies to augment this visibility and combat sophisticated attacks across all key security domains. If customers wish to exceed this 10 GB per day allowance, a seamless upgrade to the fully featured next-generation SIEM offering is quick and easy.

CrowdStrike brings all of this together into a single unified console, which your team can drill down into attack paths and explore impacted hosts and identities, providing the context that is needed to triage, remediate, and manage security operations with confidence and speed. The CrowdStrike AI-native XDR platform is cybersecurity's AI consolidator, and it's purposely built to stop breaches. It is powered by a single lightweight agent, which collects and integrates data from across the enterprise, including endpoints, cloud workloads, identities, and third-party data sources. By unifying disparate data sets and building conversational AI and automation on top, security teams are able to ask any question of all data and drive automation across the SOC to gain the speed required to beat the modern adversary. The platform consolidates and replaces legacy point products across key areas of security and IT, delivering a unified modern approach that reduces complexity and cost, saves time, and stops the breach.

Free Security Risk Reviews

Debbi Blyth:
Lastly, if you want to get a quick view into your security posture or try some of these capabilities, it's really easy and it costs nothing to get started. CrowdStrike offers three different security risk reviews at no cost to give you visibility where you might be lacking currently and that might help you justify additional controls that are needed or actions you might need to prioritize for remediation. We have an identity security risk review, a cloud security risk review, and something brand new — a SaaS security risk review. You can reach out to your regional sales manager or get started using these QR codes. Thank you so much for your attention. I know we're a little bit over time, so now we're going to open it up for any questions you might have either for the Grants Office or for the CrowdStrike team.

Q&A Session

Michael Paddock:
Great, thanks very much, Debbi — great information there. I really appreciate your contribution. We did have a couple of questions come in. One came in regarding the federal delay on the release of SLCGP funds to some states. I would encourage you to reach out to the Grants Office team directly for information about your state specifically. We also have a living page right off our homepage that's constantly being updated with new information about the various executive orders, the status of various grants, and so on. You can find that right on our website at grantsoffice.com.

Q1: Can grant funds be used for multi-year contracts?

Amanda Day:
That's a good question. That comes up a lot, actually. It depends on the state that is administering the grant. In the case of SLCGP, the state of Texas will fund a one-year contract, but other states, if it's a three-year grant, they will fund three years. The State Homeland Security Program is a three-year grant, so that will fund a three-year contract. But it really is in the guidance for specific grants which grants will fund multi-year contracts and which will not. So it's really a matter of either reading that guidance, and if it doesn't specifically say, reaching out to that program manager and asking that question, because that question does come up a lot when I'm consulting with local governments.

Q2: Will the FCC release another application this year or in the following years for the Schools and Libraries Cybersecurity Pilot?

Sam Rawdon:
Great question, Michael. As of now, the FCC has not announced any plans to open another application window for the Cybersecurity Pilot, not only for this year but also in subsequent years. That initial application period closed back on November 1, and the selected participants were announced back in January. These participants are currently engaged in the program, which spans a three-year term. But given the high demand of over 2,700 applications requesting $3.7 billion in funding, the FCC is likely going to consider the strong interest when they are evaluating the pilot's outcomes and deciding on future funding opportunities. That's a really good question.

Closing

Michael Paddock:
Great. We are out of time, unfortunately, but I want to thank our presenters Matt Singleton, Debbi Blyth, Amanda Day, and Sam Rawdon for sharing your knowledge and insights with us. I did warn everybody that we had a lot of content to cover today. Thanks for sticking with us. A big thanks to our sponsor CrowdStrike for sponsoring today's session and making it possible for us to bring you this

information, and to all of you — really appreciate your participation in today's session. Great questions. I hope you found this a valuable use of your time, and we'll look forward to seeing you again on a future webcast. Have a great day, everybody.

— End of Transcript —

Grants Office, LLC • empowering communities • Recorded May 6, 2025

About This Transcript

This transcript was generated using Webex's automatic caption feature and subsequently reformatted with the assistance of artificial intelligence. While we make every effort to ensure accuracy, errors may remain. If you notice a discrepancy, we welcome your corrections — please reach out to education@grantsoffice.com.

Live sign language interpretation is available upon request for future Grantscast® events. To request an interpreter or learn more about accessibility accommodations, please contact accessibility@grantsoffice.com.