WHITNEY BELL: Hello and welcome to the GRIP Training for Secured by Design Considerations. I'm Whitney Bell with ICF and I'll be your host today. First, we have a few housekeeping items for today's webinar. This WebEx meeting is being recorded and may be used by the U.S. Department of Energy. If you do not wish to have your voice recorded, please do not speak during the call. If you do not wish to have your image recorded, please turn off your camera or participate by phone. If you speak during the call or use a video connection, you are presumed consent to recording and use of your voice or image.

Luckily for you, all of our attendees, you are in listen only mode. If you have any technical issues or questions, you may type them in the chat and select send to host. There will be a Q&A following today's presentation, so please submit all your questions in the chat box and select send to host. We will only answer questions related to Secured by Design plans during today's webinar. Any other questions that come in may be used to update the GRIP Program FAQ, that link should be showing up here in the chat momentarily for you. If you need to view the live captioning, please refer to the link that will appear in the chat now. Finally, and the question that we get most often, we will post a copy of today's presentation on the GRIP Program webpage by tomorrow and the recording of today's webinar will be available on that same page in about two weeks. We will send an e-mail to you, anyone that is registered letting you know when that is available.

All right. So to kick off today's training, we'll hear from Colin Meehan, the Project Manager of the GRIP program with GDO for some introductory remarks. Colin, welcome.

COLIN MEEHAN: Thank you, Whitney, and thank you everyone for being here today. We're really happy to have you at this training. As a reminder, I'm sure you all know, we have several topic area deadlines coming up over the next month and a half and we want to make sure that everyone is well prepared. We're holding this training today for two primary reasons. We've had a lot of stakeholder interest and feedback on grid security issues. And second, we want to make sure everyone understands the need to have best practices and grid security embedded into all elements of the GRIP Program, each of the topic areas, which is why we're calling this training Secured by Design.

As a reminder for everyone, we've received over 700 concept papers across all three of our topic areas within the GRIP Program. As a result, we're expecting each program to be highly competitive and we're encouraging applicants to do everything they can to ensure that their application meets the needs of a modern grid. This includes ensuring that security, risk evaluation and mitigation measures are an active component in a project. This is critically important to making sure that we have a successful modernized grid and a successful operation of each of these different topic areas within the program. So I'm really happy to have you all today and really appreciate PNNL for hosting this training session. It's going to be important for all of us as we get ready for the application period. With that Whitney, I'll turn it back to you and thanks again for everyone joining this training.

WHITNEY BELL: Thank you, Colin. So now we'll hear from David McKinnon. He's a Senior Cybersecurity Researcher with PNNL who will lead today's training. David, welcome, I'll go ahead and turn this over to you.

DAVID MCKINNON: Oh, thank you. Hi, I'm glad to be able to participate in the webinar today and we're going through several Secured by Design Considerations to help you with your projects as you bring things together. The goal today is to or GRIP’s scope is to support [unclear] in the energy sector and all of the industry priorities. What we really want to focus on is the security must be baked in, you know, by design from the very beginning. And that we want you to be able to adequately evaluate the risks as you go throughout the life cycle.

So security assurance. We want you to focus on much more than just cybersecurity, you know, physical security, the standards of detect, deter, deny, delay, defend. Many of these projects will be out in the open. You need to consider the risks that will be associated with that from the physical security perspective, and we're seeing renewed interest in that across the grid. Cybersecurity, traditionally confidentiality, integrity and availability, and the power grid is more focused on the operations and integrity is generally prioritized first. And then of course the cyber-physical security, how can someone do a blended attack now? Start in the cyber domain crossover to physical and then come back again or vice versa?

Also, there's resilience, this notion that we'll also talk about later, but you need to be prepared to be breached and so you need to have a plan so that you can continue operations, you can be resilient against an attack. Information assurance, the information that you're reflecting and gathering is important, how are you going to protect that? Make sure that it is suitable for use at all times. And supply chain.

Again, the topic with renewed and increased interest across the grid.

So we've got all of these perspectives and I kind of like to think of this, you know, the story of the blind man and the elephant. Now each one of them had a different perspective of the elephant, whether it was a tree, if you remember the story, because of the tree trunks, the legs, just focusing on the legs or the body of the elephant being a large wall. You know the flaps, being it's a tarp or a tent. We can't focus on just one aspect of security when you're working on your projects. And so hopefully today we'll give you some ideas on how you can step back and see the whole elephant.

Lifecycle considerations, there are several that we've want you to consider. Several of these came from the R [?] Project a number of years ago, and when DOE was investing in the smartgrid they had a similar effort where all of the awardees submitted cybersecurity plans and had an opportunity to work with the department subject matter experts to help them design cybersecurity into their process. And the things that we focus then at that point was, how are you going to mitigate the risks at each stage of the lifecycle? Because there are distinct lifecycles here? You've got a concept you're going to submit it for funding. And as you just go on with any standard project, you've got a design, you get to that 80% design, you take it all the way through, you start construction, you go into operation, you operate for a number of years, perhaps decades and then at the end of the life of the project or the equipment, it needs to be decommissioned. Are there risks at each of those points? How are you going to focus on those?

Cybersecurity, again, you need to focus on your vendors because it'll be very hard for your project to be more secure than what the vendors actually give you with their hardware. So when you have a choice between two vendors, are you going to look at how they mitigate cybersecurity risks in their products or in their services? Will that be a factor as you consider vendor selection? Then of course, there's the relevant cybersecurity standards and best practices. There are a lot of standards out there, which ones are going to be relevant to your project? You will need to have a plan for identifying those because there's simply too many and some of the standards won't be a good fit for your project.

Back then, we focused on the emerging smartgrid cybersecurity standards. They're still being worked on many years later, there will still be new standards that continue to emerge. So does your project and project team have a plan in place to how to track those standards as they emerge? And how you'll implement those and incorporate those into your project over the lifetime of your project. And of course, integrity and confidentiality, integrity and availability and that's the key triad. Your project and your security insurance plan should be able to speak to each of those.

And any lifecycle, discussion that doesn't talk about how you're going to log, monitor an alarm based on the evidence that you're gathering, that would be incomplete. So if you're not logging data, you're going to be completely blind to anything that's happening within your environment. You're not going to have any data to go back through if you need to do an investigation to determine what happened. And then your best practices, can you provide evidence that you're following your practices, that you're actually walking the talk that's in your plan? And all of those are considerations as you go forward with your projects.

One of the key updates since our was -- and this was released in their cybersecurity framework, this came out because an executive order and it's a nice framework that can help ground you on the different aspects of what you need to look at. It's a risk-based approach, it makes sense. There's core concepts here: identify, protect, detect, respond and recover. To identify, can you understand to manage the risks to your systems? Can you identify what they are? Can you put safeguards in place to protect against those risks? And if there's an event, do you have monitoring in place so that you can actually detect that an incident occurred? And once you know that something has happened, do you have a plan to go through and respond to that event? And of course, after every event, is there mechanisms in place so that you can recover, if you're subject to a ransomware attack? Do you have backups so that you recover and start over and start over again as needed?

And the other aspect of this new cybersecurity framework is this notion of implementation tiers is that you can go from partially implementing some of these concepts, to being risk informed, you know what the risks are, you've analyzed them. Do you have a repeatable process that takes you up -- just shows a bit more maturity in your process and your overall commitment to security assurance? And of course, adaptive, if things change over the course of your project or the system’s lifetime, do you have a process in place that you can continually learn and adapt to the evolving threats?

So in a nutshell, then the cybersecurity framework, we could spend much, much more time on that, but for today, we wanted to keep it a simple high level overview. And then from the cybersecurity perspective, DOE may require any award or funding recipient to demonstrate the cybersecurity maturity of the project that they've submitted. And you know, per that note, DOE will want to know what the minimum contents of your cybersecurity plan are. Are you planning to use open standards and guidance such as DOE’s cybersecurity capability maturity model, C2M2?

If you're going to use proprietary standards, have you documented those? And for all of those you will coordinate with the DOE program office, in this case it's GDO with the GRIP Program. There's a note here that once the plans have been selected, you'll receive more guidance from the program office. There's a lot of pieces that are in motion and so just be prepared to get, you know, receive updated guidance as you continue to work through the funding process. James, would there be anything else you'd want to add speaking towards this?

JAMES BRIONES: That's good Dave, thank you. Just to piggyback on what Dave said, it's basically further guidance and support will be provided by DOE once we get into that phase where we're selecting awards. So again, as it's mentioned here, we are going to provide you some technical support and some assistance so that as you go through your processes on negotiating the award, once it's selected, there's additional guidance that will be coming up.

DAVID MCKINNON: Thank you, James. Excellent point. DOE is planning to support your projects. We're here to help. We're not just going to say “do it” and leave you all on your own to identify the risks and map them and put plans together. Where possible, DOE will bring subject matter experts to bear on your individual projects to help you achieve success. That's what we all want here.

And there are several risk-based principles and these ten areas come out of DOE’s C2M2, the cybersecurity capability maturity model. The key here is that we're going to apply defense in-depth. You're going to layer the security mechanisms so that you can get -- protect the system as a whole, and multiple security controls will come in and protect a given system. We will cover these more in depth as we go on. The inventory and configuration management, do you know what assets are that you need to protect? Are you monitoring the threats and vulnerabilities? Do you have a strong process for evaluating and managing risks? Do you have a risk register? Can you do that?

Access control and recognizing that both physical and logical security and access to your system needs to be managed. Are you aware of your cybersecurity environment and can you maintain situational awareness? Do you have an operational center that tracks physical and cybersecurity for your project? Can you respond to incidents and events? We've already mentioned supply chain, it's critical. Are you buying legitimate parts or are counterfeits being substituted in your supply chain, so that you end up using an inferior product from what you had intended to use for purchase? Training, your staff are your frontline [unclear] or frontline defenders, they will be adequately trained, they will be able to identify issues that will have a security impact for your project. So have you trained them? That could be your frontline defenders. Do you have an architecture in place so that your program works as an effective whole? And of course, are you managing the whole project?

And then just going back to the principles. We want a plan of action for cybersecurity that your team will generate and submit. And it's the guide for the teams to follow, we know it's a plan, and we know that all plans are subject to change once they're put into implementation. We want to know that you have a plan so that you can go forward. And then is your plan comprehensive? Does it address the full computer network and all of your systems in your project? If your project is a small piece of a much larger system, then are you able to focus in on that smaller piece, but also talk about the integrations and how you will protect those integration points with the larger systems?

And of course, make sure that you have covered all the broad categories in your plan, that no important elements are missing. This second primary bullet here, this should be a manageable plan. There is no one-size-fits-all cybersecurity plan or security awareness plan. Some systems need to be highly protected. The bulk electric system, the standards for that are much, much greater than what you would have for a small municipality or co-op system. A system that supports residential housing might not need the same level of protections or monitoring as something that protects a high value transmission substation.

And given that this is a DOE funding opportunity, we encourage you to use all of the research that DOE has invested in over the last several decades. The department has produced many tools that will be of value to you as well as standards and guidance such as acetyl M2, NIST has put out the cybersecurity framework, we've already talked about that briefly. Reference these documents, you don't have to reinvent everything all over again. You use what's already been produced as much as you can.

OK. Next we'll go into more depth on each of those ten areas. These come from C2M2 and they should all be addressed. For some of the smaller projects, you might only need to consider a few paragraphs or sentences, for a larger project that will have a greater impact to the grid, we'd expect you to analyze the domain more in depth and provide more answers and more details in your cybersecurity plan.

So for asset, change, and configuration management, you need to maintain an inventory of the digital assets and systems that you have in place. It's really hard to protect the system if you don't know what the moving parts are and you don't know where they are. So the first step is identifying the assets themselves. If you're in a building, are you aware of all of the operational technology that's in the walls and in the ceilings? Can that have an impact upon your project? Who are the other folks that are cross connected into your network, the vendors and others?

So go through and develop a system so that you can identify the project’s assets and of all those assets, some of those assets who will be more important to your project than others, those will be your critical assets. Just briefly describe that lists of assets. Or sorry. Describe the categories of assets, but we're not looking here for a full listing of all the devices that you have. All the devices, that's information that belongs to you, we don't need to know all that, but we do need to know that you have a process in place so that you can generate a comprehensive list for you to use on site within your project, within your company.

And once you have that list, how are you going to implement and maintain that process so that on day one, you have a list of assets? Now a year from that, how do you know that that list will still be accurate and valid? And is there a way to manage that change control over time? Do you allow just anybody to replace the workstation or a server? Or do they need to go through a configuration review board of some sort to gain approval to replace a critical server in a data center? Speak to some of those points.

And of course, for all of these, you'll see a reoccurring theme is that, what are the standards and guidance that you're going to use as you plan out your asset change configuration management? And then the fourth point here, having a great plan will not be of help if you can't assign the staff and the resources to manage the process, so you need to have a great plan and you need to be able to allocate budgets and staffing time to work that plan.

OK, threat and vulnerability management, the second one that we talked about. You need to outline a plan to monitor the threats and cybersecurity vulnerabilities, you know, the security vulnerabilities in your project systems and assets. So again, identify the plan to identify and address the vulnerabilities. This needs to be a plan that can be worked over time. At the start of a project, identify the vulnerabilities and then put that on the shelf for five years and have a commitment and an appropriate time interval for your project to go back and reassess what those vulnerabilities might be. Vendors will change, products will change, the environment will change. So having a process there.

And again, we've got the point is identify the standards and guidelines, industry best practices and guidance that you're using. If you belong to an industry trade group and that group has put together guidance that you're already using, claim credit for using that guidance already. And, you know, being part of in this case, maybe a threat intelligence cooperative or subscribing to a vendor’s threat intelligence reporting system or referring to the alerts that the government puts out as well. Again, the last bullet: make sure that you can assign the resources to work your plan.

Risk management. Risk management is critical because there are so many risks that are out there and you can't address them all. So you need a mechanism to prioritize the risks that will be of value, or the risks that will have the greatest impact to you. And so, you know, putting together a risk plan to have a risk register to track your risks, to track whether you're going to mitigate the risks, whether you're going to accept the risks as is or transfer those risks to someone else or a third party contract or some other mechanism. You need that plan and you need to have that plan for risk management.

Again, NIST just put out some guidance and others for how to manage risk and the risk management kind of undergirds everything that will be in your plan. Because every project is unique, which means that every project will have different risk tolerance and so risks that might be accepted by one company or one project, because it won't have a large impact, that same risk might be devastating if it were to be realized for another project. So personalize your plan to the risks and the risk tolerance of your project.

Identity and access management again is important. We talked about needing to know all of the systems, the physical assets and the logical assets in your system. You also need to know who the users are. And for the workstations and devices that are talking to each other, machine to machine, you also need to manage their identities. So again, having a plan to manage the identities or using Active Directory and LDAP system. Well, lots of different opportunities here depending upon the technologies that you're using, that you need to be able to manage the identities and you also need to manage authentication.

Is that given user - Can you authenticate them for access to a given system? And that plan needs to cover your access to all of the key systems and critical assets within the system. Again, if these plans that you're going to submit to DOE or just, if you will, the tip of the iceberg for what likely should exist already within your company. And you know, if you do have, I haven't mentioned before, but if you've already got corporate standards and policies put in place that address these things, there's no need to reinvent the wheel. In that case, mention that, per your corporate standards, reference it by name, say that we will follow these standards that address identity and access management.

Give us enough of a notion to know that the company is already doing this and that you're going to follow your existing plans there. If you're already doing it accurately, there's no need to create a second process just for DOE in this project, you know, continue on with the good work that you're doing. Again, you know, identify the standards, and of course, in every one of these bullets, have a plan for how you're going to assign the proper resources.

Situational awareness is important because the landscape is always changing, so you need to have a mechanism to monitor the security environment and maintain your situational awareness. Do you have to identify your plan for how you're going to monitor your systems? Now what is the login that you're doing? And then are you doing the analysis? If you’re just logging on, when people log into the system, that's useful, but if you're not doing the analysis to identify that somebody logged in remotely outside of your service territory then you're not going to have that situational awareness that that might be a rogue login.

Or maybe it's one of your technicians is on travel, is offsite supporting somebody else, but they still need to log into your system, having that situational awareness of where your people are, where your logins are coming from is just one aspect of monitoring your security environment. So talk about your situational awareness. If you have an operations center, I'll speak to the fact that that operation center is tracking your environment so that when anomalies occur, you're aware of them and you can take proper action. Again, follow the standards and make sure that you assign adequate resources to accomplish the tasks at the level that is needed to meet the risks for your project.

All right, event and incident response and continuity of operation. This is important because there will be events and incidences that occur. It's just a given that something's going to happen to your system. Even if it doesn't come under malicious attack, you're going to have equipment failures, you're going to have a user that fat fingers the command or accidentally issues a command that shouldn’t have been issued, and you need a mechanism to respond to that. So think about how you want to detect, characterize and respond to security events and then document that in the plan. Again, if your company already has a process for that, that you can use for this project, then again, mention that you're going to follow your company plan.

And a lot of this will speak to, you know, as these event incidents come in, have a mechanism for triaging these, being able to identify which ones are critical and need immediate remediation today and which ones you can address tomorrow. Again, follow standards and best practices and make sure that you have staff that can work an incident when it occurs. If it's a large incident, you might need to be able to bring in extra people to work in that incident until it can be resolved.

Supply chain and third-party risk management. We have mentioned this briefly. It's critical because nobody is able to develop all the products in house. You're going to have to buy goods and services from other companies. Some of those companies will be well known to you because you have long-standing relationships with them. Some of them you might not know. Some of them might be based in the U.S., some might be owned by multinational corporations. You need to identify the possible risks that you have there. It's well known that there are a lot of, the gray market exists where counterfeits are introduced into the supply chain. Do you have a mechanism to ensure that all of the products that you were buying are legitimate products?

If you have a vendor that is critical to your operation, have you ever been on site of their corporation or their factory to see how they monitor the security so that the products that they produce, so that you can build an awareness and a comfort level on the fact that they will meet your needs and that all of the products will meet the quality that you want, that they design and the security that's needed. And this is all important because we have seen several attacks over the years where adversaries have gone after a third-party supply chain. Embedded malware and devices that are then bought by other corporations or that software is part of a managed service and so the malware works its way through the third party into your corporate environment. And then from there, will lie dormant for a while, and then be activated and cause havoc or cause an incident that you'll have to respond to. So whatever you can do to manage those supply chains and those third-party risks, please be aware of that and focus on that. And again, doing all of that requires resources and if you can use existing standards, then you don't have to reinvent the wheel.

Training. We've mentioned this, people are your first line of defense. There’s too many situations for us to document them all, but if the staff has been trained and then they will notice what's going on. Many power operators just have a sense of what the hum of normal daily activity is and they can identify when equipment is starting to fail just because the sounds, it sounds different. It would be hard to document exactly what sounds different, but your operators know that. They're the people that are working in your operations center or your staff and engineers, they also can develop a sense of normal and so if you can train them just so that they're aware of what's normal and abnormal then they can assist your security assurance team in implementing your security awareness program.

So provide the training and make sure that that's a reoccurring training. Now there's some training that you can take once, when you're on boarded, other training that's important enough will be an annual reoccurrence, maybe more frequent. Safety, everybody values safety and safety training is an ongoing process. Future security training, the same way. Training your staff when they start and then always provide refresher training and vary that training based upon what the current active security environment is. And by now you're used to follow the standards and assign the resources.

For the cybersecurity architecture, the architecture is how you're going to fit everything into a complete whole. We want to know that the team is considered the architecture. Network architecture is one element of this. You can implement your network just so that there are protections, that you've got enclaves or, you know, protected enclaves where engineering works within their own space. You know, HR, finance could also have their own carve outs so that attacks can't immediately spread corporate wide. So a flat network that allows an attacker to spread corporate wide without effort is really going to hinder your ability to respond to an activity.

Whereas if you can isolate your network segments, then you can stop an attack before it spreads to corporate wide. So again, you know, have a plan for how you're going to look at your architecture, have a plan for when you bring in new systems, how that will get integrated into your system because it's just bolted on or just throw it into the middle without thought, you might be able to implement it quickly, but if an incident occurs later, that the effort to respond will be quite significant. And then if you're doing this, how are you going to do you software and data security too? Does your architecture ensure that you've got trusted software? Do you whitelist your software? Do you know what data actually matters is? Is the reporting that's coming off of your power flows, is that critical to system operation, is that critical to billing?

What's the relative priority of operations and billing? Think through those things so that you can develop an architecture that fits your needs. And again, follow the standards and assign resources to the projects that you can accomplish this. For an architecture, you need someone to design it and you'll need to invest upfront. So please assign those resources.

Program management. We've talked so much, every one of these slides talks about assigning resources, that comes down to management. So have a management program. Is there an individual that has executive authority over this project, so it can ensure that the security awareness receives the funding that it needs as a whole? And is that manager or executive, that leader, do they have the skill set that they need to allocate the budgets into each of these 10 domains appropriately? Do they have staff that report to them that can help them make informed decisions?

So put together this plan for managing the process. Make sure that we've also got a continuity plan when that manager gets promoted or transfers, retires, is there a pipeline for Mark to ensure that there is a successful leadership transition? And think management office for your project. Again, follow the standards. And now at this level, do the chief executives for your company, do they have their support, have they adequately funded the cybersecurity and security assurance that's needed for this project? Make sure that you have the executive level buy in.

OK. So that was the 10 domains. Next, we're transitioning a bit. We're going to talk a bit about the design principles to adopt. And there are many design principles, one I've taught cybersecurity as an adjunct professor. We can spend days, every one of these topics we could turn into hour long lectures in and of themselves. So we'll briefly highlight some of these, but again, if you can apply these design principles, that are tried and true, they will help you if you go forward to implement your process.

There are many of them, we’ll just focus on eight in the following slides. The first one on this lead off slide: defense in depth. It's critical, it's the first one because it's that critical. Your system will be breached so the castles of, you know, back in the day, they had a moat, they had a wall, they had an inner keep, there are multiple layers of defenses before someone could get to the crown jewels. And then there were the planes that surrounded the castle as well. You need the ability to defend in depth. If there's any spot where there's only one mechanism, one chance to keep an attacker out, then you've already failed because the attacker will find that one spot. So make sure that they have to go through multiple locked doors, if you will, to get into your system.

Two others on this slide, they kind of go hand in hand. Similar and interrelated, but also unique. The principle of least privilege. Don't give out more privileges to people than what they need on our workstations, whether Windows, Mac or Linux. You don't run as your root admin user all of the time. If you've got those privileges, they're in a separate account, but for your day-to-day, e-mail and everything else, you're doing that as a regular user. That's an example of least privilege. You only function as root level administrator when you need to, for that given a task.

So you're going to go through and ensure that people have the permissions that they need, but you're only going to give them just what they need. Sure, it's convenient to give everybody, you know, a master key to the building because just copy one key, but then every room is potentially at risk if that key gets lost. Just so you know, it might be more difficult to cut two or three keys so that somebody only has access to the labs or the rooms that they need, but that's going to protect everybody else in the building because only those three labs would be at risk or those three offices if those keys were to get lost.

So think through what's the minimum required access that they need. And then once somebody transfers out of a building, they don't need to keep those keys. And so again, and we understand this in the physical sense, the same things exists in the cyber domain as well. If somebody moves out of HR into finance, they should lose access to the HR systems and be granted access to the finance systems, but you wouldn't necessarily give them access to both, that's not least privilege. And by doing this, again, you reduce the risks that can occur, because if someone's identity is co-opted, they can only do the least amount that you have given them. They don't have access to everything.

On the other side of this slide, we've got least functionality, least functionality. We're going to give them the minimum functionality that they need, they might not have a lot of privilege, but again, now we've already focused on that, the least functionality. We're only going to let them have the minimum access that they need. So that if you're in HR, you've only got access to the HR systems. If you’re systems engineer, you have access to the engineering tools but you can't do anything in HR or in finance, you can't work in operations either.

Your functionality is limited to the role that you have that day. If you transfer again, then those roles and assignments are changed as well. This least functionality, it also applies to devices themselves. So often we think of the people, but the systems also need to be designed this way as well. Default settings are something that you really want to look at because many things come out-of-the-box configured to do everything because that allows you to get started quickly, but the trouble is later you can do everything and if something goes wrong then something could go wrong with everything.

So focus on least privilege and least functionality. In the banking. back in the day when there were two signature checks, the person that wrote the check wasn't necessarily the person that signed it or you needed two signatures to ensure that one rogue person couldn't embezzle funds or commit fraud, think of this in the cyber domain as well.

Zero trust is something we've heard of more recently. There are mandates to adopt zero trust. A lot of the vendors or marketing systems they're talking about zero trust. You need to think about how zero trust works within your organization. In many cases, if you could get into the front door of a building, then people could walk around all, up and down every hallway and look into every lab. That could be a bit of a risk. And so you want to make sure that you've got, if there's a research and development wing in your building that there's a second set of doors that you have to walk through just so that you can get in and showing, proving who you are, going back to identity management that we talked about, those are principles of zero trust.

Don't assume that just because somebody got into the building or was able to log into the system, don't allow them to go throughout the whole system. Every time they come to a locked door verify who they are. Verify that this system is able to -- has permission to access another one, if you've got machine to machine communication. So identify your systems and don't evaluate them just once when they first boot it up, but evaluate them daily, hourly, whatever is needed, every transaction to verify that that device is still good or that user is still employed or still needs access to operations or still needs access to engineering. Verify that, constantly check it. Don't assume that just because they're there, they're trusted.

Continuity of operations, another key principle here. Assume breach, assume that someone will get into your system, assume that a ransomware attack will happen.

Can you recover from a ransomware attack? Can you quickly identify that it has happened? Do you have the backups in place? Now, if you're under ransomware attack, it's too late to do your backups, because at that point you're just backing up the ransomware. So have the plan in place ahead of time.

From a fault tolerance perspective, many systems are designed with a hot standby. So that if one system fails then the other one can immediately swap in without any loss of operations. Can you do that in your cyberspace as well? And prepare now so that you can recover later because a breach will happen and these are projects that are associated with the grid, the lights need to stay on. So focus on that, have a plan for that.

Data minimization. OK, these projects, they have the potential to capture a lot of data. Do you need all of that data? What's the minimum set that you need for accurate billing? What's the data sets that you need just so that you can maintain situational awareness? We're tempted often to collect everything that we can, because storing data is so cheap, but managing that data can become expensive. And if you're over collecting data and your systems are breached and all that data is exfiltrated for your site, it's moved off site, criminals or others now have access to all of that data and they will find connections that you might have missed.

And so it puts the privacy of your systems in jeopardy, it puts the integrity of your systems, the potential jeopardy if there's enough data there that your system can be completely reverse engineered based on an over collection of data. And again, there can be needs to collect your data, but when that data is no longer useful, when it's become too stale, then have a plan in place before how you would delete that data and sanitize the systems where it was stored.

Configuration management, we've spoke about this, it's a design principle you need. You need to manage your systems. You need to go through and ensure that the configurations that you're using are appropriate. The last point here is fail secure failures will happen. And safety systems, people understand that devices will fail and so they will design them to fail safe. In our cyber systems and cyber-physical systems, we also need to fail safe, we need to fail secure. If you've got an electronic access control system that monitors all the doors for your building, you need to think through is it appropriate to, if the system fails, to open up all the doors? Or do you lock down all the doors and you require physical security to show up with the key to let people in and out?

So those are the points. When the slides are sent out, we've got resources, we won't go through all of them here, but again, each of the 10 domains in this, it's got standards, there's Special Publication 800-128 focused on configuration management, others for continuous monitoring. A lot of the talk about supply chain with the efforts that are coming out there and the government and this focus on supply chain. And then others here are focusing on training programs and information assurance, cybersecurity management.

So I’ll wrap up with the official piece here, and then we scheduled a lot of time because we wanted to allow for Q&A at the end, so hopefully you can stay for that. I think there's some questions already coming in. But in conclusion, the point of this effort, the security assurance program that GRIP is putting in place, is we want you to think about all these design decisions ahead of time and we want you to bake in the security. We don't want you to fold it on after the fact because the performance will never be as effective as if you bake it in.

And the other key point here is focus throughout the lifecycle, you're going to start with development, you'll go to implementation of construction, building your project, and then you're going to operate it for a number of years, and at some point, you'll have to decommission it. Security assurance applies to each of those stages.

Alright, I have talked for a while. I think it's time for some Q&A and I think there's already a question or two that came through.

WHITNEY BELL: Thank you, David. I appreciate everything. So we do have time for Q&A now. As we stated before, please submit your questions to the host using the chat. We will focus on answering questions related to the Secured by Design Considerations presentation, any other questions may be used to inform our FAQ at a later date. We are bringing up a couple of other people to help answer some questions as we go through this. So let's go ahead and get started with our first question. This one is confirming per the FOA, cybersecurity plans are only required for topics 2 and 3 and will be required after submission of the application, not part of the application.

JAMES BRIONES: Yes, that's correct. And as I mentioned or as David mentioned in the beginning of the presentation, additional information will be coming in terms of the requirements of cybersecurity plans and all of the language in the FOA is what you should always follow, right? Like, what it says on the FOA, that's what you should follow. So yes, it's only for topic area two and three, but as you consider your projects right, like any other projects, I think it was mentioned by David earlier as well is that during the ARRA funding and I believe some of you might be participants on that is that when we start looking into security, I think there's some aspects of that cost wasn't considered in the beginning. And we now have some shortage of resources to apply security controls on some of the projects. As it applies, right? Some of it doesn't need it, some of it needs more, so you got to consider those risks. Thank you.

WHITNEY BELL: All right. So the next question here, I do want to reiterate because we do continue to see questions come in about this, so if you've got specific questions about the cybersecurity plans process, we will provide additional guidance in the near future and all applicants will be notified, accordingly, when it becomes available, I just want to reiterate it, we've seen those questions come in several times today. So our next question here, is the cybersecurity content you're covering today relevant to the grant application in detail, or is the cybersecurity content come into play for the discussion and definition after the grant application is submitted? This is kind of similar, but for example, during the negotiation phase. I'm going to keep asking because we keep getting the question.

DAVID MCKINNON: It clearly comes into play afterwards because that's when the plan will be finalized. I'm not one of the program officers, but to me it'd be nice if the application spoke to the fact that you knew that you needed a plan. If you're completely silent on the plan, you're probably going to be in compliance with the FOA, but I think the intent here is to get you to an accurate plan. Now, I might be overstepping there, but I'm biased because, you know, cybersecurity is my day job. You know, the security awareness. So I will put you over to James for a more authoritative answer.

JAMES BRIONES: So, you know, you can look at this process in phases, right? At this point, we are in the application phase. So all the applicants are providing their project proposals, right? And then once a review happens, there's a negotiation of award or selection process. So when we hit that process, a lot of this question is about cyber security plans, what are the requirements? How many pages? It will come into play, right? Those are like the process part, but if you look at your project right now and you step back and say hey, you know, what kind of security controls do I need? This training is what we're trying to kind of give you that, you know, hey, you know, set that spark to say, OK, we gotta think about security because in our project these things could need some security controls, right? So, you know, think about the process on what to submit about it later. In this case, we just want you to kind of process it so that, OK, you have to consider security assurance and security controls as you think through your projects.

WHITNEY BELL: Thank you for the clarification. Another question, in the area of OT protection and supply chain risk management, newer innovative modalities not envisioned in the original standards offer better risk management. Will the inclusion of newer, non-standardized defenses be penalized? Or is the inclusion of newer mechanisms viewed favorably and encouraged?

DAVID MANZ: David, I can answer a couple of the next few questions because I've been looking at the answers, obviously chime in. But this is David Manz, another David from PNNL, and that's a great question, this is exactly what we're talking about. Cybersecurity standards are important, but they often lag what we're doing to actually manage the risk. So no, you're not going to be penalized for doing something that you think is better and more relevant to your proposal, to your environment, you'll never be penalized. If you grab something that's esoteric and off the wall that we may not have heard of, we'll have to actually look it up, and if it's fly by night or snake oil that you might be penalized. But I definitely want you to be thinking about risk management, not compliance. So I think the heart of that question was very good. And there is a reason there are standards and cryptography is a great example of where you don't want to roll your own, but if you have a reasonable justification, share that justification with us and I'm sure you won't be penalized.

DAVID MCKINNON: Exactly. Most of the slides, part of the reoccurring theme there was use the open standards and guidance, but if you're going to deviate, explain it. So to what David said, explain why you're going with the newer solution and it can be as simple as this provides better security assurance. And if you can explain that, we will understand that because, as I said, the standards take time to be implemented. The research is always out there on the cutting edge, and then as they get adopted, they turn into standards. But if your company is able to move quicker then feel free to innovate quicker.

WHITNEY BELL: We have another question about vendors and supply chain. Is there a consolidated list of vendors that are not allowed, for example, for the supply chain?

DAVID MANZ: Yeah, that's another great question. And so the answer is no, but there's a reason it's no, right? We, on behalf of the federal government, cannot endorse vendor X over vendor Y because that's favoritism and none of us want that from the government. So we cannot do that, but we do have some procurement language available from the Department of Energy that can use you at procurement time to really hold your vendors to the fire and make sure that they're going to produce something that's going to help you and then help you win this proposal. So I think it's worthwhile Googling, you know, procurement language from DOE and it's an easy find.

And the other thing I think is important is, to go back to what David previously said about vetting your vendors and looking at, of course, if things are multinational, as most things are these days, you know, where is the ownership? What does that mean for your risk, for your corporate risk? And just being a cognizant consumer of, it might even be an American product, but the software or the firmware or the hardware was actually from somewhere else, and just understanding that. It's an exhausting question, but it is one that you should have some sort of policy and management on. And so another thing to do is look at what your peers are doing. I think that's a good conversation to have, to understand what vendors they're going for and why, it may not be the answer for you, but that's a good thing to look at. So there isn't a consolidated list of vendors. You can see what the federal government has used as an example, and you can definitely, at procurement time, force security policies that you see fit.

WHITNEY BELL: Thank you. The cybersecurity principles being presented today are appropriate for securing the entire enterprise. However, some proposals are for either point solutions or enhancements to the grid to enable advanced grid resiliency. Is the intention that almost all proposals must implement the entire suite of protecting the entire service provider or do the proposals only need to address those cyber protections, design and principles that relate to the program being funded by DOE? If you need me to reread it, let me know.

DAVID MANZ: No, you don’t have to - So essentially, do we have to secure everything or do we have to secure the part we're proposing? And no, we want you to do a risk-based approach and some of the security elements we presented may not be relevant at all. And perhaps you'll just do one or a subset. You don't need to secure the entire system like your entire OT/IT environment or your entire enterprise, but we do want to see evidence of a reasonable plan for securing the part that you're proposing. And so just convince us that you've thought about the security consequences of when things go wrong and right with what you're proposing and how you plan to manage that. David, do you have anything to add?

DAVID MCKINNON: Good point. We want you to right size the plan for what you're doing. I'm making up an example on the fly here. Let's say your proposal is to put a fence around the building. If you're just building a fence, there's no need to discuss identity management because the fence doesn't care who you are, so on that section it would be does not apply. Let us know that you've thought through it, if it doesn't apply, just say no, it doesn't apply. If your corporate standards already address that, say, we're going to inherit all of the controls from our corporate that help us manage these risks here.

But if it's a point solution then define the security assurance that's needed around that point. We don't want -- There's no intent that you're going to define corporate security because you've got a point within the corporate footprint. Just talk about your piece and how it fits in, but focus on your piece and if things don't apply then let us know that you've thought about it. I mean that would be my preference because if you don't talk about it at all, we're going to have to guess as to whether you thought about it. But if you bring it up, say we thought about it, there's nothing to discuss here because it does not apply to our point solution, that lets us know that you've addressed the question, you've thought about all the questions, and that's what we want.

WHITNEY BELL: Thank you. So this one is for you, Dave McKinnon, could you clarify the difference between the principles of least privilege and least functionality? In the grid space, least privilege relates to or what has access to data or functions available within the system, but principle of least functionality is about limiting the data that is produced or function that can be performed by the asset or system. The first tries to limit the number of people or systems who have the ability to access the system and the second tries to limit the damage that could be done if a device or system is compromised. So could you clarify the difference between the principles of least privilege and least functionality?

DAVID MCKINNON: OK, good question. There is some overlap there. Least privilege that people have just enough, privilege. Yeah, if you're – that they blend, sorry.

DAVID MANZ: Well, I mean, I've got an example of this.

DAVID MCKINNON: Okay, thank you, David.

DAVID MANZ: In a control center environment, least privilege would say your operator doesn't need engineering access, right? The least privileged to do the job. The operator has all the authority they need to do their job to monitor the system, to push a red button, to pick up the phone, right? But they don't need to necessarily have engineering access to roam on devices, they don't need to change billing information, right? So if you give them a user role, that role is tailored to their job, and they don't have extraneous permissions. The worst example is giving everyone root or everyone admin, right? They have the least privileges to do their job.

And then least functionality is another good example from, let's say, a substation now. You've got a PLC and it's electromechanical or you've got a protective relay and it's electromechanical, 50 years ago, and then it got upgraded, and now it's got some integrated circuits. And now you bought the newest product and you know what? It's actually a full computer that's still performing the same function. And you're like, oh, it's cheaper, better, I get better telemetry, but it also has a web server running on it, it also has a wireless dongle on it because it is built that in, right?

That is all functionality that you don't need and potentially from a security perspective could be very bad. So least functionality says that device only can do what it needs to do. So you actually have to do more work to turn things off or rip them out or break it, but that's the principle of least functionality that that remote device, the field device only has the functionality it needs, because extra functionality means extra areas that I can do a buffer overflow and use the web server to now get into your data concentrator, for example.

DAVID MCKINNON: Thank you, David, great examples. When we went to buy a new stove recently, you can buy stoves with Wi-Fi and I'm just like, why do I want Wi-Fi? I mean, the little buzzer that used to ding when the cookies were done was good enough, I don't need a message going to my phone to tell me that I'm done baking my cookies. Again, so limit the functionality of your devices because if my stove can talk to my phone, my phone can talk to my stove or my oven that could open me up for burned cookies, per say. If you think about it, about the devices and the people, it helps you a little bit, as David explained. But again, focus on the roles and what you need, and no more, no less. I think one of them is more horizontal and one's more vertical, if it helps you think that way, too.

WHITNEY BELL: Thank you. And I will be sure to not buy any ovens with Wi-Fi. [laughs] Another question here, how should we address cybersecurity for non-connected devices proposed in Topic Area 2?

DAVID MANZ: Yeah, great question. So non-connected devices to me sounds like an assumption. If I was teaching my class, I would say this air gapped isolated system gets breached in two ways, and I'd ask the class what the two ways are and they'd be stumped. The first way was when you procured it, supply chain, right? Someone else built that device and probably someone else third-party provisioned it and installed it in your environment. So even if it's a standalone device, I don't have to worry about cybersecurity. Well, supply chain, you do have to worry about where you sourced it, how it gets maintained and updated and what it actually is doing. Is it least functionality or is there extra functionality? That's a wireless dongle you didn't know about and so it's actually not standalone, right? OK, sky is falling. It's enough of that.

But the second area is sneaker net, as I like to call, right? So even if it's a standalone device, do you have engineers who access it, do you have physical security people who monitor it, right? There are still breaches to this isolated device with sneaker net or people. So do you have appropriate policies in place? How do you update it or monitor it? So yes, isolated devices are good and we shouldn't rush to put everything online, but it doesn't mean it's a panacea cure all to say, “Oh, everything is isolated, I don't have to worry about cybersecurity.” Unfortunately, we don't live in that world. Supply chain and sometimes people who make mistakes or people who do malicious things can touch the device too, so that's – [unclear]

DAVID MCKINNON: Yeah, great points. Just because you're isolated today doesn't mean that tomorrow the service tech won't bring in a laptop and cross connect into the device and go over cellular modem back to corporate. You still need to think about the overall security assurance, and I loved how David mentioned the device could even be compromised before you deploy it, if you weren't paying attention to supply chain. And in the simple case as a counterfeit, you've bought something that's supposed to have a 10 year warranty for service, but it's a counterfeit, so it's all going to last two years and then it's going to, you know, because they used shoddy parts or gray market parts. You still need to have that plan to ensure that your operations are going to go on.

WHITNEY BELL: Thank you so much. So if you are not NURKS [phonetic] certified, are your security protocols evaluated differently?

DAVID MCKINNON: I'm not sure on the mix of the projects, but I suspect many of these projects won't meet the threshold for requiring NURKS, in which case you're not going to be expected to abide by the NURKS ZIP standards. That's where you're going to go back to the relevant standards for the market niche that you're in. If it's a point solution and you're bringing in a 10 megawatt solar farm, that easily could be under the thresholds of the NURK ZIP [phonetic] requirements. You won't be able to default to those, you're going to need to explain why your corporate standards, existing management policies are sufficient, or what new practices you’re going to bring to bear to help secure that point solution.

WHITNEY BELL: We have, I believe, just one more question here. For Topic Area Three, with public entities being the lead applicant and often relying on industry team members for cybersecurity expertise, how do you expect the prime applicants as public entities to be involved in the cybersecurity plan and associated implementation?

DAVID MANZ: Yeah, not an easy question, you probably want to hear from all of us on, frankly. If you're the submitting party, right, you ultimately have the responsibility. So again, outsourcing that is totally appropriate if you have a consulting firm that's doing cybersecurity or if you're relying on your partners to bring their cybersecurity expertise. Again, that sounds reasonable to me, but articulate that, articulate how you've evaluated their cybersecurity powers, articulate how they're bringing something to the table that’s going to help you. You don't need to be the expert on everything, but do articulate where you are planning to manage cybersecurity risk, convince us of that. And so the way you do that is again to show that you've thought it through and you understand that this is a potential weakness and so I'm shoring it up by doing this. That's my short answer.

DAVID MCKINNON: Yeah, great points, I'll extend it a little bit too. You're going to be the prime and all of those subs need to abide by the standards and policies that you're going to put into place. So it doesn't make sense for the prime to commit to strong identity management when there's no requirement for the subcontractors and they can go and get anybody from a job shop, put a vest on them that day and let them walk into your facility. If you're going to do strong identity management and access control, you need to ensure that your subs are also doing strong identity management and access control too, because otherwise your subs are going to be a backdoor to open up vulnerabilities into your project. You're hiring them because of their expertise in cybersecurity, well, then that's good, just make sure that you've got a holistic plan that you benefit from the expertise they bring and that any requirements that you commit to in your proposal also flow down to them as well.

WHITNEY BELL: All right, I believe that brings us to the end of our Q&A today. There are a couple of questions that we didn't get to, but we will be putting those answers into the FAQ and we will send out a note to everyone when that is updated, so you are aware. A copy of today's slides will be available on the GRIP Training for Secured by Design Considerations webpage. We'll have that up by the end of the day tomorrow and the recording will be available in two weeks. We will send you a note when that is available, just so you know, you will hear from us on that. To find out more information about the GRIP Program, please visit the program webpage, find that in the link, in the chat right now. And then thank you to our full panel here of answering all of those questions today, I really appreciate it. And special thank you to David for your presentation. And thank you to all of our attendees who were participating, asking questions, really, really appreciate it. So take care everyone and we will see you next time.

DAVID MCKINNON: Thank you everyone for joining.

END OF FILE