GRANTS OFFICE
empowering communities

Cybersecurity Grant Funding Strategies for Schools, Public Safety, and Government Agencies

Webinar Transcript • August 12, 2025

Hosted by Michael Paddock • Presented by Amanda Day and Sandy Trowbridge • With Katherine Osorio of Check Point • Grants Office, LLC

Sponsored by Check Point

Welcome and Introductions

Michael Paddock:

Hello everyone, and thanks for joining us for Cybersecurity Grant Funding Strategies for Schools, Public Safety, and Government Agencies. 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 cybersecurity funding. Before we get started, I want to thank our sponsor Check Point Public Sector for sponsoring today's session and making it possible for us to bring you this information. Big thanks to Check Point.

Housekeeping

A few housekeeping items for you. As many of you know, you can listen hands-free over your computer speakers or headphones. There's no need to dial in. But if you do become disconnected, you can go to the audio and video menu at the top of your screen to access alternative ways to connect to the audio. If you don't see the audio and video menu at the top of your screen, there's a little “Show Menu Bar” chevron that will drop that down for you.

Also, you can ask questions at any time using the question and answer interface at the bottom right-hand corner of your screen. And again, if you don't see it at the bottom right-hand corner of your screen, just click the three dots and you'll be able to open the Q&A interface that way. Feel free to send in as many questions as you'd like over the course of today's session and we'll get to as many as we can toward the end. We normally save the questions for the end.

The session is being recorded, and the replay will be available at the same place where you registered for today's session. As soon as the session is over, the resources page will come up with the replay from today's session and the slides. That is being placed in the chat by our intrepid GrantsCast producer Kate, and she'll probably be putting that in the chat a couple of times over the course of today's session. So you'll see that come through on the chat in case you don't recall where that might be.

Today's Agenda and Presenters

We are going to be talking about cybersecurity funding. The agenda reflects that. We're going to be starting with a general overview of grant funding just to level-set for everyone, and then we'll get into the landscape of cybersecurity funding and specifically cybersecurity funding for education. Then we'll get into a little bit of the tips and strategies for including cybersecurity in your grant applications. As we know — and I'm sure our team will be talking about this today — with cybersecurity, there are some grants specifically for cybersecurity, and then there's every other technology grant that funds technology that can also fund the security of that technology. So the strategies for including cybersecurity in your grant applications will vary depending on what type of grant you're applying to: whether it's a cybersecurity-focused grant, or just a technology-friendly grant for which you can include cybersecurity as a way of securing the technology you're planning to deploy as part of your project.

We'll talk more about that in terms of strategies, and then we'll get into the Check Point Grant Support Program. Check Point is not just a sponsor of today's session; they also have a grant support program. Grants Office is happy to be working with them on that, and we'll hear more about what that program involves and how to access it. And then, as I mentioned, we'll get to your questions with any time we have remaining.

I'm joined by a great group of panelists today — a very knowledgeable and experienced group who live, eat, and breathe cybersecurity every day. Katherine Osorio is the Strategic Program Manager for Check Point. Amanda Day is a Grants Development Consultant here at Grants Office. And Sandy Trowbridge is a Grants Development Associate here at Grants Office. So, welcome to our presenters. We've got a lot of great content for you today. With that, I'm going to turn it over to Amanda Day to get us started on a grant funding overview. Amanda —

Grant Funding Overview

Amanda Day:
Thank you, Michael. I appreciate that. And welcome, everyone. Thank you for joining us. We do have a lot to go over, so hopefully this information will be very helpful for you in your search for cybersecurity grant funding.

Navigating the Shifting Federal Funding Landscape

First, I want to address the federal funding grant landscape — tips for navigating this shifting landscape. We're really now seeing some grants open from the Department of Homeland Security, Department of Transportation, and Department of Agriculture, but some programs from other agencies are on pause while funding offices review the guidance and ensure that the program priorities align with the current

administration's priorities. We at Grants Office continue to monitor the status of federal grants very closely.

For all of you, keeping tabs on federal grants is very important, because first, grants are not going anywhere. Things shift with each change of administration, so funding will continue to flow to these programs — it's just based on the priorities of the current administration. Again, it will change in four years. These programs are being reviewed, and we are starting to see a little uptick in the release of some of the programs, as a lot of you saw that the Department of Homeland Security grants were all released last week.

In addition to federal programs, there are state-funded programs as well as private foundations. So if that federal grant hasn't opened yet, there are alternatives — you have options. Some states focus on different priorities, so it's a matter of doing your due diligence and keeping up with what these states are releasing in addition to those federal funds that are coming out.

Additionally, make sure you're keeping up with the executive orders from the White House. These contain important information about where this funding is headed, what they're focusing on, and what direction grant funds are going for this cycle. It's also important to stay informed about federal budget processes — they will start talking about the next federal budget in the coming months, so it's really important to keep up with that. It's important for you to keep up with the news and what's going on in the financial world.

Finally, stay motivated. Don't give up the search because there are some delays. Keep that search going. You shouldn't stop because of these delays. Do what you can so your organization is prepared when the grants do open. We'll provide some helpful tips later on in the presentation on how to get your organization grant-ready and how to incorporate cybersecurity in that grant proposal. But really, continue the search for grant funding. It's out there.

Three Main Types of Grant Funding

For those of you who are new to grant funding, there are three main types of grant funding. There's federal government agencies, which provide the most financially to grants, obviously. There are state government agencies. And then there are private foundations, including corporate foundations, community foundations — and individuals sometimes provide funding for foundations. So when you're considering your next steps, it's important to understand the differences between these sources. There are advantages and disadvantages to each type of funding. Determining which type is going to fit your organization and your project needs is very important.

Federal grants are generally the largest amounts since applicants nationwide can apply, but these grants can be extremely competitive and proposal requirements can be pretty lengthy. The grant applications

are time-consuming, but the monetary payout is worth all of the effort. The number of opportunities and the large amounts make them a great option for applying for grant funds.

State agencies or state-funded opportunities tend to be a little less competitive, since it's just the people in your state. The funds tend to be smaller amounts, and it really comes down to your state's budget and priorities. For example, some states may invest heavily in public safety grants, while others will focus on healthcare or education grants. It really depends on the state you're in. Again, keep up with what's going on in your state, sign up for listservs, and check state agency sites to see what grant funding is out there.

And finally, those private funders — examples include corporations, families, and community foundations. These grants range from very small amounts to pretty large amounts in size, and they're just as varied in terms of competitiveness. The application load for foundations tends to be the lightest in terms of these three sources of funding. Sometimes it's a letter of interest; sometimes it's just a short application asking some yes-or-no types of questions. Again, do your research, check what the guidelines are, check what the application process looks like. Generally, these funds are focused on nonprofits and 501(c)(3)s. And while there is some foundation funding out there for public agencies, it's just really not that common. So you'll want to keep your eyes open for any local foundations that may fit with your organization's goals.

Funding Flows: Direct vs. Pass-Through, Competitive vs. Entitlement

Within those types of funding, there are different flows and different types within those grants. Grant funds are either provided directly to organizations as direct grants — you apply to that organization and they directly award funds to you — or there are pass-through grants. An example of a pass-through grant might be a Department of Homeland Security grant like the State Homeland Security Grant, in which the state applies for their allotted amount of funds. Once the state is approved for those funds, they then open a state-level program, and local governments, schools, hospitals would apply to that program to get funds. You'll often hear the term sub-recipient in that case.

Both direct and pass-through grants can involve competitive or entitlement funding. Competitive application processes require scoring each proposal based on a specific set of criteria. Entitlement funding refers to award amounts that are predetermined based on something like population size or poverty levels — they are pre-allocated amounts that the entity would apply to and say, yes, we would like to get these amounts. When the application is approved, those funds are then funneled to that applicant. It's important to understand the differences, as it impacts how you approach applying for grants. The application for entitlement funding is usually a formality, since those funds are already technically allocated. Whereas the application for competitive funding determines whether or not you'd

be awarded based on your proposal, your need, your project, and if it aligns with what the organization is looking to do.

Cybersecurity Funding Landscape

I'm going to cover general cybersecurity funding for local governments, police departments, and the like. Sandy will go more in-depth on education, because education has a lot of differences compared to the kind of funding that I'm going to talk about.

Building a Comprehensive Project Around Cybersecurity

When we think about grant funding for cybersecurity software, cybersecurity hardware, and training, we really have to think about building a more comprehensive project. As Michael was saying, yes, there are a few grants out there to just fund cybersecurity. It's very few and far between. We call them the unicorn grant, because there are very few grants out there developed to fund one thing — a body-worn camera grant or a cybersecurity grant. That brings us to a lot of funding opportunities that are cybersecurity-friendly or technology-friendly grants, where there is a comprehensive project for, say, traffic safety, and part of that project involves cybersecurity for the technology involved. You have to think about it that way when you're looking for cybersecurity funding.

These grants will absolutely fund cybersecurity — those technology-friendly grants — as long as you're able to connect the dots back to how cybersecurity is part of your project, and not the only thing you're looking for funding for. If you're just looking for a firewall, that's not really how it works. You need cybersecurity solutions as part of a comprehensive project.

Some examples are on the screen. Homeland security projects are a really good example, because they include anti-terrorism, and cyber crimes are considered terrorism, emergency preparedness, and election security initiatives. Law enforcement programs like body-worn cameras and ruggedized laptops need cybersecurity protections, as sensitive information is at risk from hackers and cyber criminals. All that information that's going from the camera into the cloud is at risk — we really need to protect all of those systems.

For water and sewer projects, organizations may receive funding to improve cybersecurity for water and sewer. These systems become increasingly connected through digital technologies, and they become potential targets for cyber criminals or ransomware. And finally, public healthcare projects — they're a huge at-risk sector, and you'll see a lot of this in the news. Ransomware is a big problem for public healthcare because they're operating life-saving equipment, and if there is a ransom attack, the hospital has to decide: is this a valid attack? Should we pay the ransom because lives are at risk? It's a different kind of beast when you're talking public healthcare and cybersecurity. It's really important for those facilities to be able to provide cybersecurity for those systems. For telemedicine, keeping that

information confidential is essential. So healthcare is another at-risk sector. They're starting to add cybersecurity as a budget line in healthcare grants, which is a really good sign. There are many other areas that cybersecurity can be a component of, but I wanted to focus on these four because they really show how important cybersecurity is in keeping the public safe and keeping information and human lives safe.

State and Local Cybersecurity Grant Program (SLCGP)

As we said, there are a few grants that focus on cybersecurity. The first is the State and Local Cybersecurity Grant Program. This was released with the Infrastructure Investment and Jobs Act under the Biden administration. It's a four-year program, fiscal year 22 to 25 — we're in the last year. States will apply for their funding by Friday. Again, that's a pass-through grant. They'll apply for their funding, and then the state opens their own program for local governments, school districts, and tribal governments to apply for funds through the state.

This is technically the last year. We're hoping to see in the next budget that this is a continually funded program like the other DHS programs. It's run through DHS and FEMA, like the State Homeland Security Program or Port Security Program. We are hoping that it will be funded. There are people out there fighting for this funding, giving the argument that it's not going to solve itself in four years — that funding just isn't enough. We can see in the next budget round what's going to happen with those funds.

When the funds are passed through, 80% will be passed down to local governments and local applicants. 20% is kept at the state level for state agencies, because they obviously need cybersecurity as well, but 80% will be passed down to local applicants. Every state is going to be different — I can't state that enough. All 50 states run their program differently. Some are doing direct grants; some are providing cybersecurity solutions. It's really important to keep up with what your state is doing and follow their guidance when you're applying. If you go into Grants.gov to look up this grant, it's not going to make any sense to you because it's the state level that's in there. You want to find out what organization in your state is administering these funds — whether it's Homeland Security in your state or Emergency Management in your state — and find out the guidance so that you can apply for those funds. I'm not going to say that they're all going to open after this round of funding, because the dates span the whole year. So really, it's up to you to do the research and find out what your state is doing and what the deadlines look like.

Tribal Cybersecurity Grant Program (TCGP)

The next program is the Tribal Cybersecurity Grant Program. This is actually part of the previous program — funds from SLCGP are funding this program. So this is essentially the same grant but aimed at tribal governments. Tribal governments will apply for funding and receive funds for their

cybersecurity needs. The previous round of funding awards are listed on the FEMA website if you want to take a look. They changed things up a little bit this year — they have select tribes listed on the website that can apply, and that is due August 15th. If a tribe doesn't apply for their funds — if they don't need them or they decide to decline them — then those funds will go back in a pool. Take a look at that guidance. If you have any questions, it's on the FEMA website or the Grants.gov website. You'll hear me say Grants.gov a lot — that is a website to keep up with. Check it every day. All federal programs will be announced through that website.

Homeland Security Grants as Cybersecurity Funding

There is an electric grid cybersecurity grant, but there are just so few cybersecurity-focused grants at the federal level. There are a few at the state level that I'll talk about a little bit later. But obviously, the Homeland Security grants are a really great source for cybersecurity funding. Cybersecurity is one of their priorities and has been for the last couple years. They will fund cybersecurity projects. Again, these are anti-terrorism programs or transit security programs, so the project has to be there and cybersecurity would be a component of that project. There's a series of Homeland Security grants — the State Homeland Security Grant, Tribal Homeland Security, Transit Security, and the Nonprofit Security Grant Program. They will all fund cybersecurity as part of a larger project. These are really, really good options. These open for states to apply for their funding, but each state will have different homeland security and urban area security initiatives, so it varies. Check out the FEMA and DHS websites for more details.

Four Vital Areas Where Cybersecurity Funding Applies

If you think about it, cybersecurity can be part of any grant application that's looking to fund cybersecurity or to fund technology. If you're looking for body-worn cameras, if you're looking for a SCADA system, cybersecurity has to be part of that. On the screen you'll see some examples of funding areas — grants that are out there for these different areas. The technology we're looking at protects digital systems, networks, and data from unauthorized access, theft, or damage. The four vital areas listed are utilities, healthcare, transportation, and criminal justice. Again, it's not everything; I'm just listing what I feel is the most important ones to talk about today.

Cybersecurity is critically important for utilities because these systems are foundational to national infrastructure and safety. Electric, water, gas, telecommunications — they form the backbone of this country. A cyber attack on these services can cause widespread disruption, economic damage, and even loss of life. Back in 2021, a water department in Florida had an attempted breach. The state noted that this was a very important threat, and in subsequent years, the state of Florida created their own Florida Local Government Cybersecurity Grant for local applicants — and they funded this for three straight years. States are seeing that there is a need at the state level as well. Massachusetts has their own

program, Arizona has their own program. I think we will see more states creating their own state-level programs in the future. The need is there, and hopefully budgets can kick in for their own state-level programs.

In transportation, modern transportation is relying more on smart technologies every day, so a lot of grants are including smart technologies in their fundable projects. Cybersecurity is at the base of that. You can't have all of those technologies — like electric vehicle charging stations or smart traffic signals — without cybersecurity at the base. Again, cybersecurity is part of a larger project. In the justice system, it's crucial because a lot of these are tied together. Courts, law enforcement, and correctional facilities share data, so a breach can compromise many different entities. In the criminal justice section, cybersecurity is a huge need, and there are grants out there that will fund cybersecurity.

And finally, grants that help public healthcare systems. Cybersecurity helps protect patient data from cyber criminals. Hospitals are often targets of ransomware. As I said earlier, it's easy to target a hospital because they may not have an option but to pay that ransom — lives are at risk. More healthcare grants are starting to include cybersecurity in their allowable budget lines. That is good news. I think we'll see that more as grants open this year as well.

I know it was a lot of information thrown at you quickly, but it does give you an idea that the funding is out there. It's how you approach getting your cybersecurity needs funded. Sandy is going to talk about education funding and then she's going to talk a little bit about including cybersecurity in your grant proposal — successful ways to do that. I'm going to turn it over to Sandy to take over.

Cybersecurity Funding for Education

Sandy Trowbridge:
Thanks, Amanda. The purpose of this next section is just to explore how cybersecurity fits into the education space in particular. Thankfully, many of the programs that Amanda touched on earlier can also assist K-12 schools and institutes of higher education in strengthening their cybersecurity posture as well.

FCC Schools and Libraries Cybersecurity Pilot Program

If you work in the K-12 space, many of you are likely already familiar with the FCC's Schools and Libraries Cybersecurity Pilot Program, which is focused on improving network security postures for K-12 schools, libraries, and consortiums of both types of agencies. The application period for this pilot program has passed, with selected participants announced back in January of this year. I've included it here just for your awareness, as we are hopeful that this will turn into something more regular after the initial three-year pilot period has ended. So while not actionable now, this is definitely something to be aware of and keep an eye on moving forward.

SLCGP, SHSP, and EMPG for Educational Institutions

Public K-12 schools and institutes of higher education can also take advantage of SLCGP to improve their cybersecurity posture. Amanda covered SLCGP a bit already, so I won't go into too much detail other than to highlight the fact that public educational institutions are eligible to apply as sub-applicants to fund things like assessments, planning, or even new technology solutions. Just be certain to review your respective state-specific guidance as to the types of projects they'll be focusing on. This detail will be covered in each state's cybersecurity plan and may differ quite a bit state to state.

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. Educational institutions can qualify for funding under both programs through partnerships with local emergency management agencies or homeland security offices. Both programs can be especially useful if the educational institution is part of a broader regional cybersecurity initiative centered on training, planning, or running simulated cyber attacks or incident response. For these two programs in particular, SHSP and EMPG, it does depend on the state when it comes to eligibility. Sometimes states will allow school districts or institutes of higher education to apply directly, while other states won't — instead relying on those partnerships. So the key is to contact the state administering agency for your state to confirm eligibility and discuss partnerships when first considering whether or not these funding sources might be a good fit for your institution.

Nonprofit Security Grant Program (NSGP)

Then we have the Nonprofit Security Grant Program, or NSGP, which can help non-public education institutions — like private or faith-based K-12 schools and private institutes of higher education designated as 501(c)(3) tax-exempt — really enhance their cyber posture against potential threats. It covers both physical and cyber needs for those 501(c)(3)s that are deemed to be at a high risk of attack due to their ideology, mission, or belief.

Cybersecurity as a Mission-Driven Priority

When we talk about cybersecurity in education, it's important to highlight that cybersecurity isn't solely a technology issue. It's also a mission-driven priority that can directly affect student learning and safety. It's this second piece that will really speak most to grant funders. To lean into this, let's consider two key points that matter most when planning a grant-funded cybersecurity project in the education space.

First, cybersecurity must be part of a broader mission-driven project. It's important to remember that these grants are not just funding software or hardware for the sake of it. We need to understand what broader mission-driven need is being met through the proposed project. This is because grant funders are really driven by a desire to fund specific mission-driven projects that provide a benefit to the broader community. So while we might know that we want to procure specific cybersecurity technology

for our organization, we need to dive a bit deeper into the why in order to successfully convince the grant funder to want to partner with us in funding this purchase.

When scoping out your project, ask yourself a few questions. What need are you working to address through your proposed project? Are you trying to protect student devices for remote learning, or protect sensitive student and staff information? If so, how will cybersecurity support those efforts? For instance, if you're expanding one-to-one devices or shifting towards a hybrid or even a fully online learning environment, cybersecurity is going to be vital in making those efforts safe and sustainable. It's also important to consider the school's current cybersecurity status when establishing your project. Are there firewalls in place? Are systems being consistently monitored for threats? Are staff, students, and faculty properly trained in various cybersecurity concerns? And finally, what are the risks of not working to advance your school's cybersecurity posture? Are there any identified risks that could lead to data breaches or system outages? What would these data breaches or system outages mean for your students and staff? As part of this process, consider conducting a vulnerability assessment to better determine what specific risks are currently being faced by your institution, and then build out your proposed project to directly speak to those identified needs.

The other side of this focuses on how cybersecurity can benefit student learning. Cybersecurity concepts can be integrated into existing curriculum as an innovative way to teach modern skills like problem-solving or critical thinking. The teaching of cybersecurity concepts can also promote digital literacy for your remote or hybrid learners. A strong case can be made for the creation of a career pathway in cybersecurity, given its ongoing connection to high-paying, high-demand careers in the field. Initiating a Career and Technical Education program, or even a club centered on cybersecurity, can spark interest and lead to real career opportunities for students. And finally, it can potentially support dual-enrollment initiatives if students are taking college-level courses online in a CTE-related field like cybersecurity or computer science. The key takeaway is that cybersecurity for a school, district, or institute of higher education is not just about a tech upgrade. It's about the safety of your students and staff and your broader educational mission.

K-12 Specific Funding Examples

With those key points in mind, I'd like to highlight some K-12 specific funding examples that can incorporate a cybersecurity component. First, Perkins Career and Technical Education funding, which supports building career pathway programs. If you're implementing or expanding a cybersecurity pathway in your school's CTE offerings, this funding source can be used for curriculum, technology, certifications, and even teacher training. Because the focus here is on workforce readiness, investments in cybersecurity infrastructure can be justified, as it's helping your students gain industry-aligned skills. While it won't protect the entire school's network, it can provide students with a separate network to

explore and learn on without disrupting regular cybersecurity systems — essentially giving them a sandbox to play in.

Another example is 21st Century Community Learning Centers, which support after-school and summer learning programs. If you're incorporating digital literacy or cyber awareness as part of those programs, you can include cybersecurity considerations as you build out your tech infrastructure to deliver those activities. The Distance Learning and Telemedicine, or DLT, program from USDA is a great opportunity for institutes of higher education to partner with rural K-12 learning institutions to deliver distance learning content securely, with cybersecurity protections built in.

Strategies for Including Cybersecurity in Grant Applications

Now I want to share strategies for successfully including cybersecurity in your grant applications. The first step is to research the grant program thoroughly. Look at past awarded projects, talk to the program manager, and review summary information of funded projects, which may note in more detail what the grant opportunity is most likely to fund. You'll want to look at if the grant program has leveraged tech solutions in the past to fulfill its mission through a close review of these past awarded projects. And then lastly, you can always reach out to the grants program manager directly to ask.

When considering applying for a grant that is particularly technology-rich, such as SLCGP, it's important to keep the bigger picture in mind. One of the most critical elements of any grant application is presenting a well-articulated need statement. Simply stating that your organization lacks modern technology is rarely enough to justify funding. Grant reviewers want to understand the why — specifically the societal or operational benefit that the technology will bring. You should focus on how cybersecurity or other technology will help address the underlying need or challenge.

For example, instead of saying “our IT staff needs improved endpoint protection,” a stronger justification would be: “to strengthen our district's ability to prevent, detect, and respond to cyber threats targeting sensitive student and faculty data, we're requesting funding for the deployment of an endpoint detection and response platform.” This type of need statement does more than just request things. It shows how the technology addresses a specific need and contributes to your project goals.

You can further detail the specifics of this in your grant application's budget and budget justification, highlighting both how your costs were calculated and why specifically the items are needed for project success. This is particularly important for your tech-focused projects where the need for a particular solution might not be immediately clear to a grant funder. Take the opportunity to think through how to best describe this technology without the use of jargon or industry-specific terminology, and further detail how it's required in order to successfully carry out a specific project activity that is in alignment with your project goals.

Also consider what additional elements beyond the cybersecurity technology itself you may need to ensure project success. This might include staff training, policy development, or consulting services, all of which can often be funded in tandem with technology investments. Equally important is involving both your IT team and solution vendors early and often in the planning process. Their input ensures the technical accuracy of your proposal and really increases the likelihood of a successful implementation. When preparing your application, be sure to save formal quotes from technology providers. These quotes are often required as attachments and really help validate your budget estimates. Additionally, your IT team and vendor contacts can help translate technical specifications into clear, compelling language for your budget narrative.

At this point, I'm going to hand things over to Amanda again to dive into some more helpful grant readiness tips so that you can really hit the ground running in your pursuit of grant funding for your cybersecurity projects.

Grant Readiness Tips

Amanda Day:
Thank you, Sandy. I appreciate it — very good information there. Now we want to discuss how you can get grant-ready before these opportunities even happen. The goal is to get your organization to a place where it's prepared to apply to any grant opportunity once it's released. It's important that you not wait until grants are released to start getting things in order, because by that time we're really chasing our tail. This is particularly important with federal and state grants. These grants typically have an open window of 30 to 90 days, but with the delay in funding in the past few months, some application windows are as short as two weeks. The more you can do ahead of time to get better prepared, the more you will be ready when that Notice of Funding is released, and we'll have all of our ducks in a row as we're getting ready to apply.

Get Your Project Ready

There's never a guarantee of funding, but there are things you can do in advance to optimize your chances of being a successful grant applicant. The first step is to get your project ready. To do so, we recommend first crafting your need statement. The purpose of a need statement is to communicate why your proposed project is needed — it's an opportunity to present your case and supply specific data that provides the broader context behind the project. The goal is to confirm that there is an urgent need, and that if it's funded, your proposed project will help meet that need. Being able to demonstrate the need greatly improves the likelihood of grant funders wanting to fund your project.

Having demonstrated the need for your project, it's time to think about how you plan to implement that project. What do you plan to do? When do you plan to do it? Who will do what? What's the end result?

What are you looking to accomplish? This information can be compiled in a standard chart or written in narrative form.

Next, it's helpful to document your project goals, ensuring that each can be tied to your project activities. When drafting your goals, ensure that each adheres to a SMART set of guidelines — I'll explain SMART later, it's an acronym. Once you've mapped out your plan and your goals, it's helpful to gather what resources might be required to implement the project within a specific timeline. Start thinking through what personnel, equipment, supplies, travel, and other direct costs might be required to complete the project. Consider whether it's possible to scale up or down the project based on what funding becomes available. It may be a state program that's not as high as a federal program, or a federal program that's offering more funding so you can scale up that project.

Next, organize the various project components and finalize the who, what, where, when, and why of your project. The reality is that funders may not be aware of your unique challenges, your organization, or the different terminology or acronyms. Taking the time to draft a compelling story about your identified need and the resulting project will go a long way in building understanding between you and the funder, making a clear path to what you're trying to get funded.

Take the time to contact program managers if it's possible. Having a short conversation with a program manager can go a long way in building relationships with funding agencies. Some applicants will apply for the same grant year after year, so they'll know the program manager, and the program manager knows the history of this organization and what their challenges are. It's really good to reach out to program managers — it's something I say often when I'm talking to applicants.

And finally, select your grants strategically. Now that you have a well-thought-out project and you've mapped out what you want to do, why you want to do it, and how long it will take, it's time to start reviewing specific grant opportunities. The fact that you've already done the prep work in building out your project will enable you to more strategically apply to grants and not waste time applying to grants that may not meet what you're trying to accomplish or are not in alignment with your identified need. Being prepared for when these opportunities open can greatly increase your chances of submitting a great proposal.

Get Your Organization Ready

After you have your project ready, it's time to get your organization ready. First, confirm leadership support of your grant-seeking effort. Your leadership has to sign off on any grant submission, so ensure that you have their support, and that if you spend significant time or resources on grant-seeking, they are in it as well and will sign off on your applications.

Next, assemble your team. Identify other personnel and stakeholders who may need to be involved in applying for the grant or completing the project. Also ensure that you have the appropriate registrations completed. Do all your research and determine what platforms or portals grant funders are using. Make sure you have access to them — sometimes it can take time to get approval. Getting all of this done before a grant opens or before your team is ready to apply is very important.

Then, work to prepare grants before they open. If it's available, review any past applications or previous guidance, because sometimes guidance is pretty much the same year to year. Whatever you can do to get ahead of that based on either old webinars or old guidance really helps in the current application. Check the grant agency's website for technical assistance as well if you need it. Many grants require a budget match, so make sure you work with your financial department to confirm you have the funds to match the grant funds.

The next step is to stay on top of grant opportunities. If you're likely to seek grants from a specific agency, be sure to sign up for their listserv, check their websites regularly, and subscribe to their email alerts. As application windows are becoming shorter, this is a really important step — so you know the day that these grants open and can jump on the application.

Create a grant-seeking documents folder. This will help keep you organized and keep all your documents — financial statements, mission statements, and other documents that may be asked for with a grant — all in one place. It will also ensure that everyone knows their role and any deadlines.

And finally, create and maintain relationships. There are partners in your community that can help you carry out some projects. Are there agencies that could provide technical assistance or letters of support? Are there institutes of higher education that could help you team up to apply for a grant? These partnerships are important for current grant funding and future rounds. It's really important to develop partnerships in your community.

Crafting the Most Competitive Proposal

We need to make the most competitive proposal that we possibly can. Because grants are highly competitive, it's important to craft a proposal that inspires funding agencies to support your project. We often remind people that grants are designed to support projects, not products. We've said that over and over on this webcast. Cybersecurity and other technologies requested should always tie back into a project, meaning that they are needed to ensure that the project is a success. This is why you need a strong need statement. Start with your goal, then figure out what you'll need to accomplish it, and put the project first, followed by the products and technologies that you need.

Third tip: learn everything you can about the grant prior to applying. Always read the guidance and make sure you understand the requirements around the grant as well as the proposal. The funder is

expecting a return on their investment. Various application elements and required post-award requirements are important to review. You need to be prepared so that you're not caught off guard with some kind of document that you might need to apply or provide after you've been awarded.

We go back to the SMART goals that I talked about earlier. SMART stands for Specific, Measurable, Attainable, Results-focused, and Time-bound. Be clear and direct about how you'll implement the project, what the outcomes will be, and how you'll measure those outcomes. Don't be vague — be succinct in your answers.

And most importantly, tip five: before you submit the application, get a second or even a third set of eyes on your application. Getting a second set of eyes may catch errors. Sometimes there are word limits. Sometimes there are specific fonts or sizes you need to use. A second set of eyes can catch things like that. They can point out acronyms you might have used or abbreviations that don't make sense to outsiders. And they might notice if an actual component is missing. Receiving that objective feedback and resolving the issues that they bring up immediately will give your application a better chance of success.

With all of that information, I really hope that we've helped you understand how cybersecurity is a fundable budget line in the context of larger projects. As we said, there are some cyber-focused grants, but it's more often a part of a comprehensive project where you'll get your solutions funded. So, good luck in your grant-seeking journey. We wish you the best. I'm going to turn things over to Katherine to tell you about the Check Point grant service.

Check Point Grant Support Program

Katherine Osorio:
Thanks so much, Amanda. Thank you so much for joining us today. Here at Check Point, we work with the Grants Office to be able to work with you for all of your grant support needs. We have an entire team here on the public sector side to support you. We have account managers ready to support you in almost every state. If you drop your emails in the chat, we'll be able to pass that over to our account managers to reach out to you.

Customized Funding Reports

If you do have any questions or concerns about any upcoming projects, we have a sample for you about the customized funding reports that we were discussing earlier. We know that it could be perhaps a little bit scary to discuss your grant needs, especially if you've never done it before, but we want to reassure you that the grant funding process is very simple. We wanted to show you what that would look like for you as a customer. This is what a sample customized funding report would look like — a table of contents depending on your needs. Whether you're looking to fund anything with cybersecurity,

mobile device management, EDR — it really could be anything under the sun. We'll be able to help you navigate through that process, and we'll be able to divide everything according to what that project looks like. There's going to be different applicable grants depending on who you are as a customer — whether you are a K-12, a university, a state and local government agency, healthcare, etc. And of course, where you fall geographically, because the grants will also vary per state. So it's very important for us to know where you fall geographically. This is what a customized funding report would look like for you. It's going to be tailored to you and only you, and it will have all of the information that you need to help you navigate through the process.

How the Process Works

When the funding report is completed, we'll schedule a call internally to review the contents of that report. On that call would be myself, one of the representatives from the Grants Office, and your dedicated account manager from Check Point. Perhaps some of you have worked with Check Point before and you might already know who that is. So you'll continue to work with them, but perhaps there might be some customers on this call that are new. We'll assign you to your correct account manager, and we will go from there.

From here, we'll be able to determine different areas where you might need additional support. We do have another sheet for you to look at — that will be your deadline sheet. See where you would need to focus your efforts: whether it's a preliminary project that you want to work on first and prioritize your time on. We want to make sure that you understand the timeline for what's coming up for you. Maybe you'll separate things per quarter or per fiscal year if you are a government agency. We want to make sure that you understand the deadlines coming up for these grants, so that you know how much time you have in order to submit. We'll provide that timeline for you in that worksheet.

We also have a dedicated web page for you to visit, as well as for you to share with anyone else in your organization that might not be on this call. This is our dedicated page for you to visit and contact us. It has a little bit of information about who we are as an organization — Check Point — as well as who the Grants Office support program is and what they do for us. It's a little bit more about what they do, and then there's a direct contact button that will reach me directly. I know Michael just dropped that into the chat for us as well.

I provided my contact information here. Again, thank you so much for all of you for joining us this afternoon. I look forward to answering every grant question that you might have and assigning you to your correct account manager for public sector. I will pass it back to Michael. Thank you so much for joining us today.

Q&A Session

Michael Paddock:
Thanks very much, Katherine — and thanks to all of our presenters. Great information. We have two minutes for questions and we have a couple of questions that have come in, so I'll just run right through these really quickly.

Q1: Do you see foundations funding cybersecurity?

For Sandy: do you see foundations funding cybersecurity? I noticed there were actually some foundations on that sample funding report that Katherine was showing. Are there foundations funding cybersecurity?

Sandy Trowbridge:
It's a great question. I was just chatting with a nonprofit last week who was in the middle of developing a purely cyber-focused project in coordination with the local foundation that had just recently added cybersecurity as one of their core focus areas. So foundations focused on cyber funding do exist, but if that's not clearly called out as a focus area, we recommend for things like cybersecurity taking a look at foundations that note a willingness for their funds to be used for operational or general support. This just means that they may be more willing to fund behind-the-scenes infrastructure that ultimately allows you to safely carry out your broader mission-driven activities. So look at those foundations that cite an openness to funding things like operational support or general support, versus purely programmatic support.

Q2: What is the cost for grant support through Check Point?

Michael Paddock:
For Katherine: what is the cost for grant support through Check Point?

Katherine Osorio:
There is no cost associated with working with the Grants Office. You can work with us for free. We have a membership with the Grants Office. Feel free to drop all of your emails into the chat. The only thing that would be at a cost to you is if you decide to use Grants Office for grant writing as a service. So that means if you want them to write the grant for you. But we can certainly discuss that offline if you want to go over grant writing as a service cost. But there is no cost to use the Grants Office.

Closing

Michael Paddock:
Thanks. I noticed a couple of you have already put your email addresses into the chat. While we finish up here, we've got about 30 seconds left. If you want to put your email address into the chat, we'll be sure to follow back up with you.

I want to thank our presenters: Katherine Osorio from Check Point, and Amanda Day and Sandy Trowbridge from Grants Office for joining us today and sharing your knowledge and experience with us. A lot of great information on cybersecurity funding — something that can be a little bit more nuanced in terms of looking for cybersecurity funding and finding it, but we have a lot of answers for you that have been presented today. Thanks to Check Point for sponsoring today's session and making it possible for us to bring you all this information. To all of you who came today, we certainly appreciate your time. 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 August 12, 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.