Rebecca Morgan: Good afternoon everyone. Welcome to today's CDSE counterintelligence webinar series.

Peter DeCesare: Today's topic is Insider Threat for DoD professionals. We'll focus on the Insider Threat policy, establishment of an insider threat program, and the multi-disciplinary approach to combating the Insider Threat. As Ms. Morgan said I'm Peter DeCesare, the counterintelligence curriculum manager here at CDSE. I'm joined by Rebecca Morgan a counterintelligence and cybersecurity instructor at CDSE. Becky?

Rebecca Morgan: Thanks, Pete. Welcome everyone. I'm really excited about today's topic. I know a lot of our listeners are standing up Insider Threat programs themselves at the various commands within DoD. And we're very lucky to have a special guest speaker today to help you address policy issues related to that. We have Mr. Don Hopkins. He's a representative from the security policy and oversight division over at OUSD(I). He works in that shop under Mr. Jim Nelson who is actually the direct POC for Insider Threat. But I think Mr. Hopkins is going to be a really great resource for all of our listeners here today. And I'm excited to have him with us. So, welcome Don.

Don Hopkins: Thank you, Rebecca, and thank you Pete for the invitation. I hope that our session today is productive and tries to get some questions that the folks in the community have.

Peter DeCesare: Before we really get in to this, Becky if you would please take a moment to instruct our listeners on how to maneuver through.

Rebecca Morgan: Yes, Pete. For those of you who have not participated before there are a couple of little tricks to navigating the meeting room.

Webinar Producer: Please standby.

Rebecca Morgan: For those of you who have not participated before in addition to occasional audio glitches, we also have some other things that will help you navigate. Up at the top right there's a button with four arrows. This will enlarge the screen. Just remember when you're in that full screen mode if you'd like to go back and participate with some of the other things we have available here in the connect room, you'll have to close that screen. And you can do so simply by clicking that icon again. We also have a file share box down in the lower portion of your screen. We have a PDF version of today's presentation available there. You can click on that and download it at any time. We also have closed captioning as a feature of today's webinar. That'll be the text representation of the presentation. If you wanted to turn that off there are some instructions in the dialogue box on the bottom right.

And then finally we will have Q&A sessions. I understand that a lot of you have questions. And we want to get to as many of those as we can. You can just simply type your question in the box

and we'll work those in throughout the presentation. So thanks once again. I'm going to pass it back to Pete. We want to get started on today's presentation, Insider Threat for DoD Security Professionals.

Peter DeCesare: Thank you, Becky. And good afternoon everyone. Thank you for joining us. The DoD Insider Threat policy was issued in September 2014. So obviously it's a hot topic. We've got over 1,000 folks registered for today's webinar. We're fortunate to have Mr. Don Hopkins from OUSDI to speak with us. I'm not sure if it's because it is such a hot topic or because Don is probably the most interesting person in the world. But in any case we're fortunate to have him here with us today. As you can see from the agenda we're going to get into the policy in general. Then we'll get down into the weeds a little bit on Insider Threat reporting requirement as well as Insider Threat training requirements. As Becky pointed out as we're discussing the Insider Threat, you're welcome to post any of your questions in the question box. But with the number of folks we have listening in, I probably won't have time to address every question. However that said, we will post any of the questions and answers in our archive after the fact. Before we get rolling here, I want to take a moment to make it clear that today we're talking about the DoD policy.

We've had several of the folks that registered today had some concern about the upcoming conforming change to the NISPOM, which will include Insider Threat to the industry policy. Mr. Hopkins will discuss a few of those points. But today's focus is more of the DoD policy. So I just wanted to make that clear. In the future once the NISPOM conforming changes are released we'll probably have a follow up webinar to speak specifically on industry. I'll point out CDSE has a job aid posted where we're providing a lot of information for you already. And I believe there is a memo available at DSS discussing Insider Threat for industry. And once that comes out to get down into that policy as well. So I wanted to make that clear upfront. We're going to focus on the DoD policy. So let's get started. Mr. Hopkins, welcome again to the CDSE CI topics. Good morning.

Don Hopkins: Good morning, Pete, Rebecca, and everybody out there in the community today. And thank you for joining us. I know this is a topic that many folks are interested in. And I would like to point out the focus of our discussion today will deal with the policy for the insider threat program at the DoD level and across the components. If you want to know issues dealing with business practices, the analysis center, the DITMAC, and industrial security and the impact on industry, those will probably be discussed in another forum. I may be able to answer some of those questions today. We'll just see where it goes. But again I wanted to remind you that the focus today will be on the policy. I'll try to touch on the points I feel are most important and hope you see it that way as well.

So let's go ahead and move on and talk about the directive that came out. The DoD directive sets the baseline policy for the program. And the department as such will implement the national Insider Threat policy. That document assigns responsibilities to the USD staff, DSS, DIA, and to all of the component heads throughout the department. And I want to emphasize that that includes those agencies such as DARPA, Defense contract audit agency, DITSA. Not only the intelligence components that feel they have a greater role within the department. So POW/MIA I'm thinking of you as well. This policy applies to all the components. Secondly I'd like to state that it also applies to all contractors and other non-DoD entities that have authorized access to DoD resources per a contract or an agreement. And as stated by Pete earlier with regards to the

industry and the contractors, the applicability of this policy will be stated or reflected in the change two. So I'll address that momentarily.

Rebecca Morgan: Mr. Hopkins if I could just jump in here, I think there's sometimes a misconception in the policy. I see it also in the 5240.06 where it applies to DoD components and contractors. What that is really stating is that it applies to contractors that are working inside a government facility. And that's different than national industrial, national industry as a whole. But the applicability is just to those working in the facility. And as Pete pointed out and you're talking to this point also there is that conforming change coming. We actually did get the opportunity to get briefed by Ms. Kathy Branch. She works right in your office there, Mr. Hopkins. And she has been briefing as Pete pointed out a memo. They're calling it an external website notice that is briefing some advanced information on intelligent, excuse me insider threat requirement for industry. And that's available not only on the DoD website but our Insider Threat toolkit as well.

Don Hopkins: Absolutely. She is working on that. And we're working in close coordination with her as to how that impacts the various components. And so continuing on this particular slide once again the principle staff is laid out. It will indeed do the functions as you see on the slide. All that information will come from a variety of sources. It'll come from counterintelligence, from security. It'll come from cybersecurity, military and civilian personnel information, as well as workplace violence, law enforcement, and other particular agencies. It requires DoD to make available the required training on Insider Threat to all personnel. And I'll highlight that in a moment. It does not negate other reporting responsibilities prescribed in other policy issuances. And the policies throughout the department must be evaluated and modified to facilitate the insider threat collection analysis reporting and response actions. And I want to emphasize that. That's much easier said than done. And so we have to look across the spectrum of all the security policies to make sure that insider threat is properly reflected in those.

Peter DeCesare: If I could interrupt a second, Don. That application in my understanding is it applies to those who have access to classified information or classified systems. It doesn't get in to unclassified access or proprietary sensitive information. Is that a true understanding?

Don Hopkins: For our particular policy, it applies to DoD resources.

Peter DeCesare: Okay.

Don Hopkins: As indicated in the directive. So at this time, I mean we're talking about facilities, we're talking about personnel, we're talking about information. It is not confined. Our policy is not confined to classified information.

Peter DeCesare: Okay, good. Thank you.

Don Hopkins: Okay moving on the next slide. We have that up now. The information that we do gather within our TMUs or hubs must be handled and protected in accordance to the policies and laws governing policy, civil liberties, and all whistle blower protections. Furthermore, they have these responsibilities. They have to implement the minimum standards. We'll cover those in a moment. They have to establish a management capability to integrate the monitoring analysis reporting and response to Insider Threat. The “Hub” as it’s been commonly called is to integrate and monitor and analyze report and respond to these threats. They must

have input and advice therefore from experts for security, for counterintelligence, for human resources, cybersecurity, mental health, as well as legal support. Component heads must also conduct self-assessments of their own programs. And they must verify that contractors and other non-DoD entities are complying with this policy.

Rebecca Morgan: Don, I would like to jump in if I could. It's probably one of the most exciting parts of the 5205.16 to me because it really recognizes that multi-disciplinary approach to combating the Insider Threat. As you say you're pulling in from a variety of resources, the cybersecurity experts, HR, law enforcement, counterintelligence. Pete and I actually had the opportunity to get briefed by two really good programs that have been recently stood up. One was DIA and the other was a major defense contractor. In both of those cases, the hub really operated as an aggregator to look for illicit activities and then they pushed it back out so those existing channels whether it be to the CI shop, HR, Security, as the case may be then acted on them and pursued them as appropriate. And I think there's been, you know, a little bit of misunderstanding as to the operational nature of the Hub. I realized implementation guidance is coming out and commands have leeway to interpret things a little differently. Stand them up a little differently, but we have seen these successful models that were analytically based, but still drew on them, pretty successfully happening out there even right now.

Peter DeCesare: We had a question come in. There was still some issues on the application of the policy to classified information. Could you restate what you said about the application to classified or non-classified information?

Don Hopkins: Well, basically the policy deals with establishing the Insider Threat program. And that deals, the mission is so we can protect all of the DoD resources that we have been given authority and control over. And so that not only means facilities, it means personnel. It means the information that we have to operate and generate. And so it is not confined solely to classified information.

Peter DeCesare: Thank you.

Rebecca Morgan: And I'm reminded, Mr. Hopkins, when we talk about protecting information, even some of the larger policies if you look at the laws, for example, Espionage. It doesn't mention classified. In fact under Title 18 it is transmittal of information with respect to the national defense with either the intent to harm the U.S. or aide a foreign power. It doesn't say classified in there either. But those kinds of indicators of activities, whether it would be espionage or some of the other things that you just brought up are similar indicators that will probably bubble up through the hub and they will be reported appropriately. It's one of the win/wins of having this kind of integrative holistic insider threat program where you can identify all those activities, whether it's capturing the transmittal classified information or some of these other issues.

Don Hopkins: Yes. Okay on this particular slide I wanted to highlight some issues that were placed upon the department as well as other departments and agencies within the government. These are the minimum standards for inside threat program. First we must designate a senior official. And what I would like to highlight there is that individual must be, or must be given the authority to oversee and manage that program. And so many folks have come in to the office and said well can we have an individual of a grade of GS9 appointed as the senior official? And the answer is I really don't expect that. But if that individual is given the proper authority to

manage and oversee the program, then that could happen. But the thing that I want to emphasize is that this is just not an assignment just by paper. The person must truly have the authority to run the program. Secondly we need to build and maintain an analytic and response capability to identify, mitigate, and counter Insider Threats. We must train those folks that will be working within those hub or activity on such things as procedures, authorities, and constraints.

We must establish procedures for the secure sharing of information or, put another way, we must be able to direct and facility access to key information. We must monitor the user activity on classified networks to detect activity indicative of insider threat behavior. The standards for that particular requirement, not only are mentioned in the minimum standards at the national level, but the committee on national security systems have established a directive number 504, which specifies what the requirements are for user activity with regards to monitoring user activity.

Rebecca Morgan: Mr. Hopkins.

Don Hopkins: Go ahead.

Rebecca Morgan: We had a question about "Will employment opportunities be opening up for management of the program at these different levels?" I guess people are wanting to know will there be an Insider Threat designation as a security identified field?

Don Hopkins: Number one, there won't be a specialized field established such as an 080; however, the identification of the position with regards to a program manager or senior official is at the discretion of the component head.

Rebecca Morgan: Understood. Thanks, sir.

Don Hopkins: The next thing I'd like to highlight is that the components must provide initial and annual refresher training to all cleared employees. And so this is a standard requirement, which is separate from the training that we provide the specialized individuals or personnel that work in the hubs or the TMUs. And so all individuals that have access to cleared (that are cleared and have access to classified information) must receive initial and annual refresher training on Insider Threat.

I'll talk a little bit about Insider Threat training later on in our webinar, but I want to point out that that initial training is required within 30 days of employment or access to classified. So we highly recommend when somebody gets read on for classified as soon as they sign that 312 that they receive some sort of Insider Threat training. And then there is an annual requirement. I'll speak to some of the training requirements later on. Thank you.

Rebecca Morgan: Mr. Hopkins, we also had another question come in. Individuals wondering how do components, non-intelligence specifically if you're not DIA or if you don't have an intel field activity stood up. How do you go about finding a good model and developing the Insider Threat program or a hub?

Don Hopkins: Well they are certainly free to contact our office. Our office is working with all 43 components with regards to the requirements here. We have a pretty good handle right now

on which agencies and components have mature programs. And we can steer them to those folks with regards to getting best practices and lessons learned.

Rebecca Morgan: Understood. Thank you. Okay, so let's move on to the senior official responsibilities.

Don Hopkins: I emphasize this particular slide because in far too many communications we've gotten word from individual assigning components that they are an individual, a senior staff officer who has basically been assigned this responsibility verbally. They've been given a second or an additional duty that they are the senior official for Insider Threat. We certainly can't control that. But what we want to do is highlight to all components that have these programs that there are responsibilities inherent with this position. And they are serious responsibilities. Again if you recall back on the first slide I indicated that the senior official must be given the authority to perform these functions, because he's going to be working with so many folks within the component. And so that individual once designated and we expect that designation to be in writing. That individual will manage and oversee the program within the component. And that he or she will be the sole individual who develops the resources that must be taken to the component head.

If this is not done, than you will never see resources. And so NITTF the National Insider Threat Task Force has developed a cost-based estimate tool that's available to all components who have Insider Threat programs to be able to establish or try to develop a cost estimate on setting up the program. But the thing I really want to stress is that the senior official must develop the resource requirements and submit it to his component head. I say that because at the DoD level, we're reaching out to all the components to find out what those particular costs might be in money and in personnel.

As you all know as you have been working with this at any time that there are no dedicated resources in any funding lines reserved for Insider Threat. Now having said that, there are frequent times when the department gets a phone call or gets an e-mail and indicates that for some reason Congress or some other agency has decided to give us some money specifically earmarked for Insider Threat activities. And we in all good faith cannot utilize those resources unless we have identified requirements. And so I truly encourage all the components that if they haven't done so already to identify what the cost might be as they stand up their programs and hold on to that estimate as an unfinanced requirement so that if at some time some external agency will contact you and say: I've been given $10 million, how can you utilize this money? You will have a viable answer.

Rebecca Morgan: Mr. Hopkins. Can I just ask is there a way our listeners can get a hold of that cost estimator that the NITTF put together?

Don Hopkins: Yes. I'll make sure that particular tool is available on our security website. Which the OUSD has a website. Rebecca, I'll get that site to you and so you can put it in the minutes of the meeting.

Rebecca Morgan: Great. Thanks.

Don Hopkins: The next slide I want to highlight is what the senior official must develop for that program. Furthermore he must develop an implementation plan that formalizes the program and

provides guidance to those who are responsible for operating the program. Next as you can see there are several reports required within an Insider Threat program. Some of those are specified within this particular document, within the .16. And others will be highlighted in the DoD Insider Threat implementation plan that will be coming out for staffing, for formal staffing, within the next two weeks. And then lastly, we have to make sure as indicated that all of our folks that are working on the Insider Threat program are trained on proper handling and use of records and data. Because as you know this information, once it comes to the folks that are working our analysis center, it will be sensitive information. And there are some parameters and guidance, and laws that dictate how we handle that, how we store it, and how we protect it.

Rebecca Morgan: And Don, I'm really glad that you brought this issue up. You know consulting with legal on some of these oversight issues is really critical. And it's not just the 12333 intelligence laws that people are thinking about. You also have to consider classification guidance for anything associated with insider threat, the managing of PII information, adherence to the privacy acts requirements. And when you start looking at all those different elements it's like a better call Saul or whatever the name of your general counsel is. Make sure you're working in concert with them. And also this is not just to protect individuals, which is of course a key component of these regulations. But when you're looking at perhaps down the road prosecuting an individual for illicit activity, not having all these ducks in a row can have a very big effect on the outcome of your case. So you really have to make sure that Is are dotted, Ts are crossed. And so any good Insider Threat program is going to be stood up hand and hand with the legal advisement at that component level.

Let's move on and talk about some of the programs you have identified.

Don Hopkins: First what I would like to do is highlight and go back to the very beginning and the initiation of the Insider Threat program. Executive Order 13857 basically established or forced those agencies and departments in the executive branch to establish an Insider Threat program. And initially the focus that they wanted to, that those programs to look at dealt with prevention. To where some of these examples that they gave were to control removable media, which we have taken action on; to reduce users on computer systems; and to establish access controls on those computer systems.

That particular executive order also established the National Insider Threat Task Force, which in collaboration with the senior committee for information sharing and safeguarding pretty much established the national policy, codified it in this particular order, and also reflected it in the white house memo that was issued in November of 2012 that established the national Insider Threat policy as well as conveyed the minimum standards for programs, as we discussed earlier. Additionally we've had program requirements that have come down from the national intelligence. Some of those have been particularly focused on the use or the control and the scope of privileged users, whether or not that scope needs to be modified. How those privileged users have access, whether that particular access needs to be modified, whether their clearances are still valid, whether they are out of scope. And so there are some steps that were addressed in those memos.

In the memos that came out, many mitigating measures to try to facilitate or reduce the number of unauthorized disclosures. Also, to mitigate any releases of classified information on the information systems were identified in those particular memos. And then lastly, the Navy Yard based upon that shooting incident we developed an implementation plan that came up with

several steps that had to be established throughout the Department. At the DoD level we've been tasked to implement continuous evaluations. And I say that because I want to highlight the evaluations as one mechanism within the Insider Threat program that is not mandated or required at the component level. Right now it is only mandated at the DoD level.

Rebecca Morgan: You know, Don, Pete and I had the opportunity to go out and provide some training for the Continuous Evaluation Concept Demonstration. And what we did was help them to identify where espionage or Insider Threat indicators manifest in records checks. And although this continuous evaluation is not required of any of the component levels, I do imagine that many of the hubs or TMUs set up are going to be relying on databases or other records for their input. So it is important for everybody to remember as you're searching that information for anomalous activity or Insider Threat indicators that it is probably going to come in that format of the records check. I also wanted to say, you know, you are listing all these additional program requirements. It brings to mind the reissuance of the DTM 08-052 which came out last October with some updates. That's a document that reemphasizes that should there be an issue with overreach or improper use of intelligence activity that those would be directed to the attorney general instead of Wikileaks or CNN News or something like that.

That regulation was strengthened in the wake of Snowden. And I feel some of our listeners as they look at this long list and they talk about these different policies. They are saying I tuned in to hear about the 5205.16 and now you're talking about all these other things that I have to comply with. I want to reassure people that this really isn't a lot of different requirements. It's a lot of things that converge and meet each other for the same goal. It seems to me to represent a real maturation of DoD policy. Much the way that the DoD Cybersecurity policy was updated last year. Some of our listeners may know it was rereleased last March under the 8500 series. What it did was align DoD information assurance with the federal requirements under FISMA. And in much that same way the Insider Threat policy is aligning DoD insider threat with those national minimum standards. And one of the cool things about the 8500 update is that it really strengthened the information and continuous monitoring, the auditing portion, which feeds right in to this insider threat. And so rather than people seeing this as a barrage of policies and how do I possibly keep them all straight - to understand that it is a holistic effort and it really represents some of this multidisciplinary approach to combating a problem that we know we've always had. The indicators have not changed and we know what they are, but we have trouble recognizing them. We can use all of these various resources and find a way to do that. And that's what I think is exciting about the .16 and how it pulls this all together.

Don Hopkins: That particular plan was approved by the secretary of defense. He directed basically four particular steps occur based upon that. One was to implement CI as I indicated earlier. The second one is to establish the DITMAC, which we're moving out on. The third one is to establish a centralized principle staff assistant, a PSA for the integration of CI and DITMAC. And that particular PSA is for intelligence. He has been duly appointed that. Then the last one is to accelerate the deployment of a tool that they are calling the identity matching engine for security and analysis. And it is called IMESA.

This particular tool provides the capability to vet the credentials of individuals, authorized access to DoD installations. And they vet that identity and credentials against DoD, federal, state, and local authority data resources using information. And so the architecture of the IMESA system will enable personnel access control systems at the gate to authenticate and approve physical access credentials. And they will do that electronically and in a secure manner.

And provide information management against those authorities' data bases. And so one particular example you might have is for a vendor that comes to the front gate of Fort Meyers, Virginia. And they will scan those particular credentials into the system. And if that individual has an open want or a warrant in the FBI data base, then we will get a red light. And if that's the case, then that individual will be brought to the side.

If the installation has any jurisdiction over that individual, the MPs will take care of that individual. If not then the individual will be asked to leave. And we'll probably not see him again. And so that's one particular system that we have operating at the gates. And I believe right now it's up to about 211 installations. And our goal is to get 385 installations throughout. We are looking at applicability, but there are a lot of privacy rules and of course international agreements that stand in the way of doing that.

Rebecca Morgan: Mr. Hopkins if I could just pipe in. We have a question about when is IMESA, if I'm saying the acronym correctly, online. And does it do live checks or are those batched?

Don Hopkins: Well, I mean it's operational right now. The only inhibiter to the system is whether or not the various installations have the appropriate devices at the gates to identify the credentials. Once it's scanned, it is instantaneous. You'll have a feedback from the FBI database.

If the component does not have this capability already, it's something that it hasn't reached that facility at this time.

Rebecca Morgan: But it's out there? It's live and working?

Don Hopkins: Correct. It's out there; it's operational. The only thing that's holding us back is installations that have not reprogrammed or budgeted money to buy the device.

Rebecca Morgan: Understood.

Don Hopkins: Okay so I believe that's the last slide that I have. Going on, Rebecca?

Rebecca Morgan: All right. Thank you so much, Don for sharing those. I did just want to point out a couple of other things while we're here with our listeners before we get to the Q&A. And one is the reporting element. I know everybody is in the process of standing up their Insider Threat programs, but just a reminder that in the interim you still have requirements for reporting activity. Whether that's in the 5240.06 CI Awareness and Reporting, which does outline in Enclosure 2 a number of potential espionage indicators or Insider Threat type of behaviors that would be reportable.

Some of those would be DoD internal to your security office, HR personnel, MILDEP CI etc. We also have requirement under the intelligence reform act for 811 referrals to the FBI if we know of active espionage going on at the moment or the active transfer, illicit transfer of classified information. That would be equivalent to a 1301 referral requirement for the industry listeners. We are also required right now even as we're standing up the Insider Threat programs to report any adverse information on individuals that hold a position of trust with the government. And so those would be items that violate or fall under the adjudicative guidelines

of the personnel security program. Those also require reporting, equivalent to what would be a 1302A referral under the NISPOM.

I've also had a lot of people asking about the DITMAC. That is a program that is being stood up. And there might be some additional reporting requirements put on the components in the future. We don't know yet exactly how that's going to look. But that's something that'll be pushed forth very much ahead of time - that sort of requirement. I just want people to understand now though that even though we're standing some programs up it does not negate the existing reporting requirements that you have. And you still need to make sure while you're putting things in place those channels are still open and you're sending that information out.

I also did want to expand a little bit on the training requirements. Mr. Hopkins went over the general requirements. And so in general, individuals are going to need to have an insider threat awareness level for all of the personnel. And then program management personnel are probably going to require some additional training. There are a lot of resources out there. I don't want people to just go looking for the training that says Insider Threat training on it. There are a variety of sources and a variety of needs that could provide this for you. Anything that has to do with some baseline auditing and continuing monitoring would probably be a good idea for some of your hub personnel. Getting back up to speed on some of the basic personnel security and even general security requirements. Even physical security requirements, if you're looking for indicators such as people coming in and out of the facility when they shouldn't. Understanding some of those regulations can be helpful as well. I would also recommend - yes, Pete.

Peter DeCesare: Becky, the national minimum standards basically require those Insider Threat program managers and those working with the Insider Threat program receive training in fundamental counterintelligence, Civil liberties, those types of things. So not only is it a requirement for everyone with access to have Insider Threat training, but there are specific requirements for additional training for those Insider Threat program managers.

Rebecca Morgan: Absolutely, and it's a wide variety of things that people are going to have to understand in order to manage effectively. And so obviously CDSE has some great stuff out there. I'll pass it off to you in just a moment to discuss the general awareness training as well as specialized stuff that we have. I do want to point out that the National Insider Threat Task Force puts on a pretty good show. They have an instructor led training that talks about TMU or hub type of activities. It's not designed for DoD per se; however, they put a really great emphasis on a practical exercise and provide a lot of opportunity for understanding how to recognize anomalous behavior that's reported from a variety of sources as well as how to manage that information once it comes in. So it is worthwhile checking that out and really there are resources out there. Pete and I have put some of that together under the Insider Threat toolkit. But I'm going to pass it over to him now and let him expand a little bit on some of the cool stuff we have going on at CDSE related to Insider Threat.

Peter DeCesare: Thank you, Becky. As I mentioned, everyone who has access to classified must receive Insider Threat awareness training within 30 days. And the CDSE developed a course, insider threat awareness. It's free and it meets that initial and annual training requirement. So, you know, come to our site. It's there, it's for both DoD or industry.

The second course you'll see under the training is Establishing an Insider Threat program. We've developed that for those who are designated as the insider threat program manager or working

on insider threat. It pretty much provides an outline of those issues that you should discuss and include when developing an insider threat program. It kind of tells you that you must reach out to the rest of your folks in that organization. Include your legal folks and your HR folks, and your CI and your security folks. And kind of take a team approach. We refer to it as a hub. But it's not just the Insider Threat program manager's responsibility to know everything that's going on in your organization. So it takes that approach - how to develop your program and tailor it to your own needs.

As Becky mentioned the CDSE has an insider threat toolkit. We've put a lot of resources and policy information there for your use. In the past we've had a few webinars that get into insider threat and other espionage indicators and CI awareness type of things that'll help you do your job in the insider threat program and report suspicious activities. I also pointed out that the DSS counterintelligence office on their website offers a lot of very good CI training materials. I'm proud to say the NITTF actually designated that Insider Threat awareness course that CDSE developed. They put out a directive basically directing all government agencies. If you don't have a good training program, they recommend you adopt this CDSE course. So I'm really proud of that course. And we expect a lot of traffic there now that this is a required training for everyone with access to classified. I think it's about time to get in to some of the questions.

Rebecca Morgan: Before we do that Pete, I want to point out we have a new job aid that just came out understanding espionage and national security crimes. That could be pretty critical for understanding the differences as well for Insider Threat program management personnel. But we do have a lot of questions out there. Everybody's interested in talking to Mr. Hopkins to hear our most interesting man in the world. Pete, do you have a couple that you wanted to start off for us?

Peter DeCesare: Well, let me start off with what will motivate other agencies to participate in information sharing?

Don Hopkins: Well, my response to that would be that we truly can't get a good picture of what the Insider Threat is if we don't have sharing of information across the various agencies. I don't understand why the motivation would be something other than wanting to preserve the security and integrity of the work force and of the DoD resources.

Peter DeCesare: Okay, good. I know we're putting an emphasize on the DoD policy, but we do have a lot of participants on the industry side. And they're sending in some questions like when do we expect the NISPOM conforming change? I believe it is due out in the fourth quarter. Is that true, Don?

Don Hopkins: The goal of publication for the conforming change two is the fourth quarter of this year. DoD is in the final stages of gaining consensus with the other security agencies. That includes the department of energy, regulatory commission, and the office of DNI, and the department of homeland security. The NISPOM change will then go through a final pre-signature edit. And then must go through a legal sufficiency review. Regrettably that's something we can't avoid, and that will take some time. But cleared contractor facilities will have no more than six months from the date of publication of the change to implement its requirements. And I know there have been some questions as to, you know, will the conforming change be different from those requirements in the .16 of the DoD directive. The answer is no. Let me recap what we are levying on industry. And they must establish and maintain an Insider Threat program.

They must designate an insider threat senior management official. That individual must be cleared in connection with the facility security clearance. And that individual is responsible for establishing the program within that particular activity. And now that individual may be the security, the facility security officer, the FSO. But he also has to be a senior official who is on the key management personnel list for the cleared contractor facility. And that individual may serve in the same role for an overarching business organization, but would have to be again on the key management personnel list. So the cleared contractor facility must have an insider threat program that gathers, integrates, and reports as required by the government CSA.

Peter DeCesare: Okay, good. I think some of my FSOs are concerned that they will pick this up as an additional duty. Do you know if the conforming change specifically says the insider threat manager must be the FSO?

Don Hopkins: Well, I do know it doesn't mandate that it be the FSO. That's left to the discretion of the organization of the industry. However, the FSO must be an integral member of declared contractor Insider Threat program team.

Peter DeCesare: Okay.

Rebecca Morgan: I just wanted to point out at the beginning of the session we mentioned that Ms. Branch, the delegate to OUSD(I), has been promoting a memo or an external website notice, I think they are calling it an external notification that they are providing some of this guidance. It is available on the DSS website. There's a link to it inside the Insider Threat toolkit that we provide here at CDSE. If you go under policy tab and DSS policy, there is a link to that external link memo.

Mr. Hopkins we're getting a lot of other questions come in. And one person has asked did we hear correctly that the OUSD(I) implementation for a 5205.16 should be out in two weeks?

Don Hopkins: It should be out in two weeks for coordination. Not final, not signed, but out for coordination within the components.

Rebecca Morgan: Understood. Okay. Now there've been a few questions about how this is going to be paid for. I know you talked about putting that cost estimator together and having it prepared should funding become available, but I see a few people asking what comes off the plate in the meantime.

Don Hopkins: Regrettably what I have told you is that you need to approach, if you're not the senior official you need to approach the senior official. If you are the senior official you need to approach your component head and indicate what the requirements are that you've defined. And it is up to the component head at that time to decide how he's going to support this program. This is nothing new. It's an unfinanced requirement. And so you must establish priorities within your particular component. And you'll fund those for the priority. We pray and hope that the Insider Threat program is given a high priority.

Rebecca Morgan: We're hoping right along with you. I have a couple other questions I want to get to. One of the listeners asked, with the insider threat program inherently fall to the special security offices of the world or can this be managed by collateral-only office?

Don Hopkins: We've heard this discussion before. I can't give you an official duty position; however, based upon some conversations that I've had with many folks that have come out of the CI world, they strongly believe the insider threat program falls within the security construct of an organization as opposed to a counterintelligence component.

Rebecca Morgan: Okay, we have some listeners wanting to know where are the specific training requirements for hub personnel identified? So not the general requirement for Insider Threat awareness, but specific to the Insider Threat management personnel.

Don Hopkins: I may have to defer to Pete on that. I do have some lists that we have captured in the implementation plan. But Pete, why don't you try to take that and I'll see if I can find my listing.

Peter DeCesare: All right, Don. In the national minimum standards it lists several (I guess four or five training requirements) for those folks designated as the Insider threat program manager.

Rebecca Morgan: Alright. Thank you so much for that, Pete. I have another one that I'd like to post to Mr. Hopkins. One of our viewers has asked "With all the information given, I'm assuming that it will take in to at least the fourth quarter to have an Insider Threat program established and possibly the first quarter of 2016 for implementation?"

Don Hopkins: The basic requirement for having an established program is that you have a senior official designated. That you have a policy developed, and that you have an implementation plan signed and developed. Those three key requirements will allow you to stand before me or anybody and say that you have an insider threat program. Of course the tenants and the parameters of that program will take time. But if you're concerned or if your senior officials are concerned, it's whether or not you can give a thumbs up or not. If you meet those three requirements then you will have an insider threat program in place.

Rebecca Morgan: All right, we have time for maybe one more question. I have somebody asking if DBIDS is the same as the IMESA system.

Don Hopkins: I'm not real familiar with DBIDS. I've heard of it. But I can tell you they're clearly separate.

Rebecca Morgan: Understood.

We do have one question "If you have a major command with sub elements. Do the sub elements require an insider threat manager as well as a major command?"

Don Hopkins: Once again we're working at the DoD level. And so we're requiring the component head to develop a program within his component. It is his discretion, his or her discretion as to how far he takes that down within his sub components.

Peter DeCesare: Okay. Very good. We are running out of time. But before we end today's discussion, I'd like to reach out to those participants and ask them to, at the end of the webinar today to give us some feedback there's a survey. You can give some information. Did you like today's webinar, dislike it, do you have recommendations for future webinars. I'd also like to

remind you that any questions that we didn't get through today, we'll consolidate them and post the questions and answers on our archive. So give us a week and hopefully we'll get those posted for you as well. Becky?

Rebecca Morgan: Yes. And we apologize that we couldn't get to everybody. We have such a large number of participants and so much information to get out there that it was hard to fit it all in the hour. But as Pete noted, we will try to wrap those questions up, get with Mr. Hopkins and his expertise, and then provide those back out in a document that will be attached to the archive webinar. I do want to thank everybody who joined us today. I want to also remind you that our next session coming up is on May 14.

We're going to be speaking with Mr. William Argue who is a unit chief in the Counterproliferation investigations division at DHS. We'll be talking about identifying, avoiding, and reporting international traffic and arms regulations violations. So I hope everybody can join us for that. Registration is now open on our website. Should you have any other questions about today's event or training in the future, Pete and I have our contact information up there on the board. And Mr. Hopkins has also graciously agreed to provide his email address. You can reach out to him. And follow up with some of those items. The cost estimator is one, but he is a good guy who is out there to serve the community. And I know he's going to respond to folks. So he provided that to you all. I do see some people out there saying boy, we wish we had a longer Q&A session, and we'll bear that in mind and maybe at some point we'll come back and do this again.

Mr. Hopkins was pretty amendable for coming up and visiting us. I'll see if I can talk him in to visiting us again. So on behalf of Pete and Mr. Hopkins and myself Rebecca Morgan, I just wanted to thank everybody for joining us. Our great producer staff today, we hope you have a great day. We'll see you next time at the CDSE CI webinar series.

Peter DeCesare: Thank you very much, Mr. Hopkins. Have a great day.

Don Hopkins: Thank you.

[EVENT CONCLUDED]