Constellations Podcast

Episode 63 – The Space ISAC, Cybersecurity and Innovation

Guest: Erin Miller, VP of Operations for Space ISAC– 18 minutes

John Gilroy: Welcome to Constellations, the podcast from Kratos. My name is John Gilroy and I'll be your moderator. Our guest today is Erin Miller, Director of Business Development at the National Cybersecurity Center. You can hear the buzz in the background here. We are recording this from Utah State University at the SmallSat Show and at Utah State we say. "Go Aggies."

Erin Miller: Go Aggies.

John Gilroy: During this episode, we'll talk about the Space Information Sharing and Analysis Center, referred to as ISAC, what it is and why we need it. We will also discuss new developments and strategies to combat increasing cybersecurity and other threats to our space assets. Today, in front of the microphone we have Erin Miller, Director of Business Development at The National Cybersecurity Center in Colorado Springs and home of the Space ISAC. Between her work at NCC and her previous experience at The Center for Technology, Research and Commercialization where she solved dozens of problems for the war fighter in space and cyber, Erin is well versed in the objectives of the ISAC. So we're going to jump right in here now and ask the obvious question. So Erin, tell us exactly what an ISAC is.

Erin Miller: Oh, John, everyone asks that. I wonder why. It's an information sharing and analysis center and it's a public-private partnership, and it was set up actually by the White House. There's a presidential directive out there from 1998 that requires ISACs to exist to protect our critical infrastructures from threats and vulnerabilities. There's about 25 out there. So for financial services, retail and others, hospitality. They're all over the place.

John Gilroy: So I guess the term we could use it as an ISAC can be sector-based or categorized, is that right?

Erin Miller: That's correct.

John Gilroy: So we have ISACs for IT. We have ISACs for aerospace and so now we have one for just regular old space. So why here? Why now? Why space ISAC?

Erin Miller: Well, I like how you call it regular old space. So why now? Well, we've obviously started evolving our market sector for space. Just being here at this conference you can see how many companies there are new and emerging technologies for space and unfortunately that brings some risk to the industry, and the federal

government in the United States has come out and said that they want to protect this sector and they want to back that. So that means we're going to have a space dedicated ISAC and it's the only one that will address space from a commercial and international perspective.

John Gilroy: We've been here a couple of days, we see all kinds of people walking by the booth here and I would suspect if we could peer into their little brains they're interested in innovation, and creativity, and doing new and creative things. Maybe cybersecurity is not really in the top 10 list there is it? And this is what you're talking about and they should have it in the top 10 list. Maybe it should be one.

Erin Miller: Yeah, that is what I'm saying. And it might not be right now and I know that's probably the perception that right now it's not about cybersecurity it's about innovation, but we really need to build cybersecurity into our innovation. We already learned that the hard way with IT and then with cyber and now space. So IT security is ITSEC, that's the beginning of all of this and now space is just that next layer we need to add on.

John Gilroy: So who are the founding members or the companies that precipitated the space ISAC?

Erin Miller: Well, we've started building our founding membership board. So we have several committed members. Lockheed Martin actually just verbally committed to us. So we're really looking forward to formalizing that partnership. We have Kratos Defense from the government side. We have the White House, NASA, National Security Council. They actually got on stage and announced this with us at the Space Symposium in April of this year, and we have some others that have joined just this week. Booz Allen Hamilton announced and we announced it in the press, at least 65 tweets have gone out on that topic.

John Gilroy: Wow. Space Dynamics Lab, we had them as earlier guests in the podcast here but these are some big hitters here, isn't it?

Erin Miller: Yeah, we have Space Dynamics Lab and we have MITRE too.

John Gilroy: Now, I understand that's the Space ISAC is housed at the National Cybersecurity Center. Tell us a bit about the NCC and how it relates to the Space ISAC.

Erin Miller: Yeah, so the NCC, The National Cybersecurity Center in Colorado Springs is a community member-driven organization and we have training for executives. We do training at the K through 12 level. We also have a big annual cyber summit. It's in September on the 19th and 20th this year at The Broadmoor hotel in Colorado Springs. I highly recommend checking it out. We will have a

space ISAC panel there. Where we will talk about the commercial and international space assets that are being developed and how they can be used by the military.

John Gilroy: Now, I've done interviews with people talking about debris in space and space junk, and I don't know, maybe from my simple perspective it looks like that a lot of the vulnerabilities are space junk colliding out there, maybe interference or something. So what type of cybersecurity vulnerabilities do you see in space that you can share with us?

Erin Miller: So space junk is, of course, an issue. We need to manage that. A lot of the cybersecurity vulnerabilities that we're going to be addressing in the ISAC relate to manufacturing, launch, payloads, communication, services. So it runs the whole gamut of the space system, and when we're looking at manufacturer we're especially looking at the vulnerabilities to the supply chain. So just one example that we've already learned about in the ISAC. We ran a secure GPS seminar for critical infrastructure and key resources just a couple months ago, and we had all of our members there, we talked about GPS and the security vulnerabilities to GPS. Do you know you can buy jammer on the internet for 20 bucks? This is basic stuff here.

John Gilroy: Wow. When I think about, you know, I'm driving around Ogden, I'm lost, I get out my phone and GPS helps me all the time. So beyond navigation give us an idea of what GPS provides or how it helps or hurts people and small satellites.

Erin Miller: Yeah. when we were at that seminar then we talked about emergency services, commercial aircraft, which is an obvious one I hope to most of us. Energy metering is actually using GPS to track how much energy use you have in your business or your home. Financial transactions are connected to GPS, ocean liners. Actually, GPS impacts all of the critical infrastructures. There are 16 of them so everything that we do in our daily life that's been deemed as a critical infrastructure is connected to GPS is what it comes down to.

John Gilroy: So we talked about the cybersecurity vulnerabilities. We talked about space assets up there. So what kind of risks do we have when we look at the smallsats and space assets out there?

Erin Miller: Yeah, we're looking at, I mentioned the supply chain. So operational technology and the business systems that we have within these companies. A lot of us, well, especially in my previous work experience we've had to start protecting our intellectual property of our companies, which includes your business system for your satellite. Maybe you're a supplier and you have a patent that you need to have in place. Well, there's other proprietary information, trade secrets that people can steal. So we clearly need to be protecting those things in addition to

the mission. And the mission is that technology that's out there and what's in flight, the payloads that are in flight, it can be compromised. So there's those three various aspects of threats and vulnerabilities that we'll be collecting information on. It's all anonymous though, I have to throw that out there for you. We're not planning on disclosing that a company has been actually hacked. That's not the goal here.

John Gilroy: Now, when I think of supply chain I think of buying a Cisco router that was maybe manufactured in China or another country and having some kind of problem with it, but supply chain can also apply to software too. And I think the whole concept of vulnerabilities, it's cyber vulnerabilities is ... [inaudible 00:08:28]. It's really hard to understand. Thousands of people have listened to this podcast all over the world. They come up to us at the show and tell us so we know. So if you're listening now and want to get email alerts when new episodes are available, go to Google, type in Constellations Podcast. Go to the Kratos site and give us your email address and we'll send you out an email, and the next time we have someone like Erin in front of a microphone.

Okay, surprise. This is the part of the show where I read a quote, could be from Ben Franklin. I read a quote, you've got to identify who said it. Here's the quote, "Our space community needs timely, actionable information to respond to attacks. We can only do this if we work together in a high trust information sharing environment." Who said that?

Erin Miller: That was me.

Erin Miller: That high trust information sharing environment is what I am super passionate about.

John Gilroy: You should put this on a T-shirt and get a T-shirt gun here at the concert and say, "Hey, before you develop that next smallsat open your eyes."

Erin Miller: Right.

John Gilroy: Trust is something in the Washington DC area where I'm from. That is kind of a difficult proposition, you know? And I think when you're talking about commercial organizations and federal organizations, you crossover into military, you crossover into an intelligence community this gets to be a very easy concept to put on paper. High concept to enact, isn't it?

Erin Miller: Yeah. The ISACs, a lot of them have experience with this already so we're expecting to share information with them. That's inherent to the nature of this whole thing, is that the ISACs have experience building trust in the community and they have already learned how to do that and the space ISAC will do the

same thing. We hope to do it really well because we are including the entire international community as well and that means we're going to need that trust piece so that people will participate.

John Gilroy: So the space ISAC, is it focused primarily on commercial space or do you coordinate with the DOD as well? Department of Defense.

Erin Miller: Yeah, that's a really good question. We are coordinating with the DOD and a lot of people may assume because of all the talk about US Space Command that we're not just coordinating with them but they're leading this. They're not actually leading it. It's a combined effort across at least 18 different government agencies to support, not through even funding, but support as a sponsor the space ISAC to exist. So it is a true public-private partnership where we'll have NASA, National Security Council, members from National Space Council will participate, which covers a wide variety of agencies like Department of Commerce and others.

John Gilroy: Well, here we are at the SmallSat Conference and you can't have big satellites or small satellites without something going on the ground. So my question to you is, what about the Space ISAC focus? Does it focus on cybersecurity threats to ground stations as well?

Erin Miller: Yeah, I think every fifth company I'm going to say that I've seen here is doing something related to the ground. They're either building the ground segment, they're doing ground as a service, or they build ground stations. I would say that physical security is a very clear aspect to that, but if you have data that's coming down through your pipes, so to speak, then you need to be concerned about security because there's a lot that can be gleaned from that information transfer.

John Gilroy: Yeah, I spoke those words earlier this morning. Ground station as a service. It's a relatively new phrase, isn't it?

Erin Miller: Yeah, it is. It's very interesting to see how we're turning everything into a service and the more we do that the more security concerns we're going to have, unfortunately. I hate to be that person, but that's just how it's going with the industry is that as these new companies emerge they can't just do lowest price, technically acceptable so to speak. We really need to take into consideration designing that cybersecurity element into it.

John Gilroy: Well here at this SmallSat Conference there's lots of small companies, and if I were to drag you down one of the aisles here and place you in front of a SmallSat company. So how would you explain to them how space ISAC can help them?

Erin Miller: I would say that as a small company then you don't have a lot of resources to be able to just hire 20 different experts in cybersecurity and because you do space does not mean that you are a cybersecurity person, or are you completely aware of all the threats and vulnerabilities. That's why we need to come together as a community so that we can build out that space layer security, and when the community comes together the sharing of the information is what creates the standards. So that prevents an environment where people feel like standards are just going to come imposed upon them without them having a say in the matter. And because we have so many US government entities that are involved and sponsors of this, then they're going to be listening, they want the information exchange and they have information to share as well. That's the other reason for the creation of the Space ISAC.

John Gilroy: I was at your website today and the phrase space threat comes up, and 10 people, 10 different interpretations of what a space threat is. Some people think of only military threats or congestion can be a threat too. So you monitor both?

Erin Miller: Yeah, the congestion thing, as soon as there's some human flight happening and someone hits something in space, then yes, we're going to have some issues there. It hasn't happened yet. We don't have active human flights that are up there, but there's technology that's being developed to manage the space debris issue. I don't think that's where the ISAC is going to start. That's just my instinct about the situation as we begin the information sharing and we have the founding board members then our concerns are going to be more about those business systems that I talked about, and then evolving to the operational technology as well as the mission itself.

John Gilroy: This morning, I picked up my phone, look what the weather's going to be and my newsfeed, you know, satellite launches are front-page news these days and feeds are coming all the time for it. I would guess with the proliferation of launches in the next few years the congestion threat can't be too far behind. Would you agree?

Erin Miller: Oh, yeah. I've sat in sessions this week and I've heard that congestion is definitely an issue and you know, John, I'll say it again. I don't think that is the number one concern that the ISACs going to address.

John Gilroy: We talked about members of the Space ISAC, some of the founding members. Some pretty big-name organizations. So what type of companies? I know MITRE is a nonprofit, couple those are profit. So what kind of companies are attracted to supporting Space ISAC?

Erin Miller: Yeah, we have companies from all over. As you mentioned, we have universities that are involved. So those universities that we're talking to have a lot of

research and development in space. We also have UARCs and those entities are associated with a university. We're talking to some federally funded research and development corporations. The next groups that we're going to be talking to I think are a lot of the small businesses and mid-size businesses, because as we have established our founding membership board those companies are going to be interested in learning about the threats and vulnerabilities that are occurring in the industry so that they can prepare to respond. There's also a lot of training and resources that'll be made available to them so they can take action, and when they get the information it's all actionable information and if you can't respond, you're not equipped, then it doesn't do much good for your business. But I can say it's going to protect your bottom line if you're willing to put in a little work to get trained from the ISAC.

John Gilroy: Yeah, it's the perfect way for a growing satellite company or a smallsat company to take and inexpensively take advantage of this wealth of information that these groups provide for them and sharing, and if you can establish that trust that would be I think the toughest part of the whole job, establishing trust and then everyone can take advantage of it. I looked in your LinkedIn profile, you've got a wide background, and if you try and look in the future, so what do you think the biggest challenges are for space ISAC in the next four or five years ahead?

Erin Miller: So let me think about that for a second here. Because I don't think that it's a technological challenge. We've got Moore's law happening here. It's not the technology that we're concerned about. It's really about the people. The technology has to be secured, but the only way to do that is to have a cultural transformation, and with IoT, 5G all the new constellations going up in Leo, it impacts transportation, it impacts our way of life. So I think the people just in general who are entrepreneurs and small business owners as well as the larger corporations we have to fully embrace this and we have to come together as a community, and that's going to be our biggest hurdle is getting that culture transformation.

John Gilroy: And the hardest one too, I think. The technology's almost there, but boy, human beings, that's tough. Well, Erin, unfortunately we are running at a time. I'd like to thank our guest, Erin Miller, Director of Business Development National Cybersecurity Center.