SLTPS-PAC 2018-01-24, Audio Recording

F: You never know [his address?] from day to day (inaudible) (laughter) [should have worn?] my sneakers. (overlapping dialogue; inaudible)

MORGAN: Hi, hi, Nancy Morgan, CIA.

F: (inaudible)

MORGAN: Nice to meet you (overlapping dialogue; inaudible)

F: Fine, how are you? [I feel like I met?] a few of you before, actually (overlapping dialogue; inaudible)

KERBIN: Valerie Kerbin, I’m with DNI, [so?] (overlapping dialogue; inaudible) (laughter)

F: (tone) (inaudible) [going to make it?] (overlapping dialogue; inaudible) I’m going to have my shoes off, jacket on. (laughter)

F: I understand. (laughter) [You go hot and cold, so?] (laughter) I understand.

F: [Yeah?] (inaudible) this week (inaudible)

F: Oh, my goodness. (laughter) (overlapping dialogue; inaudible) this [has been the oddest winter?] (overlapping dialogue; inaudible)

F: I know, yeah, 70-degree swings in five days [were kind of?] -- (laughter)

F: Right, and that’s only after being, you know, in the single digits for nearly a week, and snow -- (laughs) (overlapping dialogue; inaudible)

F: Well, it’s okay, we’ll make it through.

M: Check. (overlapping dialogue; inaudible) (tone) (overlapping dialogue; inaudible)

F: [Right?] (inaudible) [well, it’s?] nice to meet you (overlapping dialogue; inaudible)

M: Check. (overlapping dialogue; inaudible) (laughter) (overlapping dialogue; inaudible)

M: [Ten-four?].

M: Well, thanks for coming (overlapping dialogue; inaudible) [we almost didn’t have it?] --

F: I know, I know, [I was?] (overlapping dialogue; inaudible)

M: We’re looking forward to your presentation.

F: (inaudible) thanks.

M: Yes (overlapping dialogue; inaudible) [thanks for coming?]. (overlapping dialogue; inaudible) (tone) [STEINMETZ?]? Good morning, it’s [Mike Steinmetz?]. (tone)

M: [How’s it going?]?

M: How you doing (inaudible)

M: [All right, yeah?] (overlapping dialogue; inaudible) (tone) (overlapping dialogue; inaudible)

M: It’s [all so quiet here?].

M: Isn’t it? (laughter) (tone) (overlapping dialogue; inaudible)

M: Morning, how you doing?

M: I’m well, thank you. (overlapping dialogue; inaudible) (pause)

F: Good morning. (pause)

M: Okay. Okay (inaudible) two reminders (inaudible)

M: All right.

M: Oh, yeah.

M: -- the administrative stuff, so (overlapping dialogue; inaudible) on the phone -- ask them to mute their phones.

M: If they can.

M: If they can. And then, also, around the room, there is another mike over there. [People might, you know, need that?].

M: Over there?

M: [Over at the?] (inaudible) [table?]?

M: Okay, got it.

M: (inaudible)

M: Yeah. Yeah, thank you.

M: You’re welcome. (tone)

F: (inaudible)

M: (inaudible)

F: That’s what I was guessing (overlapping dialogue; inaudible)

M: Okay. (overlapping dialogue; inaudible) okay.

F: (overlapping dialogue; inaudible) your phone number [is?] (overlapping dialogue; inaudible)

M: All right. (overlapping dialogue; inaudible) (laughter)

M: Okay, [all right?].

F: (inaudible)

M: You want [those?] on the telephone to mute their phones?

F: [There was a?] meeting yesterday where they [did that?] (inaudible)

M: Well, they -- yeah, he said that, if they can, remind folks to mute --

F: Yeah.

M: -- because, apparently, it’ll create interference. So, if you want to say that for -- that’s fine. (overlapping dialogue; inaudible)

F: In the other meeting, they had ones with dry erase boards you could write it on. This one woman did this gorgeous picture throughout the meeting.

M: Oh.

F: [Right?]?

F: Yeah, (inaudible)

F: Gorgeous [painting?] (overlapping dialogue; inaudible) artwork for her agency seal and (overlapping dialogue; inaudible)

M: -- she called it (overlapping dialogue; inaudible)

F: That clock is confusing me.

M: Yeah (overlapping dialogue; inaudible)

F: [Okay, so it’s?] five of eight. (laughs) (overlapping dialogue; inaudible)

F: I’m good, [yeah?].

M: (inaudible)

F: [Was good?].

M: [Oh, yes, sir?]?

M: Do you (overlapping dialogue; inaudible)

M: [Okay, sir?].

M: Okay. (laughs)

M: Oh, yeah (inaudible)

F: Yeah.

M: (inaudible)

F: Happy where I am.

M: Can you get that other (overlapping dialogue; inaudible)

F: Is their rep coming today?

M: [You miss some of the people?] (overlapping dialogue; inaudible)

M: Oh, yeah, [it’s?] -- do you remember [Christa?] (overlapping dialogue; inaudible)

F: Really?

M: Yeah.

M: Okay.

M: (inaudible)

M: (overlapping dialogue; inaudible)

M: Yeah, no, that’s -- I was checking the list (overlapping dialogue; inaudible)

F: Thank you.

M: Yeah (overlapping dialogue; inaudible) (laughter) (tone)

F: -- yeah (overlapping dialogue; inaudible)

M: -- [everything?] --

F: -- [participated?] --

M: -- [near BWI?] (overlapping dialogue; inaudible)

F: Okay. (overlapping dialogue; inaudible)

M: Yeah (overlapping dialogue; inaudible)

BRADLEY: All right, shall we start?

M: Yes, sir.

BRADLEY: All right.

M: Okay.

BRADLEY: Welcome. We came within a hair of canceling this meeting because of the shutdown, and we decided to hold off, given the instability up on the Hill, and our gamble paid off. So, welcome to everybody who is here today. I’m glad we were able to work this in, because the next one’s not ‘till July. So, you know, it would have been a logistical challenge to reassemble the group. All right, this is the first SLTPS-PAC meeting of 2018, and the 14th overall. This is a public meeting, subject to the Federal Advisory Committee Act. The minutes of the SLTPS-PAC are available to the public. The meeting’s being audio recorded. The microphones around the table have enough cord to be repositioned in front of anyone who wants to speak. (tone) Four microphones, located at the left side of the room for audience members to use. Anyone who is making a presentation but not sitting at the table can use the podium to give your briefing. This is important, this next point: please identify yourself when speaking so we can have an accurate record of your comments. Again, we’re making a transcript of this meeting, and it’s devilishly difficult to go back and say I think that was him. No, it was actually her, or -- who said what, so just to be able to give order to this, we’d like for you to identify yourself. And if I jump in, it’s not because I’m rude. I’m going to remind you to please identify yourself, so we can keep our transcript clean. This is particularly important, too, for the people on the phones who aren’t here, if you can remember to please identify yourselves, right. So, administrative thing-- we’ve had some membership changes since last time we met. [Tip Wright -- White?], who was our ST -- LTPS vice-chairman changed jobs -- [had no one able?] to serve on the committee. [Ben Langang?], four time -- four-year term expired in December, and [Dewey Webb’s?] term ended on January 14th. We will miss them on the committee and thank them for their service. So, in order to deal with this, we called on SLTPS [entity?] members to select a new vice-chair, and we sent a request for nominations from the full membership. I’m pleased to report -- (phone rings)

M: [Sorry?].

BRADLEY: (inaudible) I’m pleased to report that the SLTPS entity members selected Jeff Friedland as their new vice-chair. Thank you, Jeff, for stepping up to serve, and congratulations on your selection. We received --

FRIEDLAND: Welcome the opportunity.

BRADLEY: Oh, you -- thank you, back. We received nominations from the membership of five very strong candidates to fill the three open positions. I made the selections and can announce two of them today. I’m pleased to welcome Thomas Woolworth, president of the National Native American Law Enforcement Association, and Mike Steinmetz, Rhode Island principal advisor for homeland security, cybersecurity, and counterterrorism. The other perspective member is still in process, and I hope to announce the selection very soon. On the federal side, there -- also a number of changes. Elaine Cummins, the FBI member, retired in early December, and Rich [Homan?], the ODNI member, retired the end of the year. From the FBI, Christopher Jones, Office of Data and Information Sharing, Office of the Chief Information Officer, is at the meeting today. From the ODNI, we have Valerie Kerbin, senior security advisor, special security director, Office of the Director of National Intelligence, National Counterintelligence, and Security Center. Right, let's go around the room and introduce ourselves. I'm Mark Bradley, Director of ISOO.

PANNONI: Greg Pannoni, associate director, ISOO, and designated federal official for the meeting.

ROGERS: I'm Charlie Rogers. I'm the DHS rep, and I deal with state and local security.

JONES: Hi, I'm Chris Jones.

BRADLEY: Oh, yeah.

JONES: I was introduced before, replacing Elaine Cummins. I'm with the FBI's Office of Chief Information Officer, Office of Data and Information Sharing. I'm the unit chief there.

MORGAN: I’m Nancy Morgan from CIA. I’m the director, information management services.

SUVER: Hi, good morning. I’m Roisin Suver with the Multi-State Information Sharing and Analysis Center, and I’m their senior liaison to the NCCIC.

SMITH: Brandon Smith, Department of Transportation Information Security.

[TAYLOR?]: [Yusef Taylor?], ISOO.

KERBIN: Valerie Kerbin, DNI.

WRIGHT: Natasha Wright, Department of Energy, here for Mark Brooks.

MASCIANA: Leo Masciana, State Department.

BRADLEY: Okay. Welcome all around the table. All right, those of you on the phone -- you please identify yourselves and where you’re from?

STEINMETZ: Mike Steinmetz from the State of Rhode Island.

BRADLEY: Hi, Mike.

PARSONS: Darryl Parsons, Nuclear Regulatory Commission.

BRADLEY: Darryl.

SCHOUTEN: Mark Schouten, State of Iowa.

BRADLEY: Great.

FRIEDLAND: Jeff Friedland, St. Clair County, Michigan.

BROUSSARD: Derrick Broussard, [Defense Security?] Service.

M: [That’s right, yeah?].

BRADLEY: Yeah.

F: (inaudible)

M: Didn’t hear that one.

BRADLEY: We didn’t hear the last one. Would you please repeat that? Anyone else on the phone?

GUIER: Linda Guier, Department of Transportation.

BRADLEY: Okay (inaudible) anyone else?

WOOLWORTH: I don’t know if you were able to get me. This was Thomas Woolworth with the National Native American Law Enforcement Association.

BRADLEY: Okay, [yes?]. Okay, thanks, Thomas.

WOOLWORTH: Thank you.

BRADLEY: All right, anybody else? All right, I guess they’ll join us in process. A reminder for the federal members sitting around this table regarding the financial disclosure forms we need. It’s been more than a year since federal government members submitted their financial disclosure forms to NARA. NARA’s required to make sure that the federal government members of advisory committees and their designated alternates do not have an actual or apparent conflict of interest with respect to service on such committees. For that purpose and subject to the bylaws of the SLTPS-PAC, NARA’s Office of General Counsel -- responsible for reviewing members’ financial disclosure forms. Federal government members and alternates will need to send either an OGE Form 450 or OGE Form 278, whichever form you are required to file with your home agency -- [Gene White?], assistant general counsel here at NARA. The process will be the same as last year, and the SLTPS-PAC staff will send their fellow members an email with the specifics. So, if you need any help with that, just let us know, all right? Lastly, please note that in the folders, these blue folders, there are copies of the agenda, meeting -- or the -- yeah, the meeting agenda, the slides for one of our presentations at today's meetings, and the minutes of the last meeting, all right? I'm going to turn now to Mr. Pannoni and go over old business.

PANNONI: Okay, thank you, Mr. Chair. Good morning. It's Greg Pannoni again. We -- a couple of things. Course, the minutes, as were just mentioned, were finalized and certified on September 8th, 2017, and once again continues -- with budgetary limitations, [we're?] unable to provide reimbursement for travel and per diem. And so, the option of telephonic communication is what we have. So, if anyone did travel to the meeting, thank you for doing that on your own dime. We have one action item from the last meeting, and this one is documented in the minutes, but I'll just go over it. It was to have a group -- convene a working group with representatives of the federal side of this committee to study the multiple, separate, and unconnected security databases in the executive branch and the effect this has on effective clearance reciprocity so that we could identify steps that could be taken -- can be taken to address any obstacles to reciprocity that may exist because of current clearance database deployment. So, that’s a big mouthful, but -- so, we did. We had that meeting, on January 12th, here at the archives. And some of you around the table participated. We had representatives from the Performance Accountability Council Program Management Office. We had the National Background Investigations Bureau, Office of the DNI, Director of National Intelligence, Office of the Undersecretary of Defense for Intelligence, Department of Homeland Security. Ourselves, ISOO. And the FBI had planned to attend but was unable to because of a last-minute commitment. So at the meeting, we discussed the various aspects of this issue that would allow select SLTPS personnel access to clearance information. As you know, this whole area of access to databases has been around for quite some time. I would say the IRTPA, the Intelligence Reform and Terrorism Prevention Act of 2004 that was signed into law by President Bush formalized this, that there would be a central verification database. I’m sure most of you, if not all of you, know that. So won’t go into a whole lot of detail on that, but essentially the government -- U.S. government cobbled together not just that as the database that OPM is responsible for overseeing, but it also leveraged that the intelligence community scattered castles for sensitive compartmented information -- the Department of Defense’s JPAS, Joint Personnel Adjudication System for their data -- and the idea was -- is that all that would feed in, although there was an exception that, in the instance of concerns about national security, some of that data could be withheld. In any event, we do address this, also, in the executive order that establishes this program, the Classified National Security Information Program for State, Local, Tribal, Private Sector. There’s, you know, some line items in there that speak to both reciprocity of personnel security clearances and facility -- physical spaces, and also of DHS having a role in tracking clearances. So what happened was, as I understand it -- and we talked about this at the meeting -- when the order was written, the SLTPS order, a group of folks representing the various agencies that have responsibility for the databases convened, and the idea was, well, let’s leverage what we have, primarily meaning the OPM central verification system. And so, a portal was created that would enable DOD to enter their data for SLTPS personnel as well as FBI and any other sponsoring agencies that issue -- conduct investigations and issue clearances for state, local, tribal, private sector personnel. I believe, for the most part, it’s working. But what came up at our last meeting, sort of via another issue that was more tactical, ultimately, was this issue of access to databases by state, local, tribal personnel. And it was primarily the inability for those that were granted clearances by the FBI to be able to access that clearance data. So, we had that discussion. As I say, unfortunately, the FBI was unable to be at the meeting, but the takeaway from the discussion was that the NBIB, the National Background Investigation Bureau, while there was an understanding of concern, not just among -- by them, but by others in the meeting that there might be some national security concerns for FBI operational personnel and not wanting to share that data in the central verification system. It was not clear why that would be a concern for state, local, tribal. So, the NBIB rep agreed to reach out to the FBI concerning the submission of clearance information for state and locals to the CVS. That was one takeaway. The other was for the DNI rep that was at the meeting, as well. Since they’re the executive agent, they would also follow up with FBI, as they have an interest in ensuring reciprocity, and without that data residing in a system where it could be accessed by the pertinent personnel, that does stymie reciprocity. So, that is essentially what was covered in the meeting. Our PAC PMO, Performance Accountability Council program management rep indicated the obvious -- the long-term plan is to have a single repository. But there's no real timetable for that. On a related note, there is a security executive agent directive, Number Seven, which is entitled "Reciprocity of Background Investigations and National Security Adjudications." That is in draft, according to our PAC PMO colleagues, it's out -- or it's come back in. There's been quite a number of comments, and they are being adjudicated as we speak by the DNI's office. So we will keep you, the membership, updated as we obtain responses to these issues that I've noted. And that's it. Any questions?

BRADLEY: Is there any solution to this, or is it just going to go on and on and on? (laughs) Is that --

KERBIN: [It's a work?] (inaudible) (laughter)

BRADLEY: [That's what I?] hope to hear.

KERBIN: -- the entire government (inaudible)

BRADLEY: Yeah, no, I know.

KERBIN: -- and now it’s complicated, you know? We’re all working on the backlog and mitigation --

BRADLEY: Right.

KERBIN: -- efforts and, you know, working with the PAC closely and the other executive agents to try and, you know, come to some solutions. But it’s a big --

PANNONI: That’s our DNI rep, by the way.

KERBIN: (inaudible)

PANNONI: For the record.

BRADLEY: Yeah.

KERBIN: Yes.

BRADLEY: Thank you, Valerie.

KERBIN: Yes.

BRADLEY: Okay, any more comments on this before we go to new business? All right.

ROGERS: So, [I’m?] Charlie Rogers. I’m [going to do this?], and usually I give some metrics about what we’re doing. Some of this is old news to people, what we are doing, so I’m not going to take a long time describing it. But we do have a security compliance program that goes out to state fusion centers on a regular basis to validate that they’re operating and managing their classified information appropriately. We started that program in late 2012. We’ve done -- I’m told we’ve done 89 SCRs, so -- since

2012. Last year, we did 13 security compliance reviews. In FY ‘18, we’ve completed five, and we anticipate doing 11 more, for a total of 16 this year. So, that’s an ongoing program. It seems to be doing pretty well. I mean, we could always improve it. We can always revisit how we do it. But it’s been established for some time. Within the states, the state fusion centers, the implementing directive to the executive order requires the state fusion centers to appoint security liaisons, and those are the reps in the field that -- is our direct conduit to manage how they are to work with -- as to how they manage their classified. So because there’s turnover with those folks and because they’re an essential, key element in safeguarding the classified in the field, we conduct webinars with them. We sometimes do eight to 10 a year, it really varies. We do that with our -- in conjunction with our intelligence and analysis folks. Last year, we did seven webinars to conduct training with the security liaison. So, we reached 49 security liaisons to [refresh their?] training with them on how to manage their secure room and any other pertinent issues that come up. This year we’ve done four, and we’ve only trained 10 so far, but we’ve done four webinars in FY ‘18. Then we have a more robust security liaison training program, which is primarily funded by our intelligence and analysis partners, and it’s a combination of security training and other useful training. And those seminars are located in Washington, and the newly appointed security liaisons fly out to Washington. So we do about two a year, lately, and train about six to eight persons per session. Last year, there were two events and 14 personnel were trained, and that’s pretty comprehensive training. I mean, it’s two days you’ve got people from COMSEC coming in. You have intelligence and analysis folks coming in and talking about the secure network and how to use it. You have traditional security education. So, none have occurred this year yet. And in the area of personnel security, metrics -- or not so much metrics, but numbers -- we’ve stayed about the same lately. We have about 1,900 private sector personnel who have security clearances that are primarily sponsored by our NPPD partners who have the cybersecurity and infrastructure mission. And we have about 5,600 state and local personnel who are cleared. So that’s a total of about 7,500 security clearances to state, local, tribal, private sector --

RADLEY: (inaudible)

ROGERS: Well, there’s a level -- almost all of them are secret, but there are 380 that are either TS or have TS-SCI access. So, the requirement for them to get TS-SCI -- the operating level in state and local is secret. The fusion center secure rooms are certified at the secret level, but we do have some of them work in JTTFs, and we have some that are detailed back to INA and work in [SCIFs?] in INA. We have some that are co-located. They have a fusion center that might be co-located with the National Guard that has a SCIF, and so some of those people -- clearances are upgraded. But TS with an SCI access is considered exceptional, so there has to be some rationale and reason for doing it. That’s pretty much it for my metrics, unless there’s any questions on that, or --

PANNONI: Does DHS -- Greg Pannoni -- does DHS have any insight into collectively how many other clearances are held for state and locals and private sector by the U.S. government, outside of DHS?

ROGERS: Yeah, not -- well, we know FBI is the next biggest player, I believe, but we don’t know because we don’t -- yeah, we don’t really track that. Under the executive order, each agency have the authority to clear their own personnel. So I mean, I guess we could talk to OPM to find out what’s -- who’s in a CVS, but I don’t know what the numbers are, total, for other agencies. I think we’re the biggest player by far, and then the FBI is the second, at least that’s my best guess.

PANNONI: Right.

BRADLEY: DOE probably has some.

ROGERS: Yeah.

PANNONI: Yeah.

BRADLEY: I’m [sorry?] -- yeah, [you can?] -- please, [go?] --

F: The NRC, also (inaudible)

ROGERS: Yeah.

BRADLEY: NRC.

ROGERS: Yeah, NRC would have -- yeah, yeah.

BRADLEY: All right, well, thank you, Charlie.

ROGERS: Okay, well, I was going to talk a little bit --

BRADLEY: Oh, I’m sorry.

PANNONI: (inaudible) two other --

ROGERS: -- about -- couple other bullets.

BRADLEY: Yeah, [right?].

ROGERS: And this may be more interesting to ICE [than to?] anybody else. But when the executive order was approved 13549, DHS stood up a division called the State and Local, Tribal, Private Sector Security Management Division. And it’s that division that had security specialist and personnel security adjudicator, which pretty much ran the programs I just spoke about. But we recently went through a realignment in the Office of Security, and this is just more for informational purposes, but the State and Local, Tribal, Private Sector Security Management Division has gone away. It’s now the Compliance, Standards, and Training Division. The state and local functions reside in the Compliance, Standards, and Training Division, and there’s a branch in there that does all the things that aren’t spoken about. We also have a branch under construction that would do this -- there’s a new industrial security program called the hybrid, and depending on how big it becomes, the compliance piece for the hybrid would be in that -- in the division. Then, the other things that were added to the division -- is all the Office of Security Compliance programs -- were transferred into the division. And our training function was transferred into the division because it was felt that they all kind of circle back and connect to each other. They -- the direct support, the oversight, and the training. What moved out of the division was the personnel security adjudicators. They were sent back and recombined into the larger personnel security division, but we don’t see that as a negative impact, because we have open lines of communication. The purpose of the realignment was -- the Office of Security was established when DHS was established and sort of grew incrementally. The new chief security officer basically wanted to review and make -- get rid of the duplication of any functions we had -- and to combine like functions into single entities, and he wanted to focus on a more strategic enterprise-wide office. And not that we don't do direct support, but to make sure that they were separated and not commingled, so that we could have a better ability to focus on those goals. And I think that pretty much covered what I wanted to say about the realignment. The last --

BRADLEY: Could I --

ROGERS: Yeah?

M: Could I ask a question?

ROGERS: Yeah, [sure?].

M: [Where the?] -- so, from what I'm gathering, the realignment, the Compliance Standards Training Division will oversee and cover the safeguarding aspects of why we have this program. And there's two things, right?

ROGERS: Right.

M: We had -- it was -- the idea was to promote sharing and standards for safeguarding among this non-federal population. So, my question is: does DHS have some sort of an office or -- doesn't have to be an office, but some mechanism or function that looks at the sharing piece and looks at it from -- how are we doing? Are we enhanced? Do we -- enhancing our capabilities in terms of sharing with either the SLTPS community, or do they gauge and measure that sort of thing?

ROGERS: Yeah, and we’ve had some guest speakers, I think. Kevin [Saup?] was a guest speaker here. I can’t really speak authoritatively. Susan, you could chime in if you like, but INA has the information sharing mission, and they are responsible for the sharing of both classified and unclassified information with the state and locals, primarily, and they have all kinds of measurements and mechanisms by which they measure the performance of fusion centers. Our role in the Office of Security is to facilitate the environment.

M: Right.

ROGERS: [What -- and our?] role is to ensure that if there’s a desire to share classified information that there are places that meet standards, and that the people are trained and that there’s -- the -- they’re safeguarding the information. But primarily, that’s with INA. Of course, NPPD also shares information, but INA supports them for intel [and?] -- did I leave anything out, Susan, or --?

BOWER: No, I don’t think so. So, we do (inaudible)

ROGERS: This is Susan Bower, she’s (inaudible)

BOWER: I’m sorry, Susan Bower --

BRADLEY: That’s quite all right.

BOWER: -- from INA. So annually, there is a fusion center [assessment?] (inaudible) your question, but they -- I’m sorry. So annually, INA does execute our performance management and evaluation branch executes a fusion center assessment. And the fusion center’s self-asses where they are and where we are in terms of information sharing, and they provide that data back to INA. And so, that effort for this past fiscal year -- we’ve done it since 2011. We publish an annual national network of fusion centers report, and the latest effort just culminated, I believe, December 1st, and so they’re validating the data right now and should be coming out with this fiscal year ‘17 report in the coming months.

M: Okay, yeah, I have --

BOWER: And we -- they also work very closely with the fusion centers on the performance metric aspect of that so that the fusion centers are aware of the questions that are going to be asked. And we have buy-in with them.

PANNONI: Thank you. That -- [that’s up and -- this is?] Greg Pannoni. We can share, right, with the committee, those reports, I think --

ROGERS: [Yes?] (overlapping dialogue; inaudible) publicly --

PANNONI: [Yeah, but?] --

BOWER: Absolutely. Yes, they’re (overlapping dialogue; inaudible)

PANNONI: -- publicly available, okay (inaudible)

BOWER: -- they’re on the DHS [website?].

PANNONI: -- right, okay. Sorry, yeah.

ROGERS: And just a last thing, I wrote new initiatives. And [under?] -- and I was going to talk a little bit about the Security Executive Agent Directive Three on reporting requirements for personnel with access to classified information. And DHS, like other federal agencies, are working to, you know, meet the requirements of C3. But within C3, State, Local, Tribal, Private Sector are called out as covered folks. So, we’re working -- I’m not personally working, but one of our divisions, the -- you know, I’m going to look it up because of the realignment. (laughter) [At one?] of our divisions, the Center for International Safety and Security Division, has taken on the primary task of working to create a system, a database, to enable DHS to do this in a more efficient way. And state and locals are going to be incorporated into that database. So, it looks -- I don’t have a lot to share, but it looks like we’ll be creating a mailbox that state, and locals can go directly to, and then this can all get evaluated. So more to follow on that, but I just wanted to say frequently, as -- because the state and locals are now under the executive order part of the federal government, and they’re considered full partners, when these kind of directives come out, we -- in DHS, we have the initial challenge of meeting our own requirements, which can be, you know, challenging for anybody. But we also have to figure out, how do we get this diverse population into it? So that’s being worked, and that’s really all I wanted to say about that, but, you know --

BRADLEY: Good.

ROGERS: -- so, yeah.

BRADLEY: Thank you, Charlie. That was, as always, useful and good information to have. All right, we’re now going to turn to Roisin Suver, who’s got a long title. (laugher) Program Executive and Senior National Cybersecurity and Communications Integration Center Liaison, comma, Multi-State Information-Sharing and Analysis Center for Internet Security. This is also [Rich Like’s?] organization, so you’re going to tell us about Multi-State Information Sharing and Analysis Center, please.

SUVER: Yes, sir. Hi, everyone. Thank you very much. That’s Roisin Suver, with MS-ISAC. So, just to give you a little bit of background on me, before working with MS-ISAC, I actually worked for the Department of Homeland Security in

Intel and Analysis, and I was with their cyber-intelligence analytic division. So, still work very closely with them in my role now. But prior to moving to D.C. and working with the MS-ISAC and INA, I also worked for the Pennsylvania Office of Homeland Security, and I was also a National Guard member in Pennsylvania, doing intelligence there. So, all of that -- my whole past career comes to the MS-ISAC and -- just following through on supporting state and locals, and it’s always -- it’s been a great privilege -- in working with this community. So, I appreciate your time here today. And what I want to do, what Rich asked me to do, is to give you kind of an overview of the MS-ISAC. I know some of you on the phone line may already know who we are, but what I want to do is kind of baseline it for everyone else in the room as to who we are, who we serve, and the different services that we offer to our members. So, the MS-ISAC is designated by the Department of Homeland Security as a key resource for state, local, tribal, and territorial cybersecurity. So, we’re not all hazards, but we are very cyber-focused in our mission. We act as a critical touchpoint for information exchange and coordination between the SLTT community and the federal government. We are actually headquartered in Albany, New York. It’s actually East Greenbush if anybody knows the area. So we’re up in New York, and the reason for that is because the MS-ISAC or the idea behind the ISAC actually started in New York State, in their Office of Cybersecurity. So, the idea was really to do cyber information sharing. It started out as a small, regional group within the state and then built into a larger coalition of state and local partners. So, the MS-ISAC actually was stood up in October of 2004 under the New York State office, and it wasn’t until 2010 that we actually moved over to CIS, or the Center for Internet Security. CIS, though, is our parent company. CIS does security benchmarks, critical controls, and other services like that. But it’s the MS-ISAC that’s a little bit different under CIS. We are actually under a cooperative agreement with the Department of Homeland Security, so we are funded by DHS to provide all of our services and support to the SLTT members at no cost to them. So, it’s a pretty good free force multiplier there for all of our members. But the stated goal, which still stands today, and I’ll read this one to you, is to enhance cyber-threat prevention, protection, response, and recovery; reduce the cyber-risk throughout the SLTT government cyber-domain by promoting cooperation and collaboration, providing direct technical assistance, expanding awareness of cyber-issues, providing opportunities for education and training on cybersecurity controls, standards, and best practices, alerting and advising on critical threats and vulnerabilities; and functioning as a centralized hub for a multi-directional information sharing between SLTT governments and the Department of Homeland Security. So next slide, please, if you will. So, who we serve. So our membership -- what I love about our ISAC is really our broad and diverse membership. There are a lot of other ISACs that are out there that support the critical infrastructure sectors. So you’ve heard of, you know, the E-ISAC, the energy ISAC, the national health ISAC, the financial services ISAC, and I could go on and on. But there are several ISACs out there -- we all partner together in a group called the National Council of ISACs, working together and sharing information. But what’s different about us -- there are a few things, but what’s different is our unique membership, because we really are across all of the different sectors, as you all know. So our membership includes 50 state governments, the 79 fusion centers. We have 43 tribal government members, over 1,600 local government members. We have law enforcement agencies as members as well, all the state capitols, the -- I think they’re still being called UASI regions, the 72 Urban Area Security Initiatives that were

DHS programs, as well as the public sector. So crossing all of those different sectors, we have airports, ports and authorities. We have transit associations. We have public utilities, K through 12 schools and public universities and colleges, as well as research, medical, and health hospitals and things like that. We have -- down to local libraries for small towns and municipalities. So, we really are pretty interesting in our makeup as far as our members go. Over the past couple of years, we've also been able to incorporate different commissions and different communities of government. So, law enforcement commissions and different groups like that, also, as members. So, we're getting as much information out to the broad audience as we can. With our growing sector focus -- so, for -- in the beginning, when we first started out, it was very state and city focused. So, we've been really increasing our membership every month, which has been really good down at that local, municipal level as well as the public sector. We are working continuously to build out different working groups based on those different public sector entities. We have -- we also have the Homeland Security Information Network portal, the HSIN portal, which is the DHS platform that we also use for our membership. So, there is an MS-ISAC HSIN portal, but also in there, we have communities of interest. So we’ve set up, you know, elections, education, transportation where our members can get together instead of just talking to our very large audience. But they can come together and kind of share within their own community best practices, and ask questions of each other, and see how one might be implementing security standards in their school, say, and then share that type of information. The next slide, please? So, how do we support? So up in East Greenbush, we have our 24-by-7 security operation center. This is where we really focus on providing our technical support and guidance, our intel support and guidance for all of our members. We have the Albert network monitoring system. So, it’s an IDS or intrusion-detection system prevention system that we also have out in the state and local communities. So, we are cover-- right now, we are in all of the states, and with the DHS cooperative agreement, two centers are at no cost to each of the states. So, that’s a pretty good insight into what the states and locals are seeing, as well, in their networks. Doesn’t mean we’re covering all of the networks, but it does give us some good insight and some really good data to understand the different malicious activities that’s occurring on state and local networks and then share that out to the broader audience. So as I said, Albert is the main platform that we use. It leverages thousands and thousands of unique signatures from various data sources that we alert onto our state and local members. So we're taking trusted third-party information, we're taking downgraded information from the intel community, as well as what we're seeing from malicious activity on networks that we are working on and then sharing that type of information out, as well -- as well as from our private sector partners across the different ISAC communities and elsewhere. So because of the large data set that we have, we feel we're in a pretty good position to understand what the SLTT community is seeing as far as cyber-incidents go. We also have an intelligence branch that is out there. They work closely with the 79 fusion centers to provide them intelligence support. Most of the time, we are working at the unclassified level, because that is where most of our members are also operating. We do have a DHS SCIF out in East Greenbush, so we have the capability to work up to the TS level if necessary. But really, by and large, it's the unclassified information that we are sharing. So what they are really doing is looking at the different cyber-actors, their tactics, techniques, the different trends that we're also seeing across the board. Our intel team is monitoring about 200 different threat actors that we have seen target

SLTT entities. So, we have this database that talks about -- that has information on the profile of the actor, the different tactics that they’ve used in the past, and then we can help identify trends and share that information with our federal government partners, as well, and into the intel community. We distribute a lot of different products, very good products, from our alerts and notifications out to the specific members, as well as to the broader products about the trends that we’re seeing over the months. So for example, we send out a monthly situational awareness report. And that is a pretty in-depth product that talks about the previous month’s activity, be it our Albert monitoring system, the different attacking IP addresses and domains, the different malware families that we’re seeing as the top, maybe 10, that we’re looking at. As well as the different incidents that state and locals are bringing to us for our emergency response team to work on and sharing that type of information out with them. But beyond that, it’s -- it talks about all of our different programs, and it is a really good product for understanding kind of what’s going on in the SLTT cyber-domain. So, we also talk about -- we send out a lot of advisories on vulnerabilities, so we see this every week. We’re sending out several different vulnerabilities, patch updates -- patching is really important to do. And so, these are the different types of things that we’re working on. And I’ll touch on a couple more of those in the next slides. So, next please? So up in Albany, we also have a CERT team, our Computer Emergency Response Team. This team provides incident response and digital forensics to our SLTT members, and even those that aren’t members can use this team that’s -- [report in a?] cyber-event. The forensic analysis helps to identity sources of compromise, the activity of the attacker, the malicious actor, while inside a network, how they got into the network, and to see if there’s any data exfiltrated from the systems or networks and recommend remediation steps. At the end of that analysis, they’ll provide a really detailed forensic analysis report to the members. That information also -- and one of the things that you’ll hear me say over and over again -- we also share that with our federal partners, so it’s not just in this closed stovepipe, where we’re actually sharing the information that we’re seeing, that we’re analyzing, and getting that out to the other intel teams and the cyber teams within DHS and other partners that are there on the floor. We do have the capability to go onsite, but really, we don’t have to do that very often. Most of the time, we’re able to do that remotely and --

from our Albany location. So, it’s a pretty good tool and team for SLTT members to utilize -- and, again, at no cost to them. Usually, we’re at anywhere from 10 to 15 cases per month that were working with our CERT team. Next slide, please? So, the NCCIC liaisons. So, I am one of two NCCIC liaisons for the multi-state ISAC. So the NCCIC, National Cybersecurity and Communications Integration Center, located in Arlington -- I sit there on the floor with all of the different partners that are there. I don’t know if any of you have been there, but it’s a very large operations center. It’s made up of the National Infrastructure Group as well as the U.S. CERT and ICS CERT, Hunt Instant Response Team, the national level. So they have the Einstein sensor system on civilian departments and agencies, which is similar to our Albert system out on the state and local network. So we’re sharing a lot of information at that level, as well. But being there on the floor really does allow us -- we’ve been there for a few years now. I want to say almost five years now, we’ve had the roles there at the NCCIC floor. But it allows us to provide some insight to the leadership there at the NCCIC as to the SLTT cyber-domain. We also partner with all of the different liaisons that are there. So we have Department of Energy liaison that’s on the floor. We have cyber-command, federal law enforcement, intelligence community partners, both DHS as well as other intel community partners that are there. You can see there’s a list of the different LNOs that are -- LNO liaisons that are out there. But on a daily basis, it allows us to really share information based on the different campaigns that are going on, based on the different vulnerabilities that are found, and we’re really sharing that information on a daily basis to ensure that the correct information is getting out to those that need to know that information, and as much of it as possible at the unclassified level. So one of the things over the past couple years that we’ve been able to work on is victim notification based on intelligence community reporting. So the intel community, I would say, over the past few years has gotten really much better at the downgrades [and terror?] lines coming automatically with reporting. So if there are any entities that area SLTT victims based on intelligence community reporting, we work with the Department of Homeland Security and our FBI counterparts to do victim coordination calls so that we’re all on the same page; so that we can look at the different actor sets, the different context that’s in the reports, and then determine who will do victim notification out to the members. So sometimes not a lot of context, but it is timely, and it is relevant, and it’s very important information that we get out there. So it is working, being there at the NCCIC and getting downgraded information out to our members. Now again, that’s very specific, based on the reporting that’s there and victim notification, but that’s something that we’ve definitely come a long way with in being there on the floor. So for creating that broad understanding of the threat landscape, but also just being those relationships and continuing to be there as the face, as the messenger for the state and local, tribal, territorial, and public members that are there. Okay, so next slide, please? So, those are kind of our group areas. We also have a team called Stakeholder and Engagement that does a lot of outreach to our state and local members that’s not on the slides, but I just wanted to mention them. But they are up in Albany, and they do a lot of work, going out and talking to different groups. There is -- different workgroups within our communities as well, working on all the different types of programs that we have. So what I wanted to do now is kind of go into a couple of our top programs and services that we have for our SLTT members, the first of which is the Nationwide Cybersecurity Review. This actually is a DHS program. They handed it over to us a few years ago, and we work in partnership with NASCIO and NACo, the National Association of Counties, in putting out this very simple voluntary self-assessment cyber tool for members. So, it’s a platform where an entity can conduct a self-assessment of their cybersecurity maturity. A couple of years ago, we took the questionnaires and mapped it to the NIST cybersecurity framework. So, all of our questions lend themselves to that and the security controls. So again, it’s -- it really is something that’s fairly simple. All of the states do participate. The past year -- it just did close in the end of December, and the report should be coming out shortly. But what this does is it allows our states, our locals, our different public sectors to kind of rank themselves against each other, without seeing, of course, who’s better than the other -- but seeing not the specific names, but being able to kind of assess your maturity. So, to be able to take that information and use that when talking to your executives and really show them scoring on where we need to move forward, where we need to spend resources, where we’re doing well compared to others in our areas. So it’s a really useful tool that, again, doesn’t take much time. And we have all the states and local jurisdictions. And so, again, this year, we’re opening it up to the public sector so that education entities can rank themselves against other education entities and so forth. We do provide a report to Congress every two years on the scoring of this so that they do have an idea of -- kind of how SLTTs are scoring themselves in cyber-risk. So, this has been a pretty good program in understanding where SLTT members see themselves as far as cybersecurity goes. Okay, the next program is called the Vulnerability Management Program, thank you, VMP. This is a proactive cybersecurity program. A lot of what we do is in reaction to, right, or on the physical side, it's post-boom, where we're reacting to and responding to incidents that have already occurred. What's great about VMP is this is where it's -- in a -- not obtrusive, and us looking at out-of-date software on different domains and IPs that are out there. So we take our database of IP addresses and domains, and I think we're at about 30,000 at this point, and we correlate against known, identified threats and compromises and then provide notifications out based on that information. What we also do, though, is identify vulnerable and out-of-date systems. So, what we do is: if you're an end-user on the internet and you're going to a state domain, we do the same kind of thing. But then we look and analyze that data that comes back to see if there are any open vulnerabilities. So, it's been a very successful program. We’ve had it running for about two years now. So, we can identify web servers not running the most current version of the software. So what it allows us to do, also, is see the time from when a vulnerability is first made known to how long it takes our members to patch. So in the very beginning, there was a longer time to patch, but now with our notices, we’re seeing an uptick in or an increase in patching quicker when it comes to these notifications. So for example, just in November alone, we had -- I think we sent over 1,000 notifications -- being sent out on vulnerable websites, right? And this is one of the easiest attack vectors for these actors to get into. So this has been pretty successful, as well. And not a lot of work on the forefront for the state and local member. It is once we send them the notices that they are vulnerable, but that is -- then we can provide them with assistance in patching or fixing that hole. One of the newer things that we’ve implemented, also -- just I think, in January -- is we started port scanning of the SLTT internet connections. So we identify, we verify that there are open ports that shouldn’t be open on the internet, and we verify that they -- those vulnerabilities are actually vulnerable, and then we go out and tell the -- and notify the members if they have ports that are open that shouldn’t be open. So I want to say the first time that we tested it, we had ICS systems 12 or 13, I believe, that came back as having open ports there. So, we were able to notify and then they were able to close those pretty easily. Okay. Next slide, please? Okay, MCAP is the Malicious Code Analysis Platform. This allows members, or even those that are non-members, but are -- they have to be SLTT-related -- to submit suspicious files for analysis. So these are all the different things that they can submit, and they can analyze domains, IP addresses, URLs, and this is all in a non-public kind of fashion. So they’re sharing all this information, they -- it allows the user to kind of identify behavioral characteristics of the malicious activity that they’re seeing, or the different malware that they might have. Through the platform, you’re able to obtain analysis results -- again, behavioral characteristics and additional information that will help explain the nature of the infection and guide incident response and remediation. At that point, if you still need additional help, of course our CERT team and our SOC can help a member as well, if they need additional support. What we’ll also do with that type of information is we keep an eye on what’s being submitted. It allows us to enhance our trending information of the attack vectors, of different malicious files that are being executed on in the -- in our state and local domains. But also, as an example, we had a phishing email that was submitted, and it as definitely -- the title of that phishing email was definitely APT, or Advanced Persistent Threat, actor type of phishing email. So we were able to go back to that entity, provide them with some downgraded information based on that APT activity, provide them with some indicators, and also get information back from them on how successful the phishing campaign was in their network, and then provide that back through various means to our federal partners, to the IC, in different reporting platforms. So that's another free platform that's available for all the different members to use in a non-public fashion. Next, please? So, automated indicator sharing. I know that that's been a big thing in the cybersecurity realm for the past couple of years. DHS has its automated indicator sharing. We used to use Soltra Edge for our STIX and TAXII automated indicator sharing. Last year we moved over to Anomali. We looked at a lot of different vendors, and this -- Anomali was the best one that we found to partner with our members. So this is a platform where our members can tie in and get automated indicator sharing. So all the different malicious IPs and domains that we have, all of the different indicators that are coming from the Department of Homeland Security or private sector sharing platforms that are automatically ingested can be shared with our members, as well. With Anomali, they also did provide free threat stream accounts. So, it’s additional threat informa-- cyber-threat information that the analysts -- cyber-analysts at the fusion centers or any of the different members can use, and also try and analyze different malicious activity that they’re seeing across their networks or in their state and localities. So again, this is no cost to our members. The Anomali feeds or the other STIX and TAXII things that we tie to are from all the different sector partners, as well. So we have FS-ISAC information coming in, we have VDHS intel community reporting that’s coming down and being fed into that, as well as other private sector partner feeds that are out there and other open source types of indicator sharing that is tied to that platform. Okay. Next, please? So really, to kind of tie it all together, there are a lot of different benefits to being an MS-ISAC member. Again, it’s all voluntary -- right -- to be a member. And there’s no mandated information sharing, although it’s very helpful if information is shared back up to us so that we can better assist other state and local members, as well as provide that information back to the sources of information, right? So, within the intel -- I’ll go back a little bit -- but within -- in our intel team, we’re writing IIRs based on some of the activity that we’re seeing so that we can provide that back to the intel community, or responding to intel community requirements, providing the different EEIs, essential elements of information or priority intelligence requirements and needs up to our intel community partners. But it allow-- the benefits -- really is -- a lot of access to information. We know that there’s not always a lot of resources that are out there for our state and local members. So we are kind of that force multiplier, if you will, for our SLTT members. But we’re also sharing all of the federal information. So when NCCIC puts out products, we’re sharing that type of information out as well. The -- one of the recent examples was FBI and DHS released a joint analysis report several months ago on APT actors targeting the energy sector and other sectors. And so, being a part of the MS-ISAC, we were able to take a look at all the indicators prior to being released out to the public, and we were able to run those on our sensors to identify any victims, and we did have several victims. So we worked with them, provided them with some intelligence information. We provided them with assistance, and we were able to get feedback from them on what they were seeing in their networks -- in their compromised networks -- and then help them with remediating those issues. So, we have CIS secure suite. That is some of the CIS programs that are now available to all of our members at no cost. We have HSIN community of interest. We participate in a lot of cybersecurity exercises, whether it’s cybersecurity exercises at the local level or the larger Cyber Guard and Cyber Storm exercises that we participate in at a national level. We also have several working groups, and one of our working groups works on education training exercises. And so, every month, we have an MS-ISAC monthly call with our members. There’s usually four -- three to four hundred-plus members that are on the call, so I think that’s a pretty good turnout for a monthly call. But they get on the call, and one of the things that we do is we provide them with a tabletop exercise, a really simple tabletop exercise that the -- they can go back and use within their own organizations to share. So, those are the small benefits of working with the MS-ISAC. Again, I said we have different working groups on education and training. One of the training resources that we were able to work with DHS -- is on the FedVTE, [at a?] federal virtual training environment. So that was free to all of the different federal employees and military members, but we worked closely with DHS to enable that to be opened up to SLTT members. So SLTT members can now access FedVTE at no cost, and there is really some great training out there on the cybersecurity side, which is free to the members now. So, those are the different types of benefit that we have that I just wanted to highlight for you. And so now, I would be happy to open it up to any questions. (overlapping dialogue; inaudible) (laughter) Three, okay.

BRADLEY: Yeah, this is Mark Bradley, the chair. How does one join?

SUVER: It’s very easy. You can go to the website and click register.

BRADLEY: Right, so that’s --

SUVER: Just have to be state and local --

BRADLEY: Okay.

SUVER: -- SLTT-related.

BRADLEY: And your funding, where does it come from?

SUVER: DHS.

BRADLEY: DHS, and com--

SUVER: Yes, sir.

BRADLEY: Completely?

SUVER: Completely.

BRADLEY: And lastly, what challenges do you face? And by that, I mean are you getting information downgraded quickly enough to be able to use it? Is there anything we here can do for you?

SUVER: So, I would say that there -- like I said earlier, they -- the intel community has come a long way. When I worked with INA several years ago, it was hard. It was also providing some awareness as to what the SLTT needs were, right? I don’t know that that was fully understood many years ago throughout the intel community. But I think we’ve come a long way in getting more of that information downgraded, getting it out to the different fusion centers, getting it out to the different members. I think there’s all -- there’s several challenges. They -- each state is different; each fusion center is different. Each cybersecurity center is different. I was at an exer-- or I was at a meeting yesterday where we were talking about an exercise, and we were talking about lessons learned. And really, it comes to information sharing and communications -- were the two big issues that continue to be problematic. And I think it’s just that there are so many different avenues where information can be shared. So, what we’re trying to do is really reach out to as many as possible in getting that information pushed out. So, I think one -- we met with ODNI several months back -- in talking about SLTT information needs and information, getting out to our members, and beyond our members. And when I say that, I mean the entire community. And they -- it was great that we’re sitting there and meeting with them, but I think there’s still a lot of work that can be done in getting more unclassified products out. So, I think that’s one thing that we’re working with our INA partners on -- we’re working with our intel community partner on -- is getting more of the unclassified strategic analysis -- and even on cyber-threat actors and TTPs.

BRADLEY: Thank you.

PANNONI: So, I have a question.

SUVER: Yes?

PANNONI: This is Greg Pannoni. Mark mentioned -- the chair mentioned the reg-- you mentioned how to register for the members, and during your presentation, you mentioned -- there was a reference to NIST standards. So, the question has to do with who -- is there any vetting of the members before they actually are accepted to make sure their own systems meet a certain, you know, moderate level of confidentiality or whatever other --

SUVER: Right.

PANNONI: -- controls (inaudible)?

SUVER: So, all of our members -- we go back to what -- the way that we work is we have state primary members, which is usually the [FSO?] -- whenever we have members that are joining from other -- from different local or county level, we will go back to that state primary and just say to them -- it’s kind of just a one-off check to make sure that they are who they are and where they’re located so that we can check those domains. We’re also going to run their domains and make sure that there’s no vulnerable holes there, and -- so those types of activities that we’re looking at before we just sign off on membership.

PANNONI: Okay, thank you.

SUVER: If that helps.

PANNONI: Yeah.

SUVER: You’re welcome.

MASCIANA: I have a question (overlapping dialogue; inaudible)

SCHOUTEN: -- from Iowa with a comment. I was a member -- we have a number of our counties and cities and school boards -- and we think the MS-ISAC is a great -- it is different than many other information-sharing centers or entities that maybe share from the ground up. This situation is different. It’s more of a centralized national system that provides local services. In that sense, it really is different, but the services they give are so scalable, there are such economies of scale that the MS-ISAC can do these things, distribute them so easily at the speed of light and provide these types of vulnerability management systems it really is a neat model, and our OCIO duplicates or actually hands off some of the MS-ISAC services to our locals. It is a really good example of how the federal government has stepped in and -- or MS-ISAC as a -- entity funded by the federal government is doing some really good things.

BRADLEY: Thank you, Leo, you --

SUVER: Thank you.

BRADLEY: -- [were saying?]?

MASCIANA: Yeah, yes, this is Leo [again?] --

M: (inaudible) [who was?] speaking on the phone?

BRADLEY: Yeah, who was speaking on the telephone just now, so we can get our transcript straight?

SCHOUTEN: That was Mark Schouten, I'm sorry.

BRADLEY: That's all right, Mark. No, no --

SUVER: Thanks, Mark.

BRADLEY: Right. Right, Leo.

SUVER: Sorry.

MASCIANA: Okay, I'm interested in your partnership with the U.S. CERT, the extent to which their incident reporting feeds into what you do, and also whether you provide essentially a greater access to U.S. CERT for your members and what you can tell us about that?

SUVER: Sure. So yes, we sit -- we work very closely with U.S. CERT, ICS CERT, and all the entities that are made up there in the NCCIC. I do believe that the naming -- the U.S. CERT name is actually going away. So that will be changing soon, just as a heads-up. But we work very closely with them. So, we are -- I actually sit in with meetings with them, almost on a daily basis. So we’re looking at the different incidents that they’re working on, that we’re working on, tying any incidents together if we can, campaign tracking kind of activity. So like I mentioned, that joint analysis report, we were able to work with them with providing our feedback so that, in their updates to that [JAR?], that was based on some of the feedback that we got from the states. So there’s that type of coordination effort that’s going on there, as well. As far as U.S. CERT product, they put out a lot of different indicator bulletins. We have within that HSIN portal, that MS-ISAC community, all of the U.S. CERT products are pushed to that portal so that all of our members have access to that.

MASCIANA: Now does that include specific (inaudible) use, like, IP attack signatures?

SUVER: Abs-- well, not signatures, so much, but it does have IP -- we put out the -- based on our Albert sensors, our weekly malicious IPs and domains. That gets shared with U.S. CERT. The -- I also should have mentioned the MCAP, all the stuff that's provided into that, and it's thousands and thousands per month, right, different executables that are put in that system. They're shared with DHS, [non?]-attribution back to the state or local entity, but that information is shared. So there's that type of technical sharing, as well, between U.S. CERT and the MS-ISAC. I don't know if that answers your question or not.

MASCIANA: Yes, it does.

SUVER: Great.

MASCIANA: Last question: do you see on the horizon a need for an international, global reporting?

SUVER: So there is, within U.S. CERT, name to be -- TBD, they have an international team that works with the different international CERTs that are out there. We have different working groups, the TLP, Traffic Light Protocol Working Group, which is through the first group, which is international CERTs coming together. So, there is that type of information sharing. There's the [FIBI?] information sharing. We just recently, actually, started sharing through that team to our FIBI partners our malicious IPs and domains. One of the other things that we’re doing -- so yes, but it is happening right now without that international type of center is what I would say to that.

MASCIANI: So, are you actually receiving --

SUVER: Yes.

MASCIANI: -- input from them?

SUVER: Absolutely. So, that team receives -- and then we get that in a weekly basis. It’s our international weekly report that we get via that team, and it’s a bunch of different countries that are reporting significant activity and cyber-threat activity and vulnerabilities that they’re seeing. So, that information’s being shared.

MASCIANI: And these details are available to your members, or --

SUVER: So, we will -- I wouldn’t send those reports out to our members, but we do take that type of information and pull that into our analysis, as well as any information that’s gleaned from that that we haven’t -- that we don’t already know will get pushed out to the members.

MASCIANI: [That’s all, thank you?].

SUVER: Any other questions?

M: (inaudible)

SUVER: Okay, great. Thank you very much again for having me. I appreciate your time, thanks. Thank you.

M: (inaudible)

BRADLEY: No, it’s the opposite. We thank you. That was very good, very comprehensive, and very well done.

SUVER: Thank you.

BRADLEY: Leading into that, you know, last year we had one of these -- similar on fusion centers that I thought was very useful. Today, we had this. Those around the table and on the phone, can you think of anything -- any other speakers or any other aspects like this that we can brief or talk about and then showcase what’s going on? I mean, I think it would be beneficial to us and to you all to hear what’s going on out there. This was a revelation to me, so I mean --

STEINMETZ: Yeah, it’s Mike Steinmetz from Rhode Island.

BRADLEY: Yeah, Mike.

STEINMETZ: Can you hear me okay?

BRADLEY: Yeah.

STEINMETZ: Yeah, I think one of the organizations that you probably should hear from is the group that’s loosely tied to the financial system. I -- yeah, financial system ISAC. And it’s called the FSARC. They are doing some very interesting things with regard to real-time analysis between some of the largest banks in the U.S. and departments and agencies within the U.S. Government that supply really sensitive information. So, they're doing some real-time analytics to take very -- I would say extraordinary measures to keep the financial sector completely abreast of the latest threats. And the president of that group is a gent by the name of Scott DePasquale. And he could be a possible future speaker to the group, talking about public/private sector information sharing and how that near real time is making it -- and secure -- helping to secure the global financial system.

BRADLEY: Good, and I think that sounds like an excellent idea.

STEINMETZ: [Yeah?].

BRADLEY: Anyone else? I mean, this is a broad field, so we should be able to, I think, attract speakers to come in -- or even on the phone.

SUVER: This is Roisin with MS-ISAC.

BRADLEY: Yeah.

SUVER: So I don't know what has been discussed before, but I know that the National Guard piece is -- has -- comes up quite a bit when it comes to cybersecurity, cyber-defense, their missions, and what their capabilities are within the state and local environment. One of the things we do is we -- National Guard entities come through the NCCIC once every month for training -- or, I'm sorry, once every two months now for training, and we'll sit down with them and provide an overview similar to what we did today, but more specific to the states that they work with, make sure that we’re kind of connecting them to the players within their state if they’re not already connected. But the National Guard is definitely becoming a mover and a shaker in cybersecurity, at least, in the state and local environment.

BRADLEY: Interesting, yeah.

SUVER: So the Guard, you know, could potentially be a --

BRADLEY: Yeah.

STEINMETZ: Yeah, and this is Mike Steinmetz again. If I could second that, we -- and I know, Roisin, you’re probably aware, we’ve got the 102nd Network Warfare Squadron here in Rhode Island, serving the United States Air Force, and we have a very unique relationship with them, public/private, and I believe the adjutant general would be delighted to have an invitation to speak about those capabilities.

BRADLEY: All right, we’ll give him one. (laughter) Yeah, good. Excellent idea. Anyone else? No?

MASCIANA: Leo.

BRADLEY: Leo? Yeah.

MASCIANA: [UFCY?] program has partnered with NIST -- I think recently, since last summer, published a guideline for private sector to follow for controlled unclassified information --

BRADLEY: Right, yep.

MASCIANA: -- system compliance, and --

BRADLEY: Right.

MASCIANA: -- and so [Dr. Monross?] might be able to provide some good background --

BRADLEY: Okay.

MASCIANA: -- on that.

BRADLEY: No, it’s a very good idea. Excellent, okay. You know, another thing we’d like to do, too, is I’d like to have -- how we’re going to do this, but throw it out -- agency updates on your own programs with this -- in this. I’d like to have more of a drill-down. So perhaps next time around, we can have something scheduled for -- one or two of you all to give a -- just a presentation on where you are. And I’m particularly interested in any type of challenges that you’re running into, anything that we can perhaps help you with.

SCHOUTEN: Mark, this is Mark Schouten. I think your point’s a good one from the state and local tribal perspective to understand the interplay among the federal agencies, which sometimes, to us, is rather confusing, but I’m sure makes sense to all of you. From our perspective, that sort of an outline or discussion, I think, would be helpful.

BRADLEY: Okay, good, good. Yes, ma’am?

KERBIN: [Maybe one?] (inaudible)

BRADLEY: Valerie?

KERBIN: (inaudible) Valerie -- (laughter) from the National Background Investigations Bureau. You know, they stood up the Law Enforcement Liaison Office and how they’re working with the FBI and local jurisdictions --

BRADLEY: (inaudible)

KERBIN: -- to ensure --

BRADLEY: -- excellent, that’s excellent, excellent, yeah.

KERBIN: -- that --

BRADLEY: Good.

KERBIN: -- you know, everybody’s feeding into the national databases, so we could get that criminal information for the background investigations.

BRADLEY: Excellent, no --

KERBIN: So, you might want --

BRADLEY: Okay.

KERBIN: -- a briefing from them.

BRADLEY: Yeah, we can do that. Yeah, no, that’s good. Anyone else? Lastly, can we think of anybody who we’re leaving out? By that I mean, you know agencies that deal with state and local, but who aren’t members of our group here? I mean, are we excluding anybody, or is anybody -- I don’t want to use the discrimination, but are we forgetting somebody or overlooking somebody?

KERBIN: This is Valerie again. Are you including the medical sector, like HHS?

BRADLEY: Good question, [are we?]?

M: Yeah.

BRADLEY: No, well, [there’s?] (inaudible) that’s a --

M: (inaudible) [good one?].

BRADLEY: -- probably a good one, yeah, I mean (overlapping dialogue; inaudible) an excellent idea. I mean, anybody else that we’re -- yeah? Anyway, give that some thought, because it’s a serious question. And I mean, we’re only as good as the members sitting around the table and out on the phone, so -- beyond that. Okay, yes, anything else on that? If not, we’re going to --

MASCIANA: I would like to --

BRADLEY: Okay, Leo, go ahead.

MASCIANA: Leo -- nominate the FBI?

BRADLEY: Well -- (laughter)

MASCIANA: As I heard, you mentioned that you assist victims with malicious code attacks and whatnot. It occurred to me, what is then done to bring them law enforcement assistance, depending on the severity or the degree of criminal damage that’s being done to their networks? I think the FBI does have programs that that might -- elaborate on that.

BRADLEY: Good, good. Good, we’ll be ecumenical and, you know, the more the better. All right, with that, let’s go to my favorite part of this, which is the open mike session. Anybody have anything they want to discuss? And again, don’t be shy, or -- I mean -- Nancy, I know -- (laughs) no?

MORGAN: [Not our usual?] (inaudible)

BRADLEY: No? No?

MORGAN: (inaudible)

BRADLEY: No? Anybody on the phone? Can you think of anything?

M: I think -- no, I think --

BRADLEY: No?

M: -- you’ve covered it.

BRADLEY: Okay, all right. Well --

M: [Let me think?] --

BRADLEY: -- okay, with that, let’s move towards adjournment. The next SLTPS-PAC meeting will be held on Wednesday, July 25th, 2018, from 10:00 A.M. to 12 noon here at the National Archives, so please mark your calendars. And again, we’ll try to digest some of the suggestions that we’ve heard today and see whether we could come up with an agenda that will have some of that on it. So, [if I don’t hear?]

anything else, then I’m going to adjourn, okay? Okay, thank you all for coming. (tone) (overlapping dialogue; inaudible)

M: Thank you! (tone)

(pause)

END OF AUDIO FILE