Stefanie Keto: Welcome to SRAI Shop Talk, a monthly podcast spotlighting the people, practices, and evolving landscape of research administration and the community that works collectively to support it. Whether you're new to the field or a seasoned pro, each episode features insights from experts across institutions, big and small, working in pre-award and post-award compliance, communication, and everything in between.

I'm Stephanie Keto based at the Office of Post-Award Financial Services at North Carolina State University. This season, we're exploring the theme bridge builders, creating unity across roles, generations and technologies.

A single oversight in research security can collapse years of hard work, which is why building a bridge between strict new regulations and our faculty has never been more vital. As technology and collaborations continue to shift, the US research enterprise has more hurdles than ever to navigate on a daily basis. That is why being informed on research security requirements isn't just beneficial, it's essential for everyone involved in the research lifecycle.

Today on Shoptalk, we are breaking down the different levels of research security and digging into the background behind why compliance in this field has become so critical. We'll also explore the importance of the new required training being implemented by federal sponsors and how it serves to protect our institutions.

Hello and welcome to today's episode of Shop Talk. Joining me today, I have some wonderful experts here who are going to talk about research security and all the challenges and information that we need to know. So first off, will you both be able to introduce yourselves and provide a little bit of overview of what you do?

Mary Millsaps: I'm Mary Millsaps. I am currently the Director of Research Compliance at NC State and in that role I serve as the university's research security officer. Prior to arriving at NC State, I was at Purdue when the proverbial research security umbrella kind of came over all of us. And so I started Purdue's program as well. So I've got to see it at two both research intensive institutions.

Lisa Nichols: I'm Lisa Nichols. I'm the Executive Director for Research Security at the University of Notre Dame. And at Notre Dame, I feel like it varies in terms of the responsibilities that is classified regulated data export controls, research security and research conflict of interest. And previously held the same role at the University of Michigan and was previous to that at the University of Pennsylvania. I have worked within government and also for the Council on Governmental Relations. So I've had an opportunity to see the various angles of this issue as it started to develop back in 2018. And so it's been a very interesting time. I also currently serve as the Deputy Director for the

NSF-funded SECURE Center and as a co-chair for the Federal Demonstration Partnerships Research Security Subcommittee.

Stefanie Keto: Thank you. And as you mentioned, Lisa, that you worked with the government and other places moving into our conversation, you helped with the architect natural frameworks like NSPM-33 at The White House level. And Mary, I know that you've led the charges at both Purdue and NC State and also you work with the Association of University Export Control Officers.

Do you both feel like the research security landscape has finally stabilized into a clear set of rules or are we still kind of in a period where things are constantly moving for researchers and the administrators?

Lisa Nichols: Yeah, I'm happy to start here and just to say that research security requirements are definitely still evolving. They can be challenging to track. We are, for example, waiting for federal agencies to implement NSPM-33. Agencies are also changing their risk review processes. The Department of Defense or WAR recently updated its risk matrix and added nine lists. So there are now 13 restricted lists that the agency uses in its risk assessment. And we see other agencies potentially poised to have at least perhaps 11 lists, restricted lists as well. In addition to that, more companies are being added to lists like the 1260H restricted list and we expect biotech companies to be added in addition to the kind of more military related companies. Data restrictions continue to increase including the Department of Justice's sensitive bulk data rule, NIH's October 2025 policy on enhancing security measures for human biospecimens. So we're seeing controlled unclassified information protections for some NIH data that isn't CUI. So we're seeing that as well.

And then in addition, NIH no longer allows foreign sub-awards and we're seeing questions from NIH regarding potential undisclosed foreign components in relationship to co-authorship on publications. And co-authorship on publications has been a challenge in terms of that serving as a proxy for collaboration as Mary knows. And so a lot is challenging, it's shifting, it's evolving and it's tough for our faculty, our researchers to track all of that. And so there is tracking this ourselves and then communicating it to others in a way that allows them to function and engage on an international basis. Mary?

Mary Millsaps: Yeah, I would agree with everything that Lisa just said. I would just add from an on the ground practitioner's perspective, I do think 2025 represented a significant shift in where we are from a regulatory framework in that prior to 2025, it wasn't clear how the agencies were going to implement it, how they were going to require it, how they were interpreting the disclosure rules, et cetera, what the cybersecurity rules were going to look like. And I do think that 2025 we started to see agencies implement specific requirements. And for

the most part, they have been consistent with the framework of NSPM-33 research security training. For example, all of them are pointing to the CHIPS and Science Act legislation. So even if you're using the NSF training versus your own, you can certify that you're meeting a specific standard.

So as a research security officer charged with explaining the requirements to my faculty, I finally feel like in 2026 we can at least put some guidance on persistent websites. We can design training that at least gets them 90% of the way there so that they understand what their disclosure requirements are, what appointments, what collaborations may cause triggers of high risk designation, et cetera. And more importantly, I've been able to explain to my leadership what this new regulatory topic of research security is. It very much is its own discipline related certainly to cybersecurity export control compliance, regulated research, conflicts of interest and conflicts of commitment, but it sits on top of all of those things. And so I can explain to my leadership what type of resourcing is needed so that we can communicate to our faculty in a coherent and a consistent way.

Additionally, we've stood up an office structure that gives agency individuals an opportunity to know who at NC State to speak to because that's half the battle. If they're communicating with PIs, "Hey, we need this requirement and RPIs don't know who to contact, that then becomes a communication loop that can delay an award or create potential non-funding issues.So I think most universities are recognizing this as a separate discipline and are staffing it appropriately. And I think communicating that out to your researchers, who at your university is charged with assisting them in this space is a critical item that we can now take action on in 2026.

Stefanie Keto: Thank you both. I think that both of you touched on the research security training requirements and I know that this is kind of a hot topic in your world right now. So as we're looking at this and these requirements are not wholly adapted by all the sponsors, they're kind of slowly coming online with DOE being the lead on it. What methods would you say that you would recommend for entities or institutions who might still need to make sure that they're meeting this requirement? Or if this is new to them, maybe they haven't worked with one of these sponsors before, what can they do if they're quote unquote out of compliance right now?

Lisa Nichols: Yeah. I-

Mary Millsaps: Yeah. Well, I-

Lisa Nichols: Oh, go ahead.

Mary Millsaps: Well, let me jump in, Lisa, because I'm going to brag on some of the efforts of the NSF SECURE Center. So the first thing I would say is institutions need to recognize when this requirement is in fact a requirement. As you mentioned in May of 2025, it became a requirement for all Department of Energy proposals in later in 2025, NSF implemented that requirement as well and then other agencies are rolling it out. So if it is a requirement that you are submitting a proposal and all senior personnel have taken research security training, it really is incumbent upon that institution to make sure that that has happened because if you don't, then you're exposing yourself to a False Claims Act. I would leverage existing resources. Certainly NSF has the four modules that were created under an NSF grant, but the SECURE Center on their website, which by the way, has a tremendous amount of resources available to institutions working in the research security space, but they have the consolidated module. And certainly if you don't have your own training, I would encourage your institution to explore that and have your researchers take that before those proposals are submitted.

In addition, I would look at perhaps figuring out how you might implement a more standard process. At NC State, our vice chancellor for research determined anybody submitting a proposal to any institution will be required to take research security training starting in October of last year. So now it's an institutional requirement that helps us meet anytime there is a regulatory requirement by the agency. And so that makes the compliance of it easier. It also makes it much easier for faculty to know when it's required or not. And so that's the approach we've taken.

And so Lisa, I'll let you weigh in.

Lisa Nichols: Sure. Yeah. And with respect to the four training modules that were developed by NSF under cooperative agreements, at this time, NSF is no longer updating those modules. So they're four one-hour modules. It was a lot of time and that is the impetus for creating a condensed module. And so with the one-hour module, all of the agencies, about half dozen agencies to date have indicated those that have acquired the training to date indicated that they recognize that training module as meeting their requirement. However, as Mary indicated, if you have training that meets the CHIPS Act requirements in the law, that works as well.

So we have this one-hour training and it is available for download into institution's learning management system. So you can download it, use it, track it there, track the training there. It's also available through the Citi Program. So many institutions are administering training that way.

And then in addition, if you are, for example, a smaller institution, you didn't have Citi or a dedicated learning management system, the

researchers can also take the training online on the SECURE Center website, which is secure-center.org and get a certificate there. So there's a number of means to do it and that is nice, right?

And what we are doing at our institution, to be honest, we have to date been requiring the training for particular agencies as they roll it out, we've been making those investigators, as researchers aware that that is required at the time of proposal within the 12 months of proposal. However, as more agencies do implement this requirement, it may just be simply easier to implement it for everyone. And so on an annual basis. So that's something that we're looking at as well. We do also have means to track that as well so that administrators can know when the training has been taken as well. So that's how we're handling it.

Mary Millsaps: Yeah.

Stefanie Keto: And I think the NSF SECURE Center has a listserv that people can sign up for and receive updates for. So that can also help out for those who need to know.

Lisa Nichols: This is a weekly briefing comes out. And so that is an easy way to stay informed on research security generally. I'll mention just too, since we're talking about the training, we actually have a refresher training that is under 30 minutes that is out for user testing right now. And so our hope is to have that completed by the end of the month, by the end of May and it includes more case studies. So to our discussion earlier about keeping researchers informed, the types of questions that we've heard from researchers are addressed there. And so that can be used as an annual refresher. It captures the information in the original one-hour module, but it condenses it further and then adds some additional information that researchers were seeking. So just another consideration.

Stefanie Keto: And now you both have talked about how your respective institutions have implemented the training and kind of maybe who tracks it a little bit. It kind of sounds like it's a self-guided tracking at both places, but what challenges have y'all seen with these new requirements in your respective institutions? Are there administrative burdens or submission delays or maybe issues with faculty engagement?

Mary Millsaps: Well, from a research security training requirement, that's one of the reasons why we implemented the requirement across the board so that faculty, senior personnel and research administrators didn't have to know when research security was required. I would also say we took that approach because we are seeing quite a few post-award requirements for research security training to be verified. So even if it wasn't in the regulation for the proposal, agencies like the

Department of Defense are asking us to certify that they've taken it at time of annual performance review, for example.

So for us to eliminate and reduce that administrative burden, we've implemented a way for proposals to be verified that research security training has been taken. In addition, our training... We don't use the SECURE Center training. We actually developed our own. It's very scenario based, but more importantly, it tells our researchers how to get help if they have questions at NC State.

So we felt that was a good investment in time. It tells them how to disclose internally because we certainly don't want them to disclose something to the federal government that they haven't also disclosed to us. And then it allows us to reach out to faculty that may be in high risk situations so that we can work with them and provide them guidance as to how to mitigate that risk.

One of the administrative burdens that we've found a local solution on, but I think was quite a challenge is the USDA's 10-year lookback on participation in an aligned foreign talent recruitment program. That is not consistent with NSPM-33 and quite frankly is very unique to the USDA, but it is a requirement that they've implemented as of the December 31, 2025 terms and conditions, which essentially anybody funded a senior personnel on a USDA award has to confirm that they have not participated in an aligned foreign talent recruitment program in the last 10 years. So we have created a way in which we get that disclosure from the individual and then deem them USDA eligible, or in the unlikely event that they did participate in an aligned foreign talent recruitment program, USDA ineligible for the period of time.

So again, we did that intentionally so that proposal submissions would not be delayed and that we can meet that requirement, both institutional certification and individual certification.

Lisa Nichols: Yeah, I'll just mention on that. We're asking of course about foreign talent recruitment program participation within the context of our outside activity disclosures. So we do have that information in system. And then in addition to that, what we've created working with one of the developers, the research administration software developers that we work with is to create a dashboard. The dashboard indicates whether they've completed their disclosure requirements, how they've disclosed related to talent programs, then in addition to that, whether or not they are current on training. So that's a means to reduce burden.

I will say quickly regarding the training. With the SECURE Center training, you can actually include institution specific information at the end. So it's true. It wouldn't be throughout the training, but at the end it allows for any number of slides, two, four, six, however many

institutions are interested in to provide that information on who to go to, what your local policy and processes and the like. So just something to throw out there.

Stefanie Keto: Now, Lisa, you had brought up before about international collaboration, so I have a question for you on that. And Mary, you can chime in too, but Lisa, what main tools are your university using to give to the PIs to check that their international collaborations are not a risk for sending anything out, like what they're doing?

Lisa Nichols: Yeah, no. And I will say, I mean, a lot of it is education, for example, on agency risk review processes and what it is that they're looking for. And in addition to that, we did add to this, as mentioned to this new training, this refresher training, more scenario type information, based again on questions that researchers are asking. And so honestly though, and I always feel like the first step is restricted party screening. So unfortunately they do have to come to us still for that. We do make that clear. Just come to us, we'll run the screening. It takes two minutes. It's so important to start in that way. But I think too, that there are questions that they have to ask. They have to be aware of who they're engaging with.

There may be others on the project that they're not directly engaging with, but what is this collaboration and who's funding the different aspects of the collaboration? And there are those great questions in the NSF report, the JSON report on fundamental research security that was commissioned by NSF. So those are great in terms of really thinking through collaborations and we've put those on our website and made those available in that training as well.

The SECURE Center has been developing a prototype and I thought it was already fantastic several weeks ago, so I'm hoping it becomes available soon. It does allow the PIs to take that first step by utilizing the consolidated screening and other lists that are available publicly, thinking about the type of research they're performing, where they get their funding from and the like gives them just an immediate how risky this might be and you need to go and talk to export controls, research security and the like, or this is not on any US restricted lists and based on the type of research it is of lower risk. And so it's something though that obviously needs to be vetted with research administrators too in terms of their comfort level with that kind of tool, but it can create an opportunity for them to just do that first pass and then come to administrators with their understanding, their interests, so.

Mary Millsaps: Yeah. So we've implemented a few tools in addition to some of the things that Lisa already talked about you. You cannot replace going out and talking to faculty departmental meetings and college level meetings and kind of educating your researchers on what this research security thing is. It's not just controlled research, although

you obviously have heightened due diligence responsibilities around controlled research. This applies to every type of research that we do, whether it's in humanities or obviously the STEM disciplines have some specific requirements, but we do not allow any agreements to be entered into with foreign entities, unless we've gone through a restricted party screening. So that prevents formal engagements with entities of concern, but we have also implemented restricted party screening for any foreign external professional activities that may be disclosed. In addition, when someone travels abroad and indicates they're visiting certain institutions or receiving support for that travel from certain institutions, we've implemented restricted party screenings for those things as well.

In addition, when someone indicates they're traveling to a country of concern or a country that presents added risk, which then captures some of the additional comprehensively sanctioned or significantly sanctioned countries, that requires an approval by the research security office before that travel authorization can be approved. So that's the way we can intercept when somebody might be going to engage in person with someone. We've also had some discussions with our college leadership, especially in our College of Engineering of how we might do a better job of capturing informal collaborations that may eventually lead to a co-authored paper or more formal engagement because if you can intercept those before that becomes a real thing, then your faculty and your researchers can make a risk-based decision on whether or not they want to pursue that relationship. So we haven't implemented anything yet, but we are certainly looking at some of our peer institutions who have to see what has worked for them, maybe what has not, because we don't want to implement something that's going to depress international collaboration inappropriately and create a burden for our researchers to engage on important scientific topics across the international spectrum.

We want the research to be protected, but not suppressed. So you've got to approach this in a very even-handed way and leverage the tools like the SECURE Center. I love the risk-based risk assessment tools that the SECURE Center has put out. We just put the two travel checklists on our own international travel website for our faculty to think about their travel as it relates to risk. This is an area that I hope the federal government becomes a little bit more nuanced over the next few years so that again, we can hit that right-sized level of compliance and regulation and don't create overly burdensome structures that suppress the science.

Lisa Nichols: Yeah. I'll just mention too that we've similarly are conducting restricted party screenings just across the board with respect to sponsored projects and procurement and outside activities and the like. We do also route travel to foreign countries of concern or embargoed countries to our research security team and provide

information there as well. And certainly we'll consult with faculty as needed depending on the situation. We don't require approval. So this is not something that is an approval process, but it is awareness for us and also awareness for those traveling on potential risks and mitigation and just ensuring that there aren't going to be any research security or export control concerns.

Stefanie Keto: Now you both kind of touched on the bad, I guess, or the ones that we shouldn't be working with, the international collaborators and things like that. What would you say are common errors that faculty make that most often trigger maybe a red flag for you when you're looking at your reviews?

Mary Millsaps: Yeah, I guess I would rephrase that question a little bit because quite frankly, faculty researchers and others can be doing perfectly appropriate and academically relevant things that still trigger them as high risk. A perfect example of that is several agencies who include the Department of Defense could potentially flag someone as high risk if they have a history of co-authorship with colleagues affiliated with institutions and countries of concern. Whether or not that research was conducted truly in a collaborative fashion with that institution, or if the research was done fully in the United States, but the publication occurred after one of the co-author's affiliation changed.

So I wouldn't say they've made an error, but we certainly are trying to educate our faculty and our researchers on what could potentially trigger them to be designated as high risk and trying to provide them with maybe some preemptive language that they can include in proposals. For example, I think it goes a long way toward the NSPM-33 principle of transparency that if they do have co-authored papers, for example, with problematic entities, that they disclose that in their proposal and they call out where that research was done. And if those collaborations continue now. And if they don't, they should say that clearly. I caution our researchers that any continued collaboration with entities that are on one of those lists that Lisa referenced, that is a risk and they need to consider that. Not because the individual may somehow be maligned, but they are working within a structure that at least the federal government has identified as potentially problematic.

One common error though that I have seen is that faculty don't appreciate that the federal agencies do consider journal editorships as professional appointments that they should be disclosing on their bio sketches. I've had conversations with both NIH and DOD and they do consider those professional appointments and those agencies that are using the common disclosure form would expect to see appointments of those types on their bio sketches. So leaving them off, especially journals that publicly make their journal, their editor

boards public could potentially trigger a identification of someone who is not disclosed as they should.

So again, it goes back to education, making sure that our faculty understand what the agencies expect to see and understand that even if they never signed a contract with that journal, if the journal has a website that says they're on their editorial, board, then they need to either ask that journal to take it down if they don't truly consider themselves an editor or they need to disclose that on their bio sketch so they don't get flagged as non-compliant with the disclosure requirements.

Lisa Nichols: I'll just follow up on Mary's points by saying, I mean a couple of things. One, I will say in this new refresher training, I feel like I'm advertising this refresher training.

Mary Millsaps: I'm really excited to take it, Lisa.

Lisa Nichols: Because it does address the issue of authorship. And really if that work, for example, DOD-funded work was conducted in the United States, that should be the affiliation. The affiliation should not be the current affiliation due to a publication lag. And also in the acknowledgement section, ensuring that who is funded by what is properly acknowledged. We are working through the federal demonstration partnership and other means with organizations like Elsevier to try to address this at the publisher level and to have standard-

Mary Millsaps: Great.

Lisa Nichols: ... right, across the publishing community. So that is an avenue we're pursuing. And then at the same time to have agencies providing that same guidance. So if we're all providing the same guidance and we're all on the same page, at the very least we can reduce future instances of you have a collaboration that you don't in fact have. So we'll see how that all comes about.

Mary Millsaps: Yeah. Just in follow up to that, I will point out that... So I wear another hat at my institution, I'm the research integrity officer. And another aspect of publications is who did what for the paper. And I think to Lisa's point, also adding who funded what for the paper will help when an agency's security team is reviewing is somebody disclosing things appropriately, calling out specifically which agency funded what portion is critical, but also who did what, what data was generated by who. Having that consistently across the board in scientific papers will go a long way to helping researchers answer questions of whether it be research misconduct or whether it be research security issues. So I love the fact that FDP Lisa is having conversations at the journal level or the editor level or publisher level because that really is where it is the best place to start it. We can

have those conversations with our faculty and our authors, but if it's not kind of consistently enforced by the publishers, it's kind of an uphill battle. So that's great to hear.

Stefanie Keto: I have one more question for both of you and this would just be more looking forward to the future. Are there any upcoming potential conflicts or problematic things, maybe AI or any other kind of thing that could be potentially problematic for the US research enterprise?

Mary Millsaps: I think we don't know. I think the nature of research security regulations for sure is tomorrow we could get another regulation that kind of upends our program. So I think it's important for professionals in the research security space to be familiar with the principles of NSPM-33 and the goals of the CHIPS and Science Act research security provisions and rely as they're making decisions at their institution about what research security controls and processes and guidance to put in place, lean heavily on those principles because quite frankly, I think the principles of NSPM-33 of transparency, disclosures, recognizing international collaborations and adjusting risk accordingly, understanding when the export control regulations come into play all still remain just as true as they were when MSPM 33 was issued in 2021 and the implementation guidance in 2022.

So be familiar with those. Don't lose sight of those principles and then you as an institution will be able to adjust to whatever comes down the pike, I would imagine. But that's how I would see it. Lisa, I'll let you have the last word.

Lisa Nichols: Well, thank you. Yeah, I think you said it very well, Mary. I think the only thing I might contribute is with the BIOSECURE Act, perhaps we'll be seeing more in the biotech space and that's something that we'll be looking for in the health research space, including some of the rules and policies I mentioned earlier, laws. So there's just more coming there, but apart from that, you're right, it can be challenging to predict.

Stefanie Keto: And it always just sometimes just takes one person to potentially cascade something that becomes a new regulation, I feel. Yeah. Well, Mary, Lisa, thank you for coming and joining us on Shop Talk. This was a really informative episode. I really hope that our listeners enjoyed it, but thank you again for coming and joining us.

Mary Millsaps: Well, thanks for the invite, Stephanie. I really appreciate it. Great conversation.

Stefanie Keto: Lisa and Mary provided an abundance of knowledge today, shining a light on the importance of why a strong foundation is so critical for these new research security requirements. They gave us a clear understanding of the training available for researchers and exactly how often it needs to be completed. Most importantly, they

highlighted the real world stakes, showing how international travel collaborations and publications directly impact a researcher's portfolio. By securing these foundations, we aren't just checking boxes. We're actively safeguarding our faculty's life work. A huge thank you to Lisa and Mary for joining Shop Talk and sharing their knowledge.

A huge thank you as always to our wonderful podcast team and everyone who continually contributes to enhancing this podcast. We are proud that this platform brings together people, ideas, and new opportunities in research administration. The conversation doesn't stop here. We would love to hear from you. Please submit your suggestions for future episodes of SRAI Shop Talk to shoptalk@srai.org.

Thank you again for listening to this episode. Don't forget to subscribe and help grow our community by sharing. I'm Stephanie Keto and I'll catch you on the next episode.