Critical Elements of a Suspicious Contact Report Webinar Transcript

Cover Slide

My name is Peter DeCesare and I am the curriculum manager here at CDSE, and your host for today's webinar. With me today I have Rachel Mongeau, an instructional designer here at CDSE who is our producer, and she will be working behind the scenes to keep us on track and on time. We also have Dominique Bishop, an intern with CDSE assisting today. Before we get started, Rachel is going to provide you our webinar ground rules for today and some instructions on how to use the tools you will need to participate. Rachel.

Navigation Slide

Ok, thank you Pete. If you have a look around your screen, you will see at the top there is a small button with four arrows. If you select this, it will allow you to have a larger view of the screen. Be sure to select it again to return to normal view and respond to any of our poll questions or chat questions, or to enter a question in the Q&A box. To have a normal view, you just select the button as I said; you'll also see there is a question and answer box on the right hand side of your screen. At any time you can enter a question into this box for our presenter; if we can't get to the question today, we will enter a response in our webinar archive online. You will also see a chat box that will move over top of that question and answer box periodically when we would like your input on a question from the presenter; simply enter your response there. We will also have poll questions; these are multiple choice questions, you simply select your response and we'll provide feedback. Additionally, at the bottom of your screen you will find a notes box. This will give you the call in number and any other announcements as necessary. We also have a file share box and there are several brochures in the file share box today along with the slides for today's presentation. Feel free to download those onto your desktop for future reference. Okay, that concludes our tour; I'm going to send it back over to Pete.

Thank you Rachel.

Over the past couple of years we've developed a couple of different training products and hosted a few webinars that discuss the importance of reporting suspicious activities to the DSS CI Directorate. When reading the NISPOM 102B, one might argue that the language is a bit vague. Today, we have one of our DSS counterintelligence special agents to discuss what information should be included when reporting suspicious activity to DSS. We had some questions sent in advanced, and Mike will try to answer them during his presentation. However, if we run out of time and don't have to time to include questions at the end of this brief, we will answer those and place those in our archives. So without further **ado**, Mr. Mike B. from Massachusetts.

Hey Pete, thanks very much. Good afternoon everyone, or good morning depending on where you're calling in from. First and foremost thank you everyone for taking the time out of your

busy day to take part in this training, its most appreciated. Time restrictions are extremely tight, that said there is no possible way we can cover everything with identifying all the elements of an SCR but we will do our best to give you some tools to take home to your facility and implement. Alright, so we'll jump right into it.

Agenda Slide

So here's a brief agenda; you'll see throughout the presentation I won't read line by line so everyone, I encourage you to digest the slide as they are presented. I will point out in this one specifically that we're going to be talking about how to identify critical elements of an SCR within multiple categories. A lot of facilities I deal with up here in Boston, especially newer ones to the program, they associate an SCR with an email – suspicious emails that come in, which is correct. But we're going to talk about multiple different categories things like foreign travel, foreign visitors, etc.

<next slide>

Alright, so what exactly is counterintelligence? I know everybody on the line here today probably has their own definition and (unfortunately you may think) so does the vast majority of federal agencies out here, military departments and what have you. Everybody puts their own spin on it, what is the same with all of them is CI is really info gathering or activities conducted to identify, deceive, destroy, or disrupt or in some cases to protect against espionage, Intel activities, sabotage, or assassinations. Now that's pretty broad, we're out there to detect bad guys stealing our technology and put a stop to it. The other very important take away from this is that when we're talking about counter intelligence there is always a foreign nexus. Things that happen here in the U.S., there is federal agencies, partner agencies that deal with that but it doesn't really fall into the realm of CI; we're talking specifically about foreign nexus.

<next slide>

Alright guys, this really isn't a punch line anymore; you really are the front line especially (I can't stress enough) when we're talking DSS CI and our partnership with you folks in industry. We can't do our job plain and simple without your assistance in providing these reports for us to look at and conduct analysis on and categorize, and I'll talk about that in a moment. We really can't; so everything you do for us in reporting these suspicious contacts is crucial and most appreciated.

<next slide>

Alright I'll give everyone a moment to digest this slide; this is just the text from NISPOM for requirements for reporting suspicious contacts. Assume everyone probably knows that inside and out, which brings us to our first poll question. I'll turn it over to Rachel for this.

Poll Question #1

Ok, thank you. We'd like to test your knowledge here: should contact reports be sent to the FBI? Would you say Yes, No, or it depends?

Well that's kind of a trick question isn't it?

Sure is.

Looks like we got a majority who feel that it depends.

Yep, it does look like the majority and for those that selected it depends, are spot on. It actually is that it depends; not all SCRs have to be reported to the FBI. That being said, if you do report them to the FBI that's perfectly fine as long as that DSS CI is receiving those as cleared industry that you definitely are reporting those to DSS CI. When we're talking specific reports that to be required for the FBI, that comes out of NISPOM 1.301. And it talks about actual, probable, possible, espionage, sabotage, terrorism, or subversive activities must be reported to the FBI with the special caveat that you must cc the cognizant security authority, which in the class of cleared industry is DSS. So thanks for answering that poll.

<next slide>

Alright in the next slide we're going to talk about some definitions here and I get a lot of interest in this because the facilities that I deal with they're not familiar with this. So hopefully this comes as welcomed information for you guys on the line. Every single report, every one of them that you submit to DSS CI, is categorize into three specific categories. We have a suspicious contact report, an unsubstantiated contact report (a UCR), or an ANV (that's an assessed no value). I'll stress that we're not saying that it doesn't have value that you're sending it to us; we're saying that there was no counter intelligence nexus that we could find. In most cases it was a plain ole spam email, so no CI value reserved in our databases. The top two, SCR and UCR, are things that we contain in our databases we hold onto them and of course we do so under applicable U.S. Intel oversight regulations. An SCR is a report that we determine has a significant CI concern of some level.

These are things like we know it's a foreign entity targeting our facility for one of your sensitive products or elicit procurement; that's just one example of many. Now and unsubstantiated contact report this is another thing we retain under Intel oversight, and I want to explain this. This is a request that comes in that we really can't point our finger on and say yes we know that person to be a foreign entity who is targeting your technology for the sole purpose to benefit that home country, as an example. That being said, perhaps you receive your request and your business development folks kicked it back and said hey we're not interested or what have you, maybe they had an embargo against the country perhaps. Now keeping that UCR in our database, if you said no to that requestor and then we see and we try to connect the dots that three or four other cleared contractors throughout the country received the same or very similar request; we connect those dots and chances are it's coming from the same requestor. Not every case is going to pan out that way, but a majority does. In those cases, we can upgrade that UCR to and SCR and therefor benefit the intelligence community as a whole.

<next slide>

Alright, next thing I want to talk about is the categories that we're going to discuss on identifying those critical elements of an SCR. As you see they're multiple categories here and we're not just discussing emails.

We'll give everyone just a brief moment, okay.

<next slide>

Alright, this slide here is an actual Attempted Acquisition of Technology (or AAT) what we commonly refer to it here at the DSS CI. You see the chat box just appeared? I want to give everybody just a few seconds to take a look at this. This was an actual request that I cleaned up to protect the actual company that was being targeted. Take a look at it and go ahead and chime in on what you think is a suspicious element of this request.

Okay a couple more seconds.

The folks that are responding here absolutely spot on; I see multiple suspicious critical elements that I'm going to circle here in just a moment. First and foremost let's start with the address; don't just focus on the name. So we see the domain and in this case we see it's a publically available domain, this is a yahoo.com and there are many out there right Gmail, Hotmail. And then various foreign countries have their own available domains as well; a simple google search can showcase all of those.

So we have what appears to be under the guise of a legitimate business request, so in this case Sally is giving her company name, phone number; she's not hiding that fact. So it looks to be legitimate at first glance. So why wouldn't Sally send this from her businesses domain? You have to ask yourself that question, we understand that not all across the board are going to have their own domain but the majority do. And again a simple google search; do that due diligence see maybe they have their own domain and it's easily you can find that on google. We have seen the majority of actually suspicious context that we can tie back to elicit procurement for example comes from a publicly available domain. Next two are the time and I circled dearest friend they go hand and hand. You're not always going to know that it's a foreign inquiry they're not going to spell it out like they did in this example.

Many will not it will just say Sally in the signature block, so you have to do a little homework try to tied it back to a foreign nexus. And you're going to do that by the time as some folks pointed out grammar, and the time here its 3:23 a.m. not normal business operating hours here in the U.S. It likely points to operating hours overseas, again not always but the vast majority of cases will. Then go to grammar, dearest friend, my dearest, esteem professor, look for grammar mistakes throughout the email; you're looking for syntax, sentence structure, spelling errors that were very common, anything like that more than likely will point to a foreign nexus. Alright, I have the SCS 3500 which actually doesn't exist I just threw it in there to protect that company. But this is a sensitive just replace it with your company sensitive whatever it be attar control, classified part it's a defense application. So we know this to be a foreign inquiry and they're look specifically for one of your sensitive products, big red flag. Especially if there is a defense embargo or a competing embargo on that company doing that request. And here we go with the next two and I'm going to circle them both they're trying to put you at ease; hey don't worry about it everything's all set here, export license has been done its all approved go ahead and ship that our here's the money.

They have unlimited resources by the way and they will do this on a regular basis; they'll send that money, they'll wire it to wherever you want it just to get that product as soon as possible. And then again putting you at ease, we're not going to use this for military defense in most cases we see that they say it's for educational purposes as an example as primaries we do see. And finally the vast majority, I can't put a number on it but it's very high, there's always a sense of

urgency, you'll see things like ASAP, right away, customer is very demanding look for those telltale signs.

<next slide>

Alright, brings us to our second Poll Question #2 and I'm going to turn it back to Dominique for this.

Okay, we would like to know how soon must a suspicious contact report be sent?

Immediately, within 24 hours, within 48 hours, or during vulnerability security assessment?

So, the polls are coming in and it looks like majority of people are saying immediately, well it's a tie.

Yea, kind of going back and forth. Well for all the people who selected immediately I'm with you and for my own selfish reasons I wish I could say immediately, but unfortunately I cannot do that. The answer is there is no specific time requirement, and I say that with the caveat that as soon as you get an SCR, if you get a report that you determine to be suspicious, the faster that DSS CI has that in our hands to do an analysis and see that a potential threat exist, the better chances are to pass that to an operational agency one of our federal partners that can take actions against that requestor to mitigate that potential threat. So as soon as possible is all we can ask for.

<next slide>

Alright foreign travel: I'm assuming that the vast majority of the folks on the line have individuals, or yourself, within your facility that go on foreign travel either for business or pleasure. With that, traveling abroad to specific of course that we won't discuss in this forum, the risk is greatly increased for those cleared individuals especially who are traveling abroad. Some things that we ask is that you pick up the phone or email your CI special agent (my equivalents throughout the country). Let them know what country that employees going to and allow us to come out and do a pre-brief and a debrief with that individual of course with you right by our side.

You may already have a policy at your facility that has these pre and post foreign travel briefings and if you do that's super we couldn't ask for much more. We can also come out and assist you in developing the correct questions that we're looking for. We don't want an employee to come back and pencil whip a yes or no question; so it's always beneficial to do a one on one interview with that employee, to kind of explain those threats. Look for any of the techniques that are listed here that may have been used. If you see any of these techniques in any of your debriefings this constitute a reportable event that you want to submit to DSS CI as and SCR. You noticed we uploaded a bunch of our CI trifolds the one that kind of goes hand and hand with this of course foreign travel. We encourage you to download it to give you some more helpful information.

<next slide>

Alright I'm going to throw a poll up here real quick. Out of all the facilities out there, how many have hosted, and you can say yes or no, have hosted a foreign visitor could be one could be a delegation of ten?

Alright, pretty good mix; I see some familiar names here so hello for those of you that recognize my Boston accent. Pretty good mix a lot of yes, a lot of no, and we see that we're seeing more and more of that in fact there are thousands literally of foreign delegation visits to cleared defense contractors that occur throughout a given year, thousands of them. Look at these collection techniques that we have listed here; there's a lot that you can do to mitigate the threat here.

First and foremost, we ask that you, as the FSO your facility, give DSS CI at least a weeks' notice if it's a day so be it whatever advanced notice that we can get the better and let us know who is coming to your facility. The more information we have the better so we can do our analysis and classified database searches to see if that individual has any nefarious affiliations, if you will. If there are, we're going to come out to your facility give you a high level briefing, let you know what that is, we'll never tell you not to do the visit; that's not in our charter we can't do that, but we will give you the tools to mitigate that threat. If that's calling off the visit then so be it. You should also go around maybe do a tour a dry run of where you're going to bring this individual, ensure it's nothing that's sensitive out there on the floor. We do have a trifold uploaded for this topic as well preparing for a foreign visitor that will give you some very helpful information.

<next slide>

In conferences, conventions, and trade shows I would say that this goes hand and hand with foreign travel, but it's not just foreign CCTs. We're talking domestic as well and in some cases even more so especially the big ones down in the DC area; so you folks who to AUSA, AUVSI big conferences like this. This is a fantastic opportunity for you as a company to get your product out there, in the public, so that you can eventually get sales out of it. We completely understand that; however, just always keep in mind that as good as an opportunity this is for you as a company, it's just as good if not better an opportunity for a foreign intel officer to go out there, walk the floor, and collect as much information as possible on your company, your products. Some of the folks that are presenting for your company they may be targeting them for future exploitation down the road.

Never bring out an actually product like a small electronic as we do know some have been stolen from these conferences and trade shows, actual pretty sensitive products. So always bring a mockup that has no sensitive parts whatsoever. DSS CI we can do specific CCT briefings for you to let you know, high level classified briefings on what the threats we know of can be at some of these bigger conferences. We can give you names of actually individuals you need to be weary of.

We do have a trifold, a CCT trifold, that is upload I encourage everyone here to take a look at that. Some things, I won't read line by line but just try to get business cards wherever you pick up or your employee picks up on something that they found suspicious. Look for photography, some aggressive that's going to be in your face, some will be done in a very shuttle almost covert manner as well. Every employee should be sensitized to that and look for it and pay attention to that and take mental notes of who that individual was; the better description we have, the better chance we have to identify them.

<next slide>

Alright now that brings us to Poll #3, and I'll turn it back over to Dominique.

Okay we would like to know do you have a social network account such as LinkedIn, Facebook, or Google Plus?

And, majority say yes.

Ah, still watching this one unfold, this is pretty interesting. I would have thought much more said yes but it is at 75% at the moment, so that's pretty high. I would've figured it been a little higher; I'm sure the DSS folks on this call all have these accounts. CDSE themselves has social accounts as most of you likely know. What I'm getting at is it's a different age everybody has these social media accounts, including a huge number of your cleared employees out there in cleared industry.

<next slide>

What we're asking is that you sensitize your employees before they post matters about their security clearance, for instance or that they work for a sensitive program. Because believe me if you do a search yourself today go on LinkedIn or Facebook and type in the search parameters you will be surprised: hi I'm a TS SCI cleared engineer working on project X. What they don't realize of course and maybe they're doing it for networking or to get a future job but foreign Intel officers you better believe are looking at this on a daily basis around the clock to identify future targets for exploitation.

We ask that you report as an SCR, when we're talking critical elements with social media, if it's unsolicited, it's foreign especially from a foreign government military or intel representative, or if it's some kind of message associated with the friend request or LinkedIn request that raises their internal red flags or alarm. For instance, hey we're really interested in your company this product especially, let's call it the joint strike rider as an example. This is something that would be hugely beneficial for DSS CI to know.

<next slide>

And our fourth and final poll question #4 at this time, Dominique take it away.

Should you report strange emails if the request is asking for unclassified information? The results are coming in and it looks like majority are saying yes.

Yea, about 2/3 are saying yes. This is a tricky one, the actually answer is it depends. Unsolicited request for information, even for unclassified commercial products, you want to report that to us as an SCR if you are the employee that receive to feel uncomfortable with stating that information. Another consideration, if you don't know who the requestor if they're asking about sensitive, proprietary, ITAR, or classified products then that would be of course reported as an SCR.

<next slide>

Alright, so finally we just talked very briefly I told you time I would be short about some of the categories and how to identify what constitutes SCR in each of those categories. Now what do you report with that SCR? Well if it's an email we don't just ask that you just send us the email, although if that's all you can do then it's still very much appreciated. But in addition, tell us what you, as the FSO, that you thought the contact was suspicious. A lot have been in this field for many years we value your opinion greatly and some of the details that you give us in those SCR's are going to help us categorize that report into and SCR/UCR or ANV category. If it's

directed at a specific individual, let us know who that individual was, just a line or two we're not looking for a full bio on why you thought they might be a target. Because potentially that's what they are, so we want to know that so we can brief that employee. Perhaps they're an expert engineer in optics as an example.

<next slide>

Additionally, if you can provide the header and I know there's a lot of curiosity with this one but the meta data in the header is things like the originating IP, server names, hot points that were used to get to your location. This is critical for us; every email service has a different means to acquire that header, so we ask that you contact your IT security manager to assist you with getting that info. And any other details whatsoever that you feel are relevant.

<next slide>

With non-email contacts just give us the five Ws: tell us what exactly happened, who that individual was break it down a description, look for tattoos, any distinguishing characteristics of that individual. Because when we plug a name in our database (and you can call your CI special agent that's assigned to you and kind of ask them to come in and look at our database). The name commonalty concerns with foreign names especially, there could be hundreds of the same name, so little bit of information we have is very critical.

<next slide>

Additionally, I had mentioned this a moment or two ago, if you get a business card that is fantastic it's going to give us a lot of information that we otherwise wouldn't have had. And for social media, ask the employee that receives that request that we determine to be suspicious from those categories I gave you to take a screen shot, this is the best way we find to do this, take a screen shot of that request that has a photo of the individual, it has their affiliation, schools that they went to. This is going to be very helpful to us in identifying that individual.

<next slide>

Alright, you are really the first, last, and only in many, many cases, (the vast majority or almost all) for us to get this information to do analysis to take action to mitigate the threat. Every single report that you guys are submitting to us is extremely helpful. If we categorize to an ANV it doesn't mean it's not helpful, it lets us know that a foreign entity is still requesting your product, every one of them counts.

<next slide>

And my final thought on this presentation and this is personal for me because I get this all the time and understand it. Our duty is to give you feedback on every SCR on every report we get. It's simply not possible in all cases, I just want to put that out there, I'm not trying to make excuses I know it can be frustrating I really do. Take into consideration one CI special agent covering five states all throughout the country; it's just impossible to get out there to give you that feedback on a specific report in many cases. And also consider that the majority, the vast majority of analysis we have on these SCRs is classified at the no foreign level, secret no foreign so we wouldn't be able to call you to discuss or email that back to you. It has to be an in person, onsite visit, which you can imagine is extremely difficult in some cases. That being said we're doing our best, call your CI special agent if you have concerns and just express it. Just talk them and just say you know I was really expecting something back. I get that all the time and I

encourage my facilities to do that and I hope your assigned agents would as well. So go ahead and reach out to them; let them know that you talked to me in this briefing and I'll take the call and deal with it.

<next slide>

Conclusion

Alright as always visit our website; everybody knows it your special agent can come out to do briefings just like this. Foreign visitors we can discuss that. Specific travel briefings that are classified, if the employee is unclear then of course we would make it an unclear presentation where we still go over some of the threats, we just won't discuss MOs and techniques that they may encounter.

If you specifically want to look at counterintelligence and that's a simple dropdown on the website, dropdown to directorates to counterintelligence. Always, as always contact your local IS rep and CISA if you have any other questions associated with this presentation whatsoever. At this time I want to again thank you so much for taking the time to participate today, and I'm going to turn it back to Pete.

<next slide>

Thank you Mike very good presentation. I think you purposely went over time so you wouldn't have to field any questions. You did answer a lot of the questions during your presentation that came in during registration and I will let the participants know that any of those questions we didn't get to, we will answer and post in our archives. So check on us in a week or so and hopefully we'll have those answers up there for you. I also want to remind you it is counterintelligence training month here at CDSE; we have lots of great training available online if you haven't seen it check it out. And if you liked what you saw today, you know like give us a thumbs up in the survey. If there's topics you'd like for us to cover in the future, let us know and we'll see what we can do to accommodate you. So unfortunately we're out of time, you'll have a great day.

Take care.

Thank you this concludes today's conference you may disconnect at this time.