DSS Counterintelligence Products and Briefings
March 14, 2013

Welcome and thank you for standing by. At this time all participants are in a listen only mode. Today's conference is being recorded; if you have any objections you may disconnect at this time. Now I will turn the meeting over to Mr. Pete DeCesare.

Hello, welcome to CDSE Learn at Lunch webinar. Today's topic is Defense Security Service Counterintelligence products and briefings. Before we get started, please be aware that the video portion of this webinar is being recorded. Once the red recording light appears we will begin. I am Peter DeCesare, the Counterintelligence Curriculum Manager here at CDSE. My production crew today includes Linda Adams and Sandy Vega. I'm sure most of our listeners today are well aware of all the web-based training opportunities that CDSE has to offer to our learning center called STEPP. Unfortunately many folks in industry or even DoD are not aware of all the great products that DSS Counterintelligence Directorate has to offer. Although the CI office is well known for their annual trends product, they also produce several other very useful products. With us today we have Mr. Brett Young, Chief of the DSS CI Production Branch. Brett has been in the intelligence business for over 23 years and with the DSS CI Directorate since December 2010. Brett, it's been a couple of years since I worked down at the DSS CI shop and I'm impressed with all the new products you are making available to our customers. Please tell us about your products and how we can obtain them.

Thank you, Pete, yes; we have added several new items over the past couple of years to meet the needs of cleared industry. Good afternoon, everyone, as Pete stated I am the Chief of the Production Branch at the Defense Security Service, Counterintelligence Directorate. Today I will present a webinar on DSS CI products and briefings.

Next slide, please.

Let's get right to this, here's the agenda. We will begin the discussion with the mission of DSS, the DSS Counterintelligence Directorate, and then cover the established product types, standards and requirements of the Intelligence Community and DoD that DSS applies to finished products. For clarity during the briefing, I will often refer to the Intelligence Community as the IC and Department of Defense as DoD and Counterintelligence abbreviated CI.

We will cover the specific DSS products, briefings, outreach and training, and finally we will discuss how DSS disseminates these products, and, naturally, how you can find these products.

Next slide.

You may already be familiar with the DSS mission statement. National security is our mission. We support national security by securing nation's technological base and overseeing the protection of classified information in the hands of industry. Our nation's technology is our

nation's jewels. They are constantly under attack by foreign collectors of technology. Protecting a technological advantage supports the warfighter while also protecting economic advantages of being a leader in technology.

Next slide.

Specific to protecting the technologies resident in cleared industry, DSS Counterintelligence directorate identifies the unlawful penetrators of cleared industry. We analyze reporting from industry and from the intelligence community in order to assess the threat posed by foreign collectors. We articulate this threat to leaders in cleared industry and the United States government. The products I will discuss today constitute a large portion of articulating the threat.

Next slide, please.

And here we have our first poll question, but we'd like to ask the folks other than the DSS DoD, how many government agencies does DSS support? Alright click in the box there folks and tell us what you think. Alright it looks like 25 is the winner of the race here is that right? They are correct.

Okay, let's move on to our next poll. I mean our next slide. Thank you.

As you can see, there's plenty for all of us in CI to do. DSS mission under the National Industrial Security Program goes well beyond just protecting technology being developed for or deployed by the Department of Defense. DSS supports 25 other government agencies outside of the DoD. Also you will note that the cleared contractor base is quite large, including over 10,000 companies and over 13,000 facilities, and 1.2 million personnel. That leaves DSS CI pretty thinly spread across a very large enterprise. Even with the large volume of reporting we receive, we receive this from just over 10 percent of cleared facilities.

Next slide.

Now we'll talk about Department of Defense Counterintelligence production and production types. We put the information and analysis into a number of different forms. We tailor the products to the content, the need, and the audience. Some are more time-critical than others; some are intended for a particular segment of our audience, such as a specific company. Most of DSS products fall into the following categories: Assessments—assessments are large finished products that include all source information and have been coordinated with our partners in the DoD counterintelligence community.

Analysis reports are generally shorter than assessments and do not require the same level of coordination.

Threat Advisories—these tend to be shorter and relate to an imminent threat or recent incident that we believe our government and industry customers need to have knowledge of. They contain information relating to the threat or incident and often have limited analysis due to the time constraints.

Current Intelligence Reports—these reports tend to be periodical; either a daily, weekly, monthly, or possible quarterly—and they are usually in the form of an activity report.

Name checks or Name traces are information reports pertaining to a company or individual, they're more like a fact sheet than a finished product.

Intelligence Information Reports, or IIR, are not finished intelligence. They are raw information reports.

Next slide, please.

We apply the Intelligence Community Analytic Standards as identified in the Intelligence Community Directive Number 203. The IC incorporated these best practices as standards to improve and ensure the quality of analysis. The Office of the Director of National Intelligence uses these standards to conduct evaluations of intelligence analysis produced by any element of the IC. DSS CI finished intelligence products are subject to these evaluations. As part of applying these standards, DSS adheres to the standards of analytical tradecraft. For example, in our products we clearly delineate analytic judgments from facts. We place analytic judgments in highlighted Analyst Comment paragraphs and include a confidence level on any analytical comments. We also include confidence level on an outlook, which is an estimate of the outcome or impact of a particular event or activity. Analytic products, such as assessments, analytical reports, and advisories have to meet the standards identified in DoD Instruction 5240.18. As an example, assessments have the most stringent requirements.

To meet the standards, an assessment expresses analytical judgments and the degree of confidence in those judgments; identifies underlying assumptions; incorporates all-source information, identifies gaps in information or intelligence, that if known would contribute to the value of the product; discusses the potential outlook; and is coordinated with other members of the CI analysis and production enterprise or the IC. This level of detail is why assessments have a long production timeline, which can run from weeks to months.

DSS applies the standards listed in the DoD instruction to our products. A quick note—during this webinar, I will mention open-source and all-source. Open-source is publically available information. All-source refers to leveraging information from multiple intelligence disciplines and including open-source information.

Next slide.

Alright, here's our second poll: Our flagship publication is known as the Trends. How often is it published? Monthly, quarterly, yearly, or as needed? Looks like we have a race going on between quarterly and yearly. Which one's right, Brett? It's an annual product, so we do it yearly. Okay, thank you.

Now we'll discuss our Strategic Product Lines. Regarding product lines, here's what we call our flagship publication known as the Trends. This is certainly not one of the new items. I believe this year's will be the fourteenth edition of the Trends. It is an annual product that we produce in both classified and unclassified versions. It sums up a year's worth of what we learned about who's doing the targeting of technology in industry, the origins of the collectors, what agents they tend to use, what methods they use, and particular technologies they target. DSS compiles the annual Trends document in response to DoD Instruction 5200.39, "Critical Program Information within the Department of Defense." The annual Trends is an assessment; its organization and format comply with the Director of National Intelligence or CI community guidance. We coordinate this with other DoD CI community agencies and also with CI organizations outside of DoD. The Trends is one of the most cited documents by other government counterintelligence agencies and DoD when referencing foreign collection threat targeting technology.

Recently, the White House incorporated the 2012 unclassified trends into the Administration Strategy on Mitigating the Theft of U.S. Trade Secrets. Along with the annual classified and unclassified reports, we produce two quarterly editions, one focusing on cyber threat activity, and one relating to targeting of a specific technology. In fiscal year 2013 we did not publish the quarterly focusing a specific technology, however, in 2014, we hope to return to publishing it. Also this year we did modify the name of the product from "A Trend Analysis of Reporting from Defense Industry," to "A Trend Analysis of Cleared Industry Reporting." As I mentioned earlier, DSS supports 25 government agencies outside of DoD.

Next slide please.

Alright here we have our poll. The question is which type of publication is Trends? Is it an assessment, an analysis report, threat advisory, current intelligence report, a name check, or an intelligence information report? Looks like we have analysis report as a winner, and what's the actual answer there, Brett? It's an assessment. Alright. We require coordination and all those horrible factors I mentioned earlier to make it an assessment. Alright, thank you.

Alright, next slide.

Continuing with the Strategic Product lines, we have a variety of other products that come out more frequently than annually—some quarterly, some monthly, some on an as-needed basis. Our Gray Torch team produces classified company threat assessments and company snapshots. They focus solely on a single cleared contractor. Gray Torch assessments provide detailed analysis of targeting of a specific company, while the snapshot is a factsheet of reporting from

that company. We produce snapshots every six months for select companies. Snapshots are unclassified. The Snapshot is an example of a name or company trace, since it is primarily a factsheet of likely targeting of their facilities or personnel. We provide the Gray Torch products directly to the company.

The Bronze Dragon team assesses the threat to specific programs. A program like a new aircraft, ship, or weapon system often includes many enabling technologies. The Bronze Dragon team provides in-depth classified assessments of the threat posed to that system as it goes through development and testing. We provide these assessments to the government agency or agencies overseeing the program development. Like all assessments, we coordinate these with other agencies, and on many we collaborate with the component or agency CI activity in the production of the assessment.

The Crimson Shield is a current intelligence report. It is a monthly classified report with articles by our analysts that identify threats to technology.

The Scarlet Sentinel is also a current intelligence report; however, it features excerpts from open source reporting, and, thusly, is unclassified. We produce it quarterly.

The Counterespionage Branch Analysis Report, or as we call it, CEBAR, is a classified quarterly report. It focuses on incidents of potential espionage indicators at cleared facilities.

Next slide.

Here we have poll number four. This is asking which of the following you have seen or read. The Gray Torch, the Bronze Dragon, the Crimson Shield, the Scarlet Sentinel, or the Counterespionage Branch Analysis Report? Looks like the Scarlet Sentinel way out in front, Brett. Yeah, that's kind of expected since it's the unclassified document so it's easier to obtain. Alright, thank you. Move on to the next question.

The next slide.

We're going to move onto Operational Support Product Lines. At times an analyst who monitors a particular subject, a country, a piece of technology will notice a pattern in data and other reporting. He or she can then initiate a report on what they have noticed. These are special products, or analyst initiative products. Depending on the type of information and coordination, analyst initiatives may be produced in many formats, including as an assessment or advisory. We produce the Cyber Activity Bulletin each week. We usually disseminate it on Fridays. It provides security professionals in cleared industry with technical aspects of suspicious network activity noted by cleared industry and government cyber security professionals, personnel. It is unclassified. We produce threat advisories to alert cleared industry and other government agencies to recent suspicious activity, or of an imminent threat. We produce them as unclassified or classified depending on the classification of the information in the advisory.

DSS Counterintelligence Directorate's Operation Analysis Group produces case studies. They base the case studies on recent incidents of suspicious activity or espionage. These cases are generally unclassified and are a good security awareness tool for facility security officers.

Next slide.

The last of the operational support products are not considered finished intelligence products; instead they tend to be information reports. The response to an SCR and the Intelligence Information Report feature factual reporting with little to no added analytical material, and also usually rely on a single source. Also these products tend to be shared within the intelligence and law enforcement communities. We create Referral and Action packages to share with law enforcement and intelligence agencies as possibly actionable information. Many of these lead to investigations and prosecutions, and occasionally convictions, and others might be leveraged by intelligence agencies. In fiscal year 2012 other federal agencies initiated 657 investigations or operations based on DSS input.

Next slide.

So mostly I've talked about our written publications to this point. But DSS provides a variety of briefings. We produce companion briefings to most threat assessments. In some cases we design briefings for DSS personnel to provide in person to cleared industry or to government agencies. We also produce briefings for the facility security officers to use as part of their security awareness program. This includes unclassified briefings based on the annual Trends document, and travel briefings to provide to employees prior to their departure on overseas travel. Over the past few years we increased the variety of briefings we prepare for cleared industry to use. They include briefings on insider threat, on cyber security, counterintelligence awareness, and more recently, on the vulnerability posed by social networking.

Next slide.

DSS outreach and training. These products include tri-folds, handouts, and web based training. The tri-fold brochures are good for awareness and reference. As you can see, they cover a variety of security and counterintelligence topics. We provide them to improve the threat awareness of employees of cleared industry. Ideally we want personnel in cleared industry to be well-informed about the methods threat actors use to steal information, and how to report suspicious activity. These are handy for FSOs to provide to their workforce as part of their security awareness training.

Next slide.

DSS Outreach and Training also includes some other materials, like fliers and mouse pads. The fliers represent other quick reference handout to provide information about a DSS service, such as the Information Sharing Portal or web-based training. We also produce a small number of

security themed mouse pads to put security information at the fingertips of personnel in cleared industry. Not specifically a DSS CI product; CDSE provides several good web-based training opportunities to improve security training and threat awareness in cleared industry. We provided the links at the end of this webinar.

Next slide.

Here's our last poll question. Which of the following have you seen? So go ahead and click if it was a tri-fold brochure, flier, security-themed mouse pad, or the CI web-based training. Looks like we have a lot of brochures out there and quite a bit of training. I'm glad to see the training because it's important. Alright, it looks like quite a few people have seen everything. Alright, thank you.

Next.

We don't produce these products; assessment reports and advisories for our sake. We create them, as I mentioned earlier, to articulate the threat to leaders in cleared industry government. So we want them in the hands of security and counterintelligence professionals, and in the hands of industry and government leaders. Naturally classified products have considerable restrictions on their dissemination. Most of our classified products can be found on the DSS SIPRNET website. Other government agencies can easily access our products; however, this network is not readily available to cleared contractors. DSS field personnel, Industrial Security Representatives and Field Specialists often provide cleared contractors with hard copies of our classified documents. As I previously mentioned the Gray Torch and Bronze Dragon products have limited dissemination, either to a specific company or a specific government agency. Occasionally we do create sanitized versions of the assessments that have no references to a specific cleared contractor and no proprietary information. We disseminate these sanitized versions on the DSS SIPRNET website. We post our unclassified products and briefings to a password protected portal. The DSS Information Sharing Portal resides on the Homeland Security information network hosted by the Department of Homeland Security. We post material that is for official use only at this portal. This includes unclassified threat advisories, the cyber activity bulletin, and the Scarlet Sentinel. Other classified products and our outreach products can be found on the DSS website, [www.dss.mil,](www.dss.mil) or ask a DSS Field Counterintelligence Specialist. The Field Counterintelligence Specialist can assist with dissemination of a product or nominate personnel from cleared industry for access to the DSS Information Sharing Portal. DSS Counterintelligence directorate does not mass email products as PDFs.

Next slide.

So there you have it, the DSS CI product line. We feel we have a good lineup of products, and we work very hard to maintain the quality of the analysis, the writing, and the presentation. We are always evaluating, tweaking, adding, and subtracting. As Pete mentioned during the introduction, we have added several of the products I told you about just in the last few years.

Nothing is set in stone; even the flagship annual Trends volumes slowly morphs as we try to make them better each time. If time permits, I will now answer any questions you have about DSS CI products.

Okay Brett, we had a couple questions that came in. I know you mentioned this, but a reminder, how do they get their hands on your Scarlet Sentinel? We disseminated the via the HSIN portal that we have, the DSS Information Sharing Portal. Also, FCISs and ISRs, excuse me, Field CI Specialists and Industrial Security Representatives sometimes present it to facilities in hard copy.

We also had a few that came in and say: How do I get one of those mouse pads things there? Well, when we ordered them we had them sent to the field, so again in this case it's the field's CI Specialist probably has them at their office and they can provide them out. If we get another order of them again, we send them out mostly to the field offices because we see fewer people from industry here at the headquarters than they do in the field.

I think on the screen the folks can see some of those courses that we have available at CDSE. We've had a lot of accolades for some of these courses; if you haven't already seen Thwarting the Enemy, I highly recommend it for those folks in industry. Counterintelligence Awareness Reporting and new requirement, a new regulation came out, it's got a lot of good stuff there. The enclosure to that is a lot of good information. What is considered suspicious and reportable? But again, a lot of good training opportunities there.

Another question: Why doesn't DSS Counterintelligence Directorate send unclassified products out attached to emails? Well, sadly, as we learned in elementary school, one bad apple spoils everything for everyone. There are nefarious people out there that spook legitimate emails and include attachments with malicious codes. You know like malware and viruses. We want to avoid spooked emails made to resemble a DSS email from being a vector for this malware. Thusly, if you know we do not disseminate through mass email, you know not to open an attachment from an apparent DSS email with this quarter's addition of the Scarlet Sentinel. This is for general dissemination. If you contact a DSS representative and ask a rep to send a specific document, the rep will likely send it to you a document as an attachment. I'm saying be aware of mass e-mailings or those claiming to be disseminating a DSS CI product widely. Okay, good, thank you.

Another question. Why does DSS apply Intelligence Community standards to its products? Is DSS a member of the Intelligence Community? Well, DSS is not a formal member of the Intelligence Community; DSS is subordinate to the Undersecretary of Defense of Foreign Intelligence. In addition, DSS CI is a member of the DoD Counterintelligence production council, which also adheres to the IC standards. As such, DSS CI products adhere to the same standard. Finally, DSS CI collaborates and shares information with IC agencies. And since much of our work resides on IC infrastructure, it's more efficient to apply these standards to our material.

Think I have time for one more here. What is the DSS Information Sharing Portal, and how do I get access? Well, the DSS Information Sharing Portal is a password protected portal hosted on the Homeland Security Information network. We use it to disseminate useful unclassified products to security personnel in cleared industry. Access is limited to security personnel at cleared facilities. To get an account to access the portal, you must be nominated by a DSS Field Representative. Contact your local DSS and their social security representative or field CI specialist if you require access to the portal, and they can nominate you and then we will create accounts. Okay, good.

Mr. DeCesare: You know, I talk to a lot of the students up here at CDSE, and specifically those Facility Security Officers, I highly recommend that if they haven't seen some of these products, specifically your Trends document, that they should be knowledgeable on which foreign entities are targeting the technologies that they are protecting in those facilities. So again, great presentation, Brett. I am truly amazed at all these wonderful products that you folks are putting out, and great job today. I really appreciate your presentation and I hope the folks listening in have learned something and go see your IS rep or your field CI guy if you would like to have access to some of these documents. So you all have a great day. And just to let you know if you posted a question online, we'll be sure to get those answered and get those up on the web as soon as we can. So keep your eye out. Thank you!