Security Incidents Involving Special Circumstances

081513 Webinar

Welcome and thank you for standing by. All participants will be able to listen only. Today's conference is being recorded; if you have any objections please disconnect at this time. I would now like to turn the conference over to Mr. Danny Jennings; sir you may begin. Alright before we get started please be aware that the video portion of this webinar is being recorded, and once the recording light appears, we will begin. Okay I've got the red light. Good afternoon, my name is Danny Jennings. I'm the Physical and General Security Curriculum Manager here at CDSE, and I will be your host for today's webinar. Before we get started, I want to thank you for taking time out of your busy schedules to join us today. My responsibility as the Physical and General Security Curriculum Manager is design of course development and office security training.

The topic of today's webinar is Security Incidents Involving Special Circumstances. My producers for today are Rachel Mongeau and Ron Adams and at this time I'm going to have Rachel provide some instructions for you on how to navigate the DCO meeting room. Okay, thank you Danny. Let's take a quick tour of the DCO meeting room. In the left hand corner you'll find a notes box. This has the call-in number and other announcements as necessary, and these notes will remain on the screen throughout the webinar for your reference. The max review of the presentation you can click the "full screen" button in the gray banner in the upper right hand corner of your screen. However, remember that when poll questions appear, you must click on the "full screen" button again to be able to respond to the poll or also if you would like to enter a question or answer in the box you need to be out of full screen.

Speaking of the Q&A box there's one on the right and this is where you can enter any questions or feedback since all of your phones are muted. This is your only way to communicate with us. Then below you'll find the file share box; there are two files there. One contains the slides for today's presentation; you can print those out and take notes as we go. There's also an excerpt from the 5200.01 that Danny will be talking about today. This shows you an example of a poll question. We'll be popping up a couple of these during the webinar; select your answer and we'll provide feedback. Ok, Danny the audience is all yours. Alright thank you Rachel.

Let's go over our webinar objectives. By the end of this webinar you should be able to: understand the importance of proper reporting security incidents, identify the steps in the process of reporting, define special circumstances, and identify the policies pertaining to special circumstances and or categories. Like with all of my webinars, I would like to start off with a

poll question. Question is: Why is it important to report security incidents? A: It is required, B: Incidents should be reported, C: To track the number of incidents that occur within the Department of Defense on the annual basis? Alright we're looking at the numbers here and we have about 91% says it is required, another 38% says incidents should be reported, and a couple of people said we should track, but the most important answer to this question is that it is required by regulation.

DoD policy states that anyone who becomes aware of the loss of potential compromise of classified information shall immediately report it to the head of his or her local activity and the activity security manager. And if you look at the slide we highlighted the word *shall* and we did that because sometimes in the Department of Defense we tend to interpret the policies and regulations by the wording that we use, and you look at the word *shall* versus *should*. A lot of times when we use the word *should*; *should* a lot of people interpret that they have some flexibility. But the policy states you *shall* and in this case you shall, you will, and you must, so it is a requirement.

Speaking of why it's important, let's look at the case of TSE Bradley Edward Manning, arrested in May 2010 for passing classified material to the website WikiLeaks was charged and convicted on most of the 22 offenses, faced the largest set of restricted documents ever leaked to the public. Understand it's about 750,000 restricted documents. This young man could face 136 years in prison. Do you think it was an impact on National Security? What was the impact of security incidents? Let's take a look. Security incidents may compromise the integrity of the information, and understand if the integrity of the information is compromised we no longer can protect it, thus nullifying all of your safeguarding's. Security incidents increase the cost of resources, money time and programs and equipment, and it also impacts the effectiveness of your DoD programs.

Understand if you have a compromise of integrity of information, nullification of safeguarding, increased cost, reduces the effectiveness of DoD and ultimately, damage to the National Security of a Nation. Which leads us to our next poll question: What is the first step in the process of handling security incidents involving classified information? Do you report it or is your first step is to try and safeguard the information? Okay let's go ahead and look at the numbers. We're looking at about 95 or 96% that says that you should safeguard the information. Understand that if you have the capability of safeguarding that information you should go ahead and do so. First you need to protect the information from further disclosure. Alright, let's look at the six step process.

Like we just talked about, the first step is safeguarding the information; you want to protect that information from further disclosure if you have the means to do so. Then you want to report that information. Try to cover the who, what, when, where, and how. The next thing

you want to do is do a preliminary inquiry. It's actually conducted for an actual potential compromise. The next step would be to conduct an investigation if the preliminary inquiry does not meet your needs. Then you want to take corrective actions. You want to identify weaknesses, enhance security, develop procedures, and educate your personnel. And also you want to impose sanctions if there is a deliberate or negligent compromise. You want to follow this six step process for the most of your security incidents unless you come across information that requires special circumstances. The information that requires special circumstances - your reporting requirements may differ. Now let's talk about the special circumstances, what type of information is that, we're going to talk about that. First let's identify it.

Special Circumstances: Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements as specified in the DoD Manual 5200.01, Volume 3. Let's take a look at that type of information. Here's a list of 12 different types of special circumstances: there are a couple more in the Volume 3, but we're going to talk about these 12, and let's look at our first group. We're going to first go over to Foreign Intelligence Service information Violation of Criminal Law and COMSEC information. Incidents involving deliberate compromise of Foreign Intelligence service or terrorist organization information must immediately be reported to the Cognizant Defense Counter Intelligence component. Security officials shall not initiate or continue an inquiry or investigation of the incident unless it is fully coordinated with the appropriate Defense Counter Intelligence Component.

Apparent Violations of Criminal Law: You need to notify the Defense Criminal Investigative Organization who is in charge of that investigation so you will not jeopardize the integrity of the investigation. Now what is Defense Criminal Investigative Organization depending on your component- let's take a military installation would be the Defense Criminal Investigative Department or CID.

COMSEC or Cryptologic Information: Report security incidents involving COMSEC or Cryptologic information to the National Security Telecommunication and Information Systems Security Instruction or (NSTISSI) 4003, Reporting and Evaluating COMSEC incidents.

Which leads us to our next question, let's review. Choose the statement that best answers this question: Which is true of security incidents that involve deliberate compromise, a foreign intelligence service, or a terrorist organization? A: Security officials will initiate or continue an inquiry or investigation, B: The incident shall be reported immediately to the cognizant Defense Counterintelligence component. Alright, 98% says B and you're absolutely correct, and security officials shall not continue or initiate an inquiry or investigation until that coordination is conducted. Next we're going to talk about SCI information, restricted data, foreign restricted data, or Information technology. Incidents compartmented information.

Report incidents involving SCI information to the activity Special Security Officer or SSO. For incidents involving SCI that become public, for incidence of involving SCI to become public you need to notify the Office of the Under Secretary of Defense for Intelligence. If another intelligence community agency is involved, notify the Office of the National Counterintelligence Executive. Restricted Data or Foreign Restricted Data: Notify the Department of Energy as necessary for incidents involving Restricted Data or Foreign Restricted Data and provide a copy of the notification to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director of Security for OUSD(I). Information Technology: Actual or potential compromises of classified information involving automated Information systems, or computer systems, terminals, or equipment shall be reported in accordance with the DoD Instruction 5200.01, Department of Defense Information Security Program and Part 2001 of title 32, Code of Federal Regulations through appropriate channels by the Information Assurance manager to the Activity Security manager. Even though inquiries into the resolution require coordination with the assistance from the local Information Assurance officials, prompt resolution remains the responsibility of the Activity Security manager. For additional guidance on handling of classified data spills, see Enclosure 7 of the DODM 5200.01, Volume 3.

Let's talk about Foreign Government Information and NATO, Classified Information to Foreign Government, and Special Access Programs Information. Actual or potential compromises involving Foreign Government Information or North Atlantic Treaty Organization information or NATO shall be reported promptly by the DoD component senior agency official to the Under Secretary of Defense for Policy, who serves as the Designated Security Authority. The Director of International Security Programs OUSD(P), shall be responsible on behalf of the Designated Security Authority, for notifying and coordinating with NATO or the foreign government as appropriate.

Classified Information Provided to Foreign Governments: Actual or potential compromises of U.S. classified information held by foreign governments shall be reported to the Originating DoD Component, the Original Classification Authority or OCA, the Director of Security, OUSD(I), and the Director of International Security Programs OUSD(P).

Special Access Programs: Incidents involving Special Access Programs shall be reported by the Department of Defense Component SAP program office to the DoD SAP Central Office and shall report to the Director of Security, OUSD(I).

Next we want to talk about improper transfer, CPI, and On-site contractors: Any activity that receives classified information that has been improperly handled, addressed, packaged, transmitted, or transported shall make a determination as to whether the information has been subjected to compromise. If the activity determines that the classified information has been

subjected to compromise, the receiving activity shall immediately notify the sending activity, which shall be responsible for initiating an inquiry or investigation, as appropriate.

Critical Program Information: Security officials shall inform the program manager of record and the Cognizant Defense Counter Intelligence component of classified Critical Program Information or Critical Program Information related to classified contracts that may have been or was actually compromised.

Next we'll talk about On-Site Contractors: Security incidents, including any inquiries or investigations involving on-site contractors, shall be handled in accordance with paragraph C1.1.9 of DoD 5220.22-R, "Industrial Security Regulation", and paragraph 6-105c of the National Industrial Security Program Operating Manual, host activity security rules and procedures apply.

Which leads us to our next poll question, let's review: True or False, security incidents involving special access programs are considered special circumstances? Alright, everyone has that true, good job! Next question. True or False, The impact of security incidents increases costs and reduces mission effectiveness? Alright, everyone's got that true, it is true.

Which leads us to we want to take a moment and address some of the pre-webinar questions that we received when we put this out and the first question says: Please discuss natural disaster and other emergency response situations. And I want to say that the caller wanted to tie that into security incidents, but the bottom line is in emergency it's about establishing emergency plans. Understand that DoD Policy states that emergency plans shall be developed to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of compromise, and for the recovery of classified information, if necessary. Now understand that the level of detail and the amount of testing and rehearsal of these plans shall be determined by the agency assessing the risk of hostile action, foreign intelligence threats, natural disaster, or terrorist activity that may place the information in jeopardy. So what you have here a DoD policy that states that you have to establish emergency plans and you have to rehearse those emergency plans that up unto a certain point, and some other things you want to consider when you're preparing emergency plans. You want to make sure that you reduce the amount of classified material that's on hand, you want to make sure you store less frequently used classified material at other secure locations, you want to create regular backup copies of information in electronic formats for off-site storage, and you want to transfer as much retained classified information to removable electronic media as possible, thereby reducing your bulk. So if you look at the trend, you want to actually try to eliminate that classified that you have on hand, and or get away from using the paper copy because it's easier to manage.

Now the next question that we have, that we want to address, is going to be a personnel question and we have Mr. Andy Reyes here from CDSE Personnel Security Training Team and Andy is going to actually take that question and address it. Andy welcome! Thank you Danny. The question is: Please provide location of where we can find guidance regarding when incidents will be updated in JPAS? I think the question really leads to where's the guidance we can find as far as what to report. One of the tools that we give our adjudicators when we teach the adjudicators is called an ADR, the adjudicative desk reference, you can go into Google and just Google adjudicative desk reference. PERSEREC did a really nice job of creating the 13 adjudicative guidelines and some examples that will guide you as far as what you should be reporting as far as incidents. Again, we have to lean towards National Security, so those guidelines will give you some good examples and also you can look at the concern disqualifiers and the mitigators and their main concern there as far as reporting would be your concern and disqualifiers. Lately we haven't done a good job as far as reporting incidents so hopefully you can took a look at this guidance and report these incidents, these violations whether they just let the adjudicators make that decision as far as the seriousness of them. But again there's the adjudicative desk reference and you can go in there, again you can get it up online and that's probably your best source. Alright Danny!

Thanks Andy for actually addressing that question for us. And guys in summary you should be able to: Understand the importance of promptly reporting security incidents as we discussed DoD policies states it required and the impact of security incidents have on National Security. We also talked about the compromise of information, the nullification of our safeguards; it increases costs to reduce the effectiveness of DoD and the overall damage to National Security. We also identified the 6 step process from safeguarding to imposing sanctions, and we also defined Special Circumstances and listed examples and policies associated with those examples.

What we liked for you do to now is tell us how we're doing. We want you to take a quick survey as we populate this for you, something new here just trying to set up so we can get that instant feedback from you, and as that populates. Okay, if you don't mind go ahead and fill out the survey for us. Tell us how we're doing and if it's anything else that you actually want to, let us know what we need to be training you on; we actually want you to do that as well. We'll give you a couple of seconds. We like instant feedback and the only way we can actually get that is actually reaching out to you guys and providing you that tool to kind of let us know what we're doing and if we're actually doing it. Alright. At this time we will actually bring it up, okay. Are we okay with it? Alright, let's go ahead and close out here.

Alright guys here's our contact information, Information Resources; if you have any questions about this webinar or any handouts or frequently asked questions about it please visit us at this below link, and if you got any questions about any information security training visit us at

InformationSecurity.Training@dss.mil. This concludes our webinar for today. Thank you for taking time out for joining us. Once again we appreciate you making CDSE as one of your venues of security education training. Well this concludes this webinar.