STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC)
July 25, 2018

TRANSCRIPT

BRADLEY: All right. Again, welcome. Thanks for coming. This is the second one of the 2018 year and the 15th overall. This is a public meeting -- let me get this microphone over here -- subject to the Federal Advisory Committee Act. The minutes of the SLTPS-PAC are available to the public. The meeting is being audio recorded. The microphone around the table -- microphones around the table have enough cord to be repositioned in front of anyone who wants to speak. A floor microphone to my left is for any audience member to use who wants to come up and speak. Anyone who is making a presentation but not sitting at the table can use the podium to give your briefing. Please identify yourself when speaking, so we have an accurate record of your comments. This is critical, because, again, we prepare this manuscript. And it’s very difficult sometimes to try to figure out who was speaking. And so if you just say, “I’m X from Y,” that would be wonderful. And if I interrupt you and remind you, it’s not because I’m rude. It’s because we’re trying to get an accurate transcript for the public. Membership changes. We’ve had quite a few. At the beginning of January we were down three, three vacancies. So I welcomed two new members at that meeting, Tom Woolworth and Mike Steinmetz. Gentlemen, you're on the telephone?

STEINMETZ: Mike Steinmetz is up. And I was actually at the January.

BRADLEY: OK.

F1: Is there anyway to make that louder?

BRADLEY: Yeah. Can we turn up the volume on the --

M1: (Inaudible)

BRADLEY: OK, thank you. Yeah. A third new member joined shortly after January meeting. Let's welcome Tom Carr. Tom is the executive director of the Washington-slash-Baltimore high intensity drug trafficking area program. A bit busy are you?

CARR: Just a bit.

BRADLEY: Yeah, just a bit. Throughout the year, three additional SLTP vacancies opened up. Rich [Lish?] left the Center for Internet Security Multi-State Information Sharing and Analysis Center and was no longer able to serve on the committee. Angus [Kirk?], who was the Washington state chief information security officer, retired. And Mark Schouten, director Homeland Security advisor Iowa, Department of Homeland Security and Emergency Management, also retired. I am pleased to welcome three new SLTPS-PAC members. Marcus Sachs, chief security officer, Pattern Computer. Marc said he would attend the meeting?

M1: Yeah.

BRADLEY: Yeah. Did he?

M1: (Inaudible) No, he’s not.

BRADLEY: All right. Douglas Reynolds, vice president of security operations, Mall of America. Doug?

REYNOLDS: Hi, sir.

BRADLEY: Yeah, welcome. Hans Olson, assistant secretary for Homeland Security state of Massachusetts. He’s on the phone, I think, right?

M1: Should be.

OLSON: Yes, good morning. Thank you.

BRADLEY: OK. Thank you. On the federal side, there was one change. Erik Galow, information sharing lead office of data and information sharing is a new member from the FBI. All right.

M1: Erik’s here.

BRADLEY: Go around the table and introduce ourselves again. I’m Mark Bradley, director of ISOO and the chair of the SLTPS.

CARR: Tom Carr with [WDCP?] and the (inaudible) program.

REYNOLDS: Doug Reynolds, Mall of America.

SACHS: Marc Sachs, Pattern Computer.

GALOW: Erik Galow, FBI.

PEKRUL: Mark Pekrul, National Background Investigations Bureau.

TAYLOR: [Joseph Taylor?], ISOO.

BROUSSARD: Derrick Broussard, DSS.

BAILEY: Marissa Bailey, Nuclear Regulatory Commission.

MASCIANA: Leo Masciana, State Department.

MORGAN: Nancy Morgan, CIA.

ROGERS: Charlie Rogers. I'm with DHS.

PANNONI: And I'm Greg Pannoni, ISOO and the designated federal officer for the meeting.

BRADLEY: All right. We'll start with this gentleman.

SCYPHERS: Hi, Jason Scyphers with DHS.

BRADLEY: Welcome.

MCCLAIN: Alex McClain, also DHS.

F2: **[Mariah Harrod], DHS**.

BUCKLEY: Stephen Buckley, DHS.

F3: **[Kersha Poindexter**, FBI.

JOHNSON: Kim Johnson, DHS.

STEVENS: Paul Stevens, FBI.

MCNEMAR: Tammy McNemar, FBI.

ROBINSON: Michael Robinson, FBI.

MACKEY: Marvin Mackey, Department of Transportation.

M2: Bob Skwirot, ISOO

BRADLEY: OK. Right.

F4: Alegra Woodard, ISOO

BRADLEY: OK. That's it, right? OK, and on the telephone. Who would like to start?

FRIEDLAND: Jeff Friedland, St. Clair County.

STEINMETZ: Mike Steinmetz, state of Rhode Island, state cyber security and Homeland Security.

BENSLEY: Glenn Bensley, Department of Justice.

BRADLEY: Hey, Glenn.

BENSLEY: Hey, how you doing.

BRADLEY: Doing OK.

KERBEN: Valerie Kerben, DNI.

BRADLEY: Hey, Valerie.

M3: [Andrew Dierbergs?], Tennessee Valley Authority.

OLSON: Hans Olson, Commonwealth of Massachusetts.

BRADLEY: Anyone else? Glad to have our friends from the TVA on the line. We just invited them this past week. So thank you for making the meeting. We appreciate that. All right, in our folders here we have copies of the meeting agenda, the slides to the presentations, and minutes of the last meeting. Let me just say briefly -- again, because we have so many new members -- what the purpose of this is. It's always good to be reminded of why we're here. We're here because of an executive order 13549, classified national security information program for state, local, tribal, private sector entities. The point of this is to -- the point of this group is to improve the program through which the federal government shares classified information with SLTPS entities. So this is kind of -- I like to think of it as kind of a troubleshooting meeting for us to raise points, not of contention, but of how we can help this program run better. Because as you know, it’s absolutely critical. Something in the paper, I think, this morning or yesterday again on attempted hacks of local power grids and everything else. I mean, we’re under unprecedented assault from all sorts of bad actors. And so it’s critical that we share our information with each other. It’s also critical that we use this platform as a way, again, to identify whatever the problems are. And so, I would like to see this as a fulsome -- I wouldn’t say the Oxford Union, the debating society, but something close to it, where we are not afraid to speak frankly to one another. Because this is the place it should be done. And then so, again, I -- collegially, obviously, but frankly. And so with that, I think I’ll turn it over to you for old business.

PANNONI: Thank you, Mr. Chair. Did someone just join on the phone? And if you would, please identify yourself if you haven’t already? Thought I heard a beep. I guess not.

And the gentleman over here, could you introduce yourself and your affiliation, please?

PARMELEE: Oh, my name is Edward Parmelee. I'm an FBI special agent.

BRADLEY: Oh, yeah, one of our speakers.

PANNONI: Thank you, and welcome. OK, so we just had one old business item from the last meeting. And just for the new members, non-federal members, we don't have funds available for travel, as you know, those of you who have been coming to the meeting. So that option isn't available for us to fund you. But we do have the teleconference capability. And also, just for administrative purposes, the minutes from the last meeting are in your folders. And they were certified on May 31st, 2018. So now, to get to this old business item, and it is starting to get old, because we first discussed this last year in July. And then we -- this is the issue that some of the SLTPS members voiced concern about the challenges facing verifying security clearances. And as a result, we bought together a working group this past January of the Federal SLTPS-PAC members to look at the multiple, separate, and unconnected security databases in the executive branch and the effect this has on clearance reciprocity in order to identify the steps that can be taken to address any obstacles to reciprocity that may exist because of current clearance database deployment. So a little background. Let me just first say, the attendees at the meeting, I’ll identify them. We had the performance accountability council program management officer. This is a body that is responsible for coordinating all issues dealing with clearances, suitability and credentialing, working under the umbrella of executive agents ODNI for security, access eligibility determinations, and OMB for suitability and credentialing. We also had the National Background Investigations Bureau at the meeting. And we have Mark Pekrul here today from NBIB. We had ODNI, Office of the Director of National Intelligence. We had a representative from OUSDI, Office of the Undersecretary of Defense for Intelligence. ISOO, we were there. And unfortunately, the FBI couldn’t make it. As far as a little bit of the discussion at that time and still somewhat where we are on this, we were discussing access to the system that would allow the SLTPS personnel access to clearance information. And many of you probably in this room know back in 2004 or ’05, the IRTPA, the Intelligence Reform and Terrorism Prevention Act, called for, among many other things, a central verification database for clearances. So that was established. And the idea was, as I understand it, was to latch up a couple of other databases, such as the DoD’s JPAS and the intelligence community’s Scattered Castle system. And other than exceptions for national security reasons, those databases were to feed into the CVS, the Central Verification System, so that we would have a current, timely, centralized, clearance database. So it -- I can’t really say 100 percent for sure the level of effectiveness. But arguably, it’s working. But there are -- occasionally we’ll find gaps where there’s concerns. And this happens to be one of them, where in this particular instance it’s the FBI which is one of the agencies that can clear state, local, tribal, private sector personnel. Their data feeds into Scattered Castles. But unfortunately, that data on the SLTPS folks that are being investigating and obtaining security clearances for whatever reason is not feeding into CVS, as I understand it. So that was in a sense why we wanted to have this meeting with those different agencies that I just mentioned. The issue still exists as I understand it. So I’m going to now ask Mark Pekrul -- and we have Erik Galow from FBI. And then I’ll ask ODI -- I believe Valerie Kerben is on the phone -- to give us a little update as to where things stand at this time. So either one of you gentleman can go ahead please.

PEKRUL: I’ll go first. And for the accuracy of the minutes, the suitability and credentialing executive agent is the director of OPM and not OMB.

PANNONI: Oh, did I say OMB?

PEKRUL: Yeah, it happens.

PANNONI: I apologize. That was a Freudian slip. I know it’s OPM.

PEKRUL: OK. No, you did a great job teeing it up. And that is -- and I was at the meeting in January, I guess it was. And the problem that was identified is that so many of the individuals in the SLTPS community who do hold clearances hold them through the bureau. And it isn’t just a matter of the SLTPS community having access. It’s their federal sponsors. So if a state employee with a clearance from the bureau wants to then work or gain access to classified information at DHS or at Department of Energy or wherever, that agency then sets about to verify that clearance. They’re not -- the clearance is not loaded into CVS or JPAS, which are the two databases agencies have most ready access to, let’s say. Most agencies can, with varying degrees of effort, get into Scattered Castles. But Scattered Castles -- and Greg, you mentioned there’s an effort underway to find a way to load the information that’s in Scattered Castles to the low side databases and that. I don’t -- maybe DNI has more information. But to -- that has long been a problem across the entire mission spaces, how to get those from the high side database into the low side. So the bottom line problem, which, again, I think you teed up perfectly, is we’ve got a lot of these individuals cleared by the bureau. The bureau loads their clearance information in Scattered Castles, which not all agencies have, or know they have, or can access Scattered Castles. The databases they use every day -- CVS primarily, but also JPAS -- does not contain that information. So that I think summarizes the issue that we discovered in January.

PANNONI: Thank you, Mark. Erik, can you add to the discussion?

GALOW: Not as substantively as I would prefer. I can say that my boss, the chief data officer of the FBI, and her boss, the chief information officer, are aware of the issue and that it has been escalated to the higher up echelons of our national security apparatus. So my understanding is that there is a subcommittee at the NSC level that was looking into this issue as well and so far as that consolidation effort pulling everything into CVS, but that nothing had been set in stone as of yet. I wish that I’d been at the meeting back in January so that I could have better engaged with our security folks.

STEINMETZ: Mike Steinmetz. Whoever is speaking right now, the microphone is cutting in and out, and we're only catching about 50 percent of what you're saying.

GALOW: Would you like me to repeat it?

BRADLEY: Please, do you mind?

GALOW: So the long and short of it is that there's a National Security Council subcommittee that has been looking into the issue, and that my senior leadership on the (inaudible) [CIOCDO?] side is aware of it. I'm not aware of any specific measures that our security division has taken to independently push FBI-vetted individual data from Scattered Castles to CVS or to JPAS for that matter. But I'd be very happy to look into that a little bit deeper prior to the next meeting, if that will suffice.

PANNONI: Yeah, I appreciate it. And if there's some temporary workaround -- because it might take some time for this National Security subcommittee to sort things out and come up with a workable solution, maybe we can try to think creatively.

BRADLEY: (Inaudible), yeah.

REYNOLDS: New guy, but -- Doug Reynolds. It's interesting. This speaks right to me. I'm a private sector guy with an FBI-sponsored clearance. And for 12 years, I've been coming to DC. And for 12 years, agencies have not been able to find my clearance. If I would have just known, hey, here’s where you can look for it, just that bit of information that I just got in the last five minutes would have saved a lot of [heartache?].

PANNONI: Scattered Castles.

REYNOLDS: Scattered Castles. Is there a way to get that information to the people with the clearances so that they can cue up the person looking for their information? Or --

PANNONI: I think as Mark Pekrul said, some agencies -- I don’t know that every single agency had -- for example, this agency, National Archives, does not have ready access to Scattered Castles, unfortunately.

PEKRUL: It varies by agency and their national security mission, or lack thereof.

PANNONI: Right, so it’s --

PEKRUL: But now, alternate --

MORGAN: You have to have -- sorry, Nancy Morgan. You have to have access to a top secret network to get access to Scattered Castles. That’s the challenge right now.

PEKRUL: Alternately, and I don’t know the answer to this -- and a lot of times what happens is the agency may not know it’s in Scattered Castles. But alternately what happens is -- and forgive me, I just lost my train of thought. There we go. That’s embarrassing.

BRADLEY: (Inaudible)

PEKRUL: What’s that?

BRADLEY: You were talking about Scattered Castles and about --

PEKRUL: Yeah, I know, I know. I’m sorry.

BRADLEY: That’s OK.

PEKRUL: So yeah, agencies may not know it’s in Scattered Castles. Some agencies don’t have access to Scattered Castles. I know that for example my old employer Department of Energy loads to both Scattered Castles and CVS. So there’s the possibility there to bifurcate your clearance load. At least some agencies do that. And I would also imagine -- now I remember what I was going to say. There must be a way for agencies to -- absent the automated route of a database check -- to contact the bureau. Or there must be -- and I’m not aware of what it is -- a number to call, a website to visit where absent access to the database, they can also get this information. Not as good as an automated database, but certainly something that can be done relatively quickly, I think.

PANNONI: As we’re talking, let me just throw this out. The chair said to speak frankly. And I’m not suggesting we add more to DHS’s workload. But DHS is the executive agent for this program. DHS has access to Scattered Castles. Am I correct so far?

ROGERS: So far. But you may not be able to keep going.

(Laughter)

PANNONI: Is there a role, temporarily, that DHS could sort of be the default, so to speak, when there’s this blockage where there’s an inability to gain access to the investigative data that resides in Scattered Castles?

ROGERS: Well, without being too blunt, it’s not a DHS problem. I want to make that clear.

PANNONI: I understand.

ROGERS: CVS -- and I was going to talk a little bit about CVS -- CVS was also designed for state and locals to use. So they don’t have access to top secret networks. So fusion centers can get to CVS though what I’ll talk about later. But if the clearances aren’t there, they can’t validate them. But even with us, our office of security and the personnel security division, reaches back to the FBI to verify state and local clearances. We haven’t been going to Scattered Castles. They’ve been going back to FBI. And that can be a time consuming -- I mean, if someone says, “Hey, I’ve got four people who want to go to a meeting tomorrow at a fusion center, can you verify whether they have a secret clearance or not, or at least a secret clearance,” then sometimes it could take three or four days or (inaudible) right person [to get it back?]. We have

Scattered Castles, but it’s not -- the access isn’t centralized. It’s typically with SSOs are usually (inaudible). And they’re dispersed throughout DHS. So I mean, I could go back and ask. But I -- we don’t have a central place with people sitting there readily available to verify clearances nationwide through Scattered Castles any more than any other agency.

PANNONI: Right. I was just thinking in the role as the executive agent. But let me ask, Valerie Kerben is on the phone, if you don’t mind, Mr. Chair?

BRADLEY: No, by no means, no.

PANNONI: ODNI, you’re the executive agent for the access eligibility determinations. Is there anything you can add to this discussion, please?

KERBEN: I was checking also with the Scattered Castles group to see if there’s been any movement on FBI loading the information. I mean, of us. But the point is here is, as -- I think it was Charlie, who said -- is the information is not at the -- they don’t have access to the higher level system, the top secret system of Scattered Castles. And because it’s a high side, we’re not moving information down to the low side. So I mean, I still think that there is the disconnect of the FBI loading information to other databases where it can be viewed by the state and locals.

So it’s not only because it’s in Scattered Castles, but I think it has to be loaded on other systems as well. And there maybe is a mechanism to feed it to the other databases. I thought FBI does load some clearance information to CVS. Isn’t that right, Mark Pekrul?

PEKRUL: No, last information I had when I checked this out in January was that the FBI does not. And in fact, our attempts to get the FBI -- not you -- but to get the FBI to load information in CVS goes back to the debut of CVS back in ’04, ’05, ’06. And I’m not saying we contact them every day to try. And sometimes many months pass. But it’s just -- it’s been an issue for us. I’m not sure how hard it’s being pursued right now, because of inability to do it for whatever reason in the past.

ROGERS: I was going to talk about (inaudible). The executive order did direct DHS to work with OPM, ODNI, and DoD to create a central repository for all state and local clearances. And it was -- we worked through this committee, and it was -- CVS was identified. And I was going to talk to this later. It was an accomplishment. We got -- OPM was key in modifying CVS and created a users’ role for state and local security liaisons. And they also -- I don’t know the right IT verbiage. But they created a bridge to JPAS. And so it enabled state and locals to go in. But it was all dependent upon all federal agencies using CVS as the portal. And at the federal side, you can go in and do a lot of things with CVS. The state and locals were limited to only being able to go in and verify a secret level clearance, because fusion centers and other state and local facilities can only host classified access --

PANNONI: Excuse me, Charlie. Pull the microphone closer to you.

ROGERS: -- can only host classified access at the secret level. So the decision was made through the committee that -- and the FBI was on that committee, too -- that there would be a limitation on what the state and locals could see, but they could certainly see what they needed to to either verify people to come to a meeting that they might be hosting in a fusion center. But it was all dependent upon CVS -- all this work was dependent upon CVS holding the clearances.

PANNONI: Well, if it's something we can bring up with the committee, the --

BRADLEY: [Race?]?

PANNONI: The race committee, too. Information access.

BRADLEY: (Inaudible) [put this back?]. Yeah, we need to get this moving. I mean, it's no good if we can't attend meetings and we can’t share. I mean, that’s the whole point of the process. If we’re choked off, it just -- it’s not helpful. So let’s see whether we can -- we can raise this with the National Security Council and with Fitzpatrick and try to get some movement.

GALOW: This is Erik Galow, again, from FBI. I’ll get together with my security division colleagues in the immediate aftermath of this meeting to try to formulate a plan moving forward, at least in the short term.

BRADLEY: Yeah, we’d appreciate it. Again, it’s critical that we get this information out. Anyone else have a comment on this?

PANNONI: I think that’s the only action item (inaudible).

BRADLEY: All right. We’re going to turn to Charlie Rogers, DHS vice chair, who’ll provide an overview update on DHS SLTPS security program. Charlie, take it away.

ROGERS: OK. So I’m Charlie Rogers with DHS. I was asked to kind of give a broader overview -- in the past I’ve given broader overviews. But over time, I was reduced to giving just sort of simple metrics. But because the committee has turned over, a lot of new members. I’m going to kind of give a longer presentation of various elements. Some of it is kind of my interpretation. So if anyone wants to tell me I’m off track or something. Because I was going to start with talking a little bit about the executive order. And not that I wrote it. But I was here in the early days. And after 9/11, of course, there was a big push to share information with state and locals, to get classified connectivity to state and locals. In 2003, DHS stood up. A big part of DHS's mission -- and we're not the only federal agency with a state and local mission. But a big part of DHS's mission was dealing with state and local, private sector. And so around the years leading up to the executive order, there were several instances of friction with state and local, private sector gaining clearances or getting different kind of guidance on how to protect classified. And the end result was in 2010 -- it was 2010 -- the executive order 13549, the Classified National Security Information Program for State, Local, Tribal, Private Sector Entities, was signed. And the purpose was -- or the short purpose was, one, to ensure that state and locals, private sector were appropriately protecting classified information in accordance with existing and future executive orders. It wasn't to change the standards, but to reach within the federal government and to take the existing national standards and impose those on the state and local, and bring them part of the community. The other part was to facilitate classified information sharing. I mean, the order doesn’t really deal with information sharing. But it tries to crate an environment in which classified information sharing can occur. So that’s how we got here with the order. And I was just going to go through some of the main elements that came out of the order. The order directed DHS to establish an implementing directive which would explicate in more detail kind of the processes by which clearances are issued or how we safeguard. Its big focus was fusion centers, because they actually store classified at their location. But there’s elements with private sector and other operational activities with the state and local. The executive order defined at the operating level, the basic operating level with state and local would be secret, which does not mean they can’t get top secret or top secret clearances with special accesses. They can. But that at the baseline operating level, it would be secret clearances. And that was stated. And then on a case by case basis, clearances can be elevated to a higher level as needed. It also codified that the governors -- I mean, there have been different DoJ, I think, memorandums and governors about governors being allowed to have classified access. But the executive order would -- it was placed in the executive order that a governor can get classified access without a background investigation. The only obligation the governor has is to sign a non-disclosure agreement. They're basically approved by the American people, you could say, for classified access. It also reaffirmed what's been in other executive orders, that clearances would be reciprocally accepted by all federal agencies, unless there were waivers or things of that nature. And the same went for physical certification and accreditations of rooms. They would be reciprocally accepted unless there was a waiver involved in that certification of the room. It defined that the physical custody of classified information that would be totally the responsibility of state and local would be at the secret level. So state fusion centers and possibly metropolitan police departments that might have classified are only authorized at the secret level unless their -- the facility has a full time permanent federal management of that. So we do have a couple of state and local in New York City and Chicago that have [skiffs?] that are TSSCI facilities. But they also have full time DHS SSOs who are deployed there. And they work there. But in the absence of that, the location would be at the secret level. The executive order called out for inspections to take place. And I'll talk a little bit about that. And audits or reviews of those locations that are storing classified. It reaffirmed the National Industrial Securities Program governance over the private sector, and the private sector contracting, and the safeguarding of classified associated with that. It established this committee, was established by the executive order, and defined that. And I actually had in my notes that it called out for the establishment of a clearance database. And I won’t go into a lot of detail, but we did have working groups with OPM, DoD, ODNI. The FBI was part of it. It was decided that OPM would be the appropriate government activity. They had CVS, that that would be the repository. And work was done to create a user role for state and locals to verify clearances. There was -- and I don’t know how technically difficult it was. But it was -- DoD was brought in to build that bridge to JPAS. And I think that was a challenge. And that was taken care of. And that was implemented in 2014, I think, that it went into the pilot, and then it got implemented. So that’s the broad overview of the executive order or the provisions of it. It’s only about six pages long, something like that. There’s a lot of implications in it. And the other part I was going to talk about is state and local, tribal, private sector, what I call classified engagement. And I can only really talk to what DHS does. But we’ve got -- and I’ll talk a little bit more about state fusion centers. And I'm not the expert on state fusion centers. But we have approximately 80 state fusion centers, of which about 55 are primary fusion centers. We've got HSDN, and I think about 56 -- the number may not be exact -- HSDN, which is the Homeland Secure Data Network. It's a secret level network. So that's a pretty big deal in those fusion centers. It's a very large classified footprint. Every location that has HSDN or is given the opportunity to have [STEES?] and is also -- I think there's a -- part of the requirement is that they deploy an intelligence officer. I think for the most part they're INA intelligence officers. But there could be CBP intelligence officers. I think it varies from location. But there needs to be a federal intelligence officer wherever HSD is deployed -- HSDN is deployed. So that's a very big part of the classified engagement that DHS is involved in. And by no means does DHS own the fusion centers. They're state entities. And they have multiple relationships. They have a major relationship with the FBI. A lot of times JTTFs are co-located or nearly -- nearby-located with them. So it's -- depending on where they're located, near the great lakes, near the borders, there are different federal agencies that are involved. If they're near a port, near the sea, they may have Coast Guard and other entities involved. So that’s one piece of the classified engagement, that this executive order facilitates. Within DHS, the National Protection Programs Directorate is responsible for currently 16 critical infrastructures. They’re not totally responsible. There are other federal agencies, Department of Energy and others, that have -- that are the sector agency for some of these sectors. But DHS is involved in these. I don’t really want to read them all, but you can imagine chemical communications, transportation, energy --

PANNONI: Financial banking, right.

ROGERS: Yeah, financial banking, health care. So there’s a whole series of those. Those DHS -- these are private sector entities. They don’t store classified information unless they were to go through the National Industrial Security Program. But we do have the authority to clear subject matter experts to assist in protecting the homeland. So there are a number of folks in these sectors who either sit on committees or have clearances and access classifieds in the fusion centers or through visiting federal facilities to help the federal community be informed about risk and to validate risk and those kind of things. Recently, there’s a subsector was stood up, the election infrastructure subsector. And so we all know about what’s going on with the election. So DHS is in the process -- there’s a program office in DHS in the process of clearing between two and four -- or more -- state and local folks in the states and territories to facilitate classified information sharing for the purpose of protecting the election subsector, the IT systems to share those kind of threats. So I’m not personally engaged in the operational stuff. The office of security is engaged in getting these clearances done and trying to expedite these clearances. Moving on about the other aspects of the classified engagement. These councils have sector coordinating councils, which are primarily the state -- or the private sector councils that they sit on. But then they interact with the federal agencies, the sector-specific agencies and government coordinating councils. So we’re clearing a number of people. And they are coming in a routine way back to DHS to get classified briefings on different issues and threats that are relevant to them. DHS has a National Cyber security Communications Integration Center, the NCCIC, which is a 24-hour operation. And it has federal representation in it. But it also has significant private sector representation. There are major private sector companies that we clear people at the TSSCI level. And they’re either detail, they’re full time, or more likely, they come once a week. And they’re engaged in helping DHS evaluate some of these cyber threats and to understand and take that knowledge back to their companies to help build the protective measures they need. DHS has a protective security advisors program, which is different than the fusion centers and that side of NPPD. These PSAs, they’re called, are in -- I’m going to read this. They’re in 73 districts. They’re in all 50 states and territories. They’re deployed. They do work in fusion centers sometimes, or they come to fusion centers once a week. And they’re out there to work with dam owners, energy. I guess the Mall of America. They -- I don’t know if they work with you all or not.

REYNOLDS: They do, very much.

ROGERS: Yeah. And they also nominate people for clearances that they believe would facilitate the conversation necessary to protect the national infrastructure. So these guys conduct surveys. And I think they provide training, and they probably do a lot of other things I don’t know they do. But I’m just trying to give a broad overview of some of the classified engagement that DHS has. And by no means -- I just can’t speak to what the FBI does and other agencies. But I’m sure that there are plenty of other activities going on where there are classified engagement by other federal agencies that have a need to share classified. So I was going to shift gears a little bit and talk about the state, local, tribal -- if I’m going too fast, or if you have any questions, just ask me. But the state, local, tribal security compliance review program -- I’ve talked about this before when we first stood it up and how we went about it. The program is really focused on fusion centers or those locations that have a major classified holdings. We’ve started the program in late 2012. The purpose is to go out and visit. Primarily we visit fusion centers. And the priority focuses are on those centers that have HSDN, because that’s the largest classified footprint. But not exclusively. There are other fusion centers that don’t have HSDN. We go out and we evaluate how they’re storing classified, how they’re managing classified, how they’re managing the secure room. Look at their training records. We develop administrative and physical security checklists, just like we would for a federal agency, but focused on what they’re authorized to do and at the level of classified. Some of them have contractors that work for the state. They come through DHS to get the 254. So we would evaluate their contracting records, look at the personnel security records they have, review classified documents, and interview folks. So we’ve been doing that since 2012. This year we -- we’re a little behind. We’ve done seven SCRs this year. I think I told you we were understaffed. But we’ve got nine more to do in the next couple months, so we’ll do a total of 16 SCRs this year. We’ve done a total of -- by the end of this year, we expect to have done 91 total since 2012. And actually, I think -- we don’t have a lot of findings anymore. Because people expect us to come, and they know. But it’s good, because there is a turnover in personnel at the fusion centers. And it helps us to update training. We don’t just go out and do the compliance review. We go out and we give training, and we try to solve problems that are identified.

PANNONI: On the training, don’t you do sort of an annual event for training (overlapping dialogue; inaudible)

ROGERS: Well, there was a -- it was like a -- every two years -- INA sponsored it. We haven’t had one for a while. But, yeah, so -- but we also -- I’ll get into the -- a little bit into the training. So in order to manage the classified at the fusion centers, they established security liaisons. And that was written into the implementing directive, that any fusion center that has classified storage has to have an appointed security liaison. So these individuals have to have a security clearance. They have to be trained within 60 days. They’re responsible for managing the secure room and the classified. There was a two-year program that INA sponsored that we brought folks into a different location. One was in Oklahoma. One was in -- I think San Antonio. And one was in New Mexico. And brought a whole bunch -- they funded to bring in a whole bunch of people in. In the absence of that, we’re conducting webinars. Last year, we did seven webinars and trained 49 security liaisons. This year we’ve done 19 webinars and trained 33 folks. We also, when we go out for an SCR, we’ve been trying to add an extra day to the security compliance review and actually have -- sit down with the security liaison. There is a certain amount of turnover. We have fusion centers that we’ve had people there five, six, seven years. They’re security liaisons. They’re probably going to retire from the locations. And then we have other fusion centers where it’s a -- another duty is assigned, and as soon as a new guy comes in, somebody tries to hand off this job to somebody else. So we’re always trying to cycle the training and catch up with people, make sure they’re trained. And then the last little metric I was going to give, which kind of supports all these other activities, is that DHS currently has 1,900 cleared private sector people nationwide that we’ve cleared. And we have 6,000 state and local personnel that we’ve cleared, which is almost -- like, 79 or something, 79 and some change. But we’re basically at 8,000 cleared people. Almost all of those are at the secret level. There are 320 of those 8,000 that have TSSCI. And some of that has to do with people who may be deployed or working with JTTF. Some of it has to do with folks that are detailed to INA or other locations. And then it has to do with private sector folks that are engaged in cyber security, because it’s basically the baseline level for these folks to get appropriate threat information in the cyber realm is at the TSSCI level. Now, they don’t access it at their facilities. They access it at federal skiffs, and not exclusively DHS. But it’s not a big number, 320. There’s no limit on the number. The mission really has informed the number. But we see that number going up with cyber initiatives with the private sector.

PANNONI: But there are more, because then we have FBI sponsored (inaudible).

ROGERS: Oh, yeah. This is just DHS numbers.

PANNONI: Right, just DHS.

ROGERS: Yeah, FBI does a lot of TS clearances with state and local.

BRADLEY: Very good. This is Mark Bradley, the chair. Let me just ask kind of an existential question, if I can. The order now is how old, Charlie?

ROGERS: Two thousand -- eight years.

BRADLEY: Eight years. Looking back, is there anything that we missed? Anything that we could fix? Anything that needs to be improved? Like you said, it’s six pages. Again, the Constitution is not a big document either, and you can read a lot into it. But I mean, looking at this program now, we have a new administration. Are there any gaps? Are there any things that we need to concentrate on? Because the reason I ask is, we are looking at amending 13526, as Nancy knows, and some of our other authorities. So as long as we’re here, can you all think of anything? I mean, if you were to give this program a grade, what would it be? It sounds, Charlie, that you all have done some very impressive work. And --

ROGERS: Yeah, I mean, we’re not the only -- we have the executive --

BRADLEY: Yeah, no. And our friends down the table here. But I mean, should we be looking at something to tighten the program, or expand it, or fix it, or -- fix it’s a broad word. But you know what I’m trying to say. Can we improve it in any way? It’s an open question. And that goes to the people on the phone, too. I mean, please.

ROGERS: And we probably should distribute the EO to the members so that they can review it. I mean, it’s available online.

BRADLEY: Please, yeah.

SACHS: Marc Sachs. Private sector, but have been in the government way too long. So let me speak from the private sector side. Getting a clearance or figuring out the process is hard for a private sector person. If you’ve been in government, you know how it works, because you’ve pretty much done it since day one. It would be helpful if both the bureau and DHS had some sort of concierge service, so if a private sector official needs to be cleared, needs to find out the status of their clearance, find their SSO, an 800 number they could call, a website they could go to. Just something where -- and a breathing human on the other end will talk to them. Just a single point where they could start and talk. I think that would be a huge improvement. Because right now it -- they sort of fly blind. If I’m a critical infrastructure owner-operator, I don’t really know what to do, how to start this process.

REYNOLDS: You know, to echo that -- Doug Reynolds. So my clearance has been in the process of being upgraded through

DHS to TSSCI for over a year. And I get that it takes time. But I'll get calls from a -- and I'll miss the call. And I'll go to call back about the status of my clearance. And you call back, and it's a switchboard that doesn't want you to call them. And that's very clear. Because you're like, "Hey, I'm calling back." "Yeah, somebody will get a hold of you." And it's like, well, there was no message left. And I understand it's about my clearance. "Somebody will get a hold of you." And then they don't. And it's -- you're kind of in a limbo state. You just don't know where you're at. You're right, there's no --

SACHS: And I know DHS is trying to hire thousands of cyber officials. But if you could hire three people who could just answer the phone and talk to the private sector about security clearance. Because that would just solve so many problems.

REYNOLDS: And it actually has a trickle effect. Because now my FBI clearance is past due to renew, but they don't want to do it, because they know I'm about to get a TSSCI. And they're like, "Well, we'll just wait." And so they're like, "Hey, you told us three months ago that you're about to get this based on an email you got. What's the status on it?" I'm like, "You tell me." So it is challenging.

PANNONI: I don’t know. Could you also leverage -- maybe you’re doing this -- but your website presence more and provide more detailed specifications about the process of (inaudible) clearance?

ROGERS: Yeah, I would have to talk to -- yeah, the process. Now, one thing in DHS that’s probably not apparent to people is that I&A is primarily -- intelligence and analysis is primarily the people who validate the clearance requirements for state and local. And we lean to the National Protection Programs directorate for private sector. So they both have nominating activities. So you’re -- now, checking on the status of a clearance and all that, and us informing you of the process is something that the office of security ought to be responsible for. But we don’t necessarily validate -- if someone calls up and says, “Hey, I’m with such-and-such company. I want a clearance.” We -- and it’s not really -- and I don’t want to sound blunt -- but it’s not what -- because there’s a million private sector folks. So a lot of people will say, “We’d like to have a security -- I’d like to have a security clearance.” You know, so-and-so has a security clearance. But it’s really based on, well, what is your relationship with DHS, or the FBI, or the Department of Energy. And if a lot of -- if you don’t have a relationship, it’s pretty hard to make too much inroads. Because the office of security is not going to clear you. And we’re going to go to somebody and say, “Are these people directly associated with your classified information sharing initiatives?” And so there -- that’s a roadblock in general for anybody. It’s a roadblock for federal employees. You know, federal employees --

PANNONI: There has to be some sort of sponsorship, I think is what you’re basically saying.

ROGERS: Yeah, there has to be a relationship. And there has to be a mission connection. Because even federal employees who say, “I’d like to have a clearance,” it’s like, well --

SACHS: I think we know that. We’re just talking about somebody who is at a critical infra-- a gas plan, a whatever, who’s been told, “Hey, you need to be cleared.” OK, what do I do? And then let’s say that person holds a clearance, but they need to go to a meeting. They have no idea how to pass the clearance. Just a number they could call where somebody could say, “OK, here’s what you need to do, Bob. Do this, this, this, and this.” And it just will make it a little easier for those outside of --

ROGERS: OK. Yeah, I’m not disputing it. Yeah, so we’ll have to figure out what that looks like.

BRADLEY: It’s a good suggestion.

MASCIANA: Well, I have a different --

BRADLEY: You're from state.

MASCIANA: A different [comment?].

PANNONI: Identify yourself, Leo, please.

MASCIANA: Leo Masciana. It's about the classified information that's being shared itself and the appropriate levels of it. I look at two authorities, this one and the IRTPA 2005 section 1016, information sharing, where it called on agencies to, under the DNI, to look at tear lines, downgrading, declassification, right to release. I don't know to what extent that's being practiced actively. But lately in the press we're seeing quite a bit of conversation about whether classification, particularly classification level, has become a barrier to what is now a priority to deter bad actors in cyber attacks. So I think that's an area appropriate for this group to be considering, maybe not for an amendment of the executive order, but in terms of its current authority, as to whether that's also one of the gaps along with access to meetings and access to information (inaudible).

BRADLEY: Right, excellent point. Yeah, very, very good. I mean, yeah, we may already have the authority. I mean, the key is, are we evolving with the threats? That's all. And again, when an order gets some age on it, it's time to look at it and make sure it’s still doing what we thought it was going to do.

MASCIANA: I’m going to add one other thing. Possibly because of the expertise in this organization, to be considering what classification guides are available, if they’re transparent, if they’re coherent across the key agencies. And maybe even a possibility of looking into a government-wide classification (inaudible).

BRADLEY: Yeah. Nancy, that sounds familiar, doesn’t it? Yeah, we’ve been working on that. It’s another challenge. But we are.

PEKRUL: Mark Pekrul from NBIB. Hearing the talk about being able to find out information on the clearance process, I’ll offer this up. NBIB has a website. And just a month or so ago, we opened a new page on the website specifically aimed at cleared industry, the FSO population. So to -- for whatever that information may get you, and it’s primarily about the investigation process, what to expect, how to fill out forms, that whole thing. We do, of course, state there that if you’ve got specific questions about the status of your own investigation, you need to go to the agency that has put you in for this, because we don’t do that. But it’s NBIB.opm.gov. It’s a public facing website. I don’t know if that’ll be a lot of help to the folks in these sectors. But if it can provide anything, certainly I'd commend it to you. Go look around and see if there's anything there. Again, it's focused primarily at federal people, and industry, and individuals that are going background investigations. It's meant as a clearinghouse of information that's available other places online. So take a look at it and let me know. OK.

BRADLEY: Of course, with the [DSS shift?], too. It's going to be a whole different problem.

PANNONI: Yeah, I don't -- Mark is mentioning -- the chair is mentioning that the shift toward investigations being conducted by DSS. And I don't know how that weights on this or not.

PEKRUL: Well, I assume most people in the room are familiar with the fact that within -- no one knows. Within 12 to 18 months, NBIB in its entirety, its mission, its resources, its people, everything else is scheduled to be, for lack of a better phrase, lifted and shifted from the Office of Personnel Management to Department of Defense Defense Security Service. So the people that are conducting the investigations today will be the people conducting investigations tomorrow, whenever tomorrow comes. And there will still be a web presence. There [will be websites?]. So everything is going to go. It’s just a question of when it happens. So that is going on.

BRADLEY: Stay tuned.

PEKRUL: We all are.

BRADLEY: You all are. Yeah, I bet. Anything else on this good discussion? All right. We’re going to turn to our next speaker. It’ll be Edward M. Parmelee, supervisory special agent, mission critical engagement unit, cyber division, Federal Bureau of Investigation. He will provide a update overview [splash?] on the FBI’s information steering mechanism and best cyber practices. And whatever’s easier for you --

PANNONI: If you prefer to sit, you can sit up front.

BRADLEY: You can sit. You can sit up front. There’s a mic. We have a -- where’s the podium?

PANNONI: There is no podium. You want to sit up front?

BRADLEY: Whatever you -- you like this chair? (Inaudible) chair.

PARMELEE: I’ll stand back here. It might be easier. (Inaudible)

F5: We’re going to test the lights.

PARMELEE: While he’s loading the presentation, I’ll just go ahead and introduce myself again. Again, My name is Edward Parmalee. I’m a supervisory special agent with the FBI cyber division. I sit out in Chantilly. I am currently assigned to the mission critical engagement unit. That’s just a cool, fancy government way to say I do a lot of outreach. My main focus is the transportation and the chemical industry. My unit as a whole has several supervisory special agents and management and program analysts that reach out into not only USG agencies but also private sector. Our main focus is the private sector. And what we’re designed to do is to push and pull intel, basically. We push intel to private sector and other government agencies in exchange for also pulling intel from them and feeding it back to our operational units. Of course, that in theory is designed to help stop, thwart, dismantle any sort of cyber threats that are inbound to the US. This slide today is a very high level overview of what sort of resources the FBI has and what’s available to you. Your primary mechanism is probably going to be through your local field office. I would encourage you to develop a relationship with your local field office. If you don’t have one or you’re having problems doing that, my information is at the end of the slide here. You’re welcome to call me or email me, and I can help facilitate a handshake. Do you have a clicker, or do you want me to just tell you next slide? Oh. (Inaudible) There it is.

Sharing is caring. It’s not always the easiest thing in the world, as you guys have all discussed. But that’s what we primarily like to do with private sector. The FBI really, truly is trying -- I know in particular our cyber division is trying very heavily to be as transparent as possible, as transparent as our policy -- which can be cumbersome -- and as the law allows. Our strategy is pretty simple. The world is not as big as we all think. Everything is interconnected. We want to put bad people in jail. We want to stop people from being victimized, and we want to stop the constant and ever-pervasive attacks against the national security of the United States. That is our main focus. We want to work with our private sector partners and our government agency partners to help develop and stop -- help develop best practices and help stop attacks against the US and its equities. Here are some of the roles and responsibilities to give you an overview. DHS, the protection of the US government networking infrastructure, prevention and mitigation in the recover of that data in the event it is compromised. DHS can probably speak a lot better to what they have as far as private sector resources available. I know there’s some mitigation assistance they can provide if you reach out for them and ask for it. If you are ever compromised, and you’ve lost a tremendous amount of data or your system has been disrupted to the point where it’s just inoperable, there’s probably -- I assume so -- DHS -- do you know anything about those? Or do you want to comment any?

ROGERS: I don’t know in great detail. I know that they do have initiatives with the private sector. And they can go out and (inaudible). I would also say it’s probably a program under development. But that might be future guest speaker or something.

BRADLEY: Yeah, excellent idea.

ROGERS: That could -- but yeah, they do have initiatives with private sector.

PARMELEE: As you see, DHS -- or DoD and NSA oversees theater of combat. You have the defense against their own network and the prevention of attacks towards their network -- excuse me -- and gathering overseas intelligence and feeding back to the intelligence community as a whole. Then you see at the bottom there, DoJ and FBI, we detect, investigate, and attribute, and disrupt cyber attacks and the cyber threats. The [PPT 41?], as you can see, the FBI has been designated the lead federal agency for investigating cyber threats and crimes. We work heavily with our government partners in doing so. Without them, we couldn’t do our job. Here are some resources that would be very beneficial to other

[USG?] agencies in addition to my state and local partners here today and those of you on the phone. Again, you can contact some of these entities through your local field office, or you're welcome to call me and email me, and I can help facilitate a handshake. But I can tell you, the normal course of business is that you would reach out to your local field offices if you have a need for some of these resources. Your local cyber crime task force would help facilitate a lot of the resources. They would utilize these resources to assist you in whatever capacity is needed. The NCIJTF is in Chantilly. It's the National Cyber Investigative Joint Task Force. It's a partner with 24 -- well, there's more than 24 federal agencies there now. DoD, DHS, NSA, et cetera. All there to share and collect information amongst each other and help thwart the cyber threats and attacks against the US and its infrastructures. But National Cyber Forensics, Training Alliance, the NCFTA, that is a non-profit group that is comprised of government, private sector, and academia that collects information and helps stop emerging cyber threats. They do so by open source information and through analysis and research and collaboration with not only the private sector, appropriate private sector partners, but also the US government and academia. It's quite effective, and it's a good -- it’s a good fusion unit. Up on the upper right, you have the Cyber Behavioral Analysis Center. That’s through our Critical Incident Response Group, or CIRG. This is the cyber element of the behavioral analysis unit. Everybody seen the TV show *Criminal Minds*? Or heard of it? OK, so they are one of several units inside the behavioral analysis unit. And their main responsibility is to focus in on cyber actors. Not only to build their profile, the psychological profile of a cyber actor, but also develop -- help assist with investigations and developing technical support to those investigations. How and why an actor does what they do. How and why a group of actors do what they do. And how we as the US government, specifically the FBI field offices and-or support elements in our headquarters division, utilize them for resources and for consultation to streamline the investigative and dismantling process against them. Does that make sense? And the cyber action team is a team of extremely experienced and very technical FBI employees that go -- they travel to a major incident, whatever that major incident may be. And whoever deems it a major incident -- but they would travel to that site, and they would assist with the investigating and mitigating of the attack against the system or a network. Actually, one recent example I can think of off the top of my head is the

[Sony?] incident that occurred a couple years ago. Cyber action team was onsite within hours of notification. CyWatch, it’s a 24-7 operation center. It’s in the same ballpark as the NCCIC. It’s a fusion center where they ingest information and complaints from, not only the public, but also through other government agencies and some FBI field offices. And they ingest the information in the event that there’s an event, or an attack, or someone wants just to make a complaint that, hey, my system was compromised, X, Y, Z style, and this is the fallout. They ingest that information, do some analytical reviews and products. And then they push that out to the appropriate field office for a follow up. Cyber Task Forces, as I mentioned earlier. They’re in every field office in the US. There’s actually 57, because one office is big enough to have two. But that’s comprised of the state, local, and tribal partners as well, and other government agencies. And it’s just designed to share information bilaterally across the state, local, and federal level as seamless as possible. All the non-FBI agent personnel that are assigned to the task force as investigators are cross-deputized as US marshals for special arrest powers that can cover them through FBI investigations. And the Internet Crime Complaint center is the forward -- it’s the public-facing website that has the ability to allow for the public and other agencies if need be to make a complaint about a cyber threat or a cyber attack that had occurred. There is a drop down menu. You just fill out the menu about what -- as much information as you possibly have. It guides you through providing information. And that information is, again, ingested into their system. There's a high level analytical product that's -- and research done on that. And then they push that through the appropriate federal agency and-or the FBI. It also houses a lot of public source information where -- I'll talk about the PIN and FLASH here in a minute. But all the public safety -- or public -- PSAs, I'm sorry. And the public information products we have about emerging cyber threats and patterns we may see, all that stuff is on the IC3 website. There are some go-tos and some information out there that can help a system administrator or just anybody, really, who's interested in hardening their system a little bit more. There's information out there that can help them do that. So here's what I mentioned earlier, the private industry notification [and the FLASH?]. So this is a main product that the cyber division pushes out for our private industry partners. The FLASH is the FBI Liaison Alert System. It is a technical type document that is meant, really for an

IT specialist or a chief information security officer to see that there’s a new threat. And we have indicators of compromise in the documents. We have some technical information in the documents that allow for a network administrator to input those roles into their network and harden their system just that much better. And the Private Industry Notifications, or the PINs, are really designed for [C suite?] level folks to -- they’re not as technical. They just show kind of an overview of what is occurring and what emerging threat may be the latest and greatest. I have an example of a PIN up front if you’d like to grab a hold of it -- here, I’ll get it. I want you guys to look at it. But on the PIN, it has contact information for CyWatch and IC3. If you have an incident in your area of responsibility that touches onto this information contained in the PIN or the FLASH, then it gives you directions on how to report that information back to the FBI. If you’re interested in being -- if you’re an IT person on the phone or in this room, if you’re an IT-type person, or you’re a program manager, a manager, or a C suite level, anybody that has a responsibility for an IT nexus in your area of responsibility, and you want to be on the PIN FLASH distro list, take down my email address at the end of this, and shoot me an email, and tell me who you are, where you work.

And we’ll get you added to the list. Fair warning, though, you’re going to get everything. There’s -- we can’t segregate it -- if you’re -- let’s say you’re energy sector, and you want to see only energy sector specific information. It doesn’t work that way. You get it all, or you get none. And I’m not talking about a heavy lift here, either. You’re not -- I’m not going to crush your email inbox with PIN and FLASH notifications. They come out as needed. But on average, you’re talking maybe 30 times a year on average, which I don’t think is too, too bad. I’m going to go back one. Talking about information sharing, we work heavily with our Information Sharing and Analysis Centers, or ISACs. Is anybody familiar with those? Yeah, OK. So there’s a lot of ISACs out there, or ISAC-ish type entities that are extremely beneficial. If you want to be part of them, then -- again, if you don’t have the ability or you don’t know where to start looking, you could shoot me an email, and I’d be happy to help point you in the right direction. But they’re also a very good resource to have under your belt as far as sharing information and pulling information. A lot of times they can get information a little bit faster than the government can, just because they’re not restricted to some degree as to what they can pull and how they pull it. But they’re also a very good mechanism to increase your knowledge base against the emerging cyber threats. Hold on, let me check something real quick. How am I doing on time?

BRADLEY: You're doing well. (Inaudible)

PARMELEE: Also there's an InfraGard -- has anybody heard of InfraGard? Yes? Is anybody here a member of InfraGard? Fantastic. So for those of you who don't know, InfraGard is a -- it's a resource. It's a -- driven by the FBI, where it allows you to join the membership in your local area. And every member -- it's designed to information share amongst your peers and other sectors, such as retail, maybe energy, chemical, transportation. It could be trucking. It could be auto. It could be oil and gas. But it's designed to share information amongst your peers. Every member that is in the InfraGard chapter is vetted. There's a background check conducted on each person. So the expectation is that the information provided to the InfraGard portal -- and if you join a special interest group that we have, every chapter and every portal has a special interest group. So if you want to share information, the expectation is that information is not going to be used to undercut your business. In other words, if you share information with a peer company or a competitor, the expectation is that they're not going to use that to undercut your bottom line. There’s all kinds of disclosures that are signed and et cetera, et cetera. So that’s also something to think about. I believe at the end there I have the -- yeah, I have an InfraGard website you can to look at and read more about it, and also sign up for the service. So who’s doing the hacking? I think everybody pretty much knows. You turn on the TV at any given second, and it will tell you somebody’s trying to do something. You have your hacktivists. You have your general criminals. Your (inaudible) threats are always a problem. Of course, you have spies trying to pull information about sensitive state secrets or proprietary information so they can reverse engineer it on the backside and try to save themselves some money. There are terrorists seeking to sabotage a computer system just to crush -- an attempt to crush our critical infrastructure. And at the very end of the spectrum, if we ever go to war, there’s always the element of the concern where there’s going to be a cyber nexus to an attack. So what happens typically with a hacker when they get on your network? It all starts with step one. They’re not going to just pick a system randomly. You know, a lot of -- a good hacker is going to do their homework. They’re going to get on your system. They’re going to do a recon. They’re going to look around, see what you have. They’re going to do their homework. They’re going to do a series of preeminent attacks, essentially, where they might try some social engineering. They might try some phishing against your company or against your employees. They’re going to do research on YouTube, Facebook, LinkedIn, and try to figure out who are the key players, and who may be the most vulnerable that they can launch an attack against. Or what type systems you have. You’d be surprised. Hacker are typically very resourceful. So they’re going to gather a lot of -- a lot of little pieces, if you will, add up to one big piece. They initially hit the -- after they compromise the system, they start to ingratiate themselves into the system, establishing their foothold. And they’re looking to see what’s there, how they can exploit what information is there, who they can compromise. And if that person has X, Y, Z privileges, they’re always looking to escalate their privileges inside the network. The goal being that they can be the root administrator, and they can have the complete keys to the kingdom. If they can own the network from the inside out, they’ve successfully fully penetrated. And they can go and see the big picture, so to speak. So then you have your internal recon. Once they get root access, they can see the big picture. Then they start seeing what is on your network as a whole. Then they begin to move laterally around to wherever they may want to end up. They expand their presence inside that network by owning and establishing a foothold in -- if you want to think of a network as a tree -- so you have the main branch on top, where that’s the big one. But then you move down. You start moving laterally across the network, and you start establishing a foothold in specific domains inside that network. And you just -- you own it. The hacker would own the network, not only from the top down, but from the middle out. Does that make sense? Then, of course, they decide what kind of data they want, if at all. They may hit you with a ransomware to lock the system out, then just extort the money out of you. But if they’re looking to pull proprietary information, let’s say, then they have the established foothold. They see what they want. They start moving the data off the system. And then they stay on there as long as they can in hopes that they can go back and keep pulling information off. This is just an example of how [off-the-network a routing can be?]. This is -- the target is in China or Asia. They jump from network to network using private virtual servers or -- virtual private servers or share file services, Tor network, where they can jump around. And they can just -- their basic -- their main goal right here is to obfuscate their path. So it makes it very difficult to trace them back -- trace it back to a single source. And when they pull data off -- I guess think of it this way. When they pull data off of a network, they’re not going to just send it from your network to their server or their computer. They’re going to jump it around all over the planet to try to hide the pathway back, to make it difficult on folks like the FBI to put them in jail, which is not cool. Here’s your different types of attacks. You have your denial of service attacks, your doxxing attack, which is just -- doxxing is gathering information about somebody or a particular person or group, gathering open source information. And they just gather all this stuff, and they release it out to the public without that person or company’s consent. It’s just really -- an example being -- let’s say a college student fails a course. And they don’t figure -- they don’t maybe think they should have failed the course. So they gather all this information about the professor in attempts to discredit them. And they throw that out in open source in the internet to -- without that professor’s consent. Theft of intellectual properties. PII and PHI is extremely valuable, extremely valuable, particularly on the dark web. Point of sale breaches. You know, the computers on the --

at the outlet stores that -- or the retail stores that have been breached. Filing false tax returns. And we've been hacked! (Laughter) Did I do that? That's OK. So you have your ransomware attacks. And then you -- of course, that's your extortion. If you get -- if you have ransomware that hits your system, you're going to have a problem. Either you can blow away your system and start over -- that's where good backups come into play. If you don't have backups, you got to have backups. Having a good backup -- let me say it one more time. Having a good backup is going to be your best friend in the event that you've been hit by ransomware. And don't think -- I give these lectures a good bit. And I've gotten into small -- very small groups. And like, "Oh, that would never happen to us. Because nobody knows who we are." (Laughs) Guess who doesn't care who you are? They care that they have found an exploit on your system. And your data is your data. It's important to you. As a bad guy, all I care is that data is important to you. And I'm going to hold it ransom until you pay me. There was just open source -- I was reading it when I was sitting over there. There was a small medical provider in Fairbanks, Alaska. Fairbanks, Alaska. Who's ever been to Fairbanks, Alaska? Right? OK. One person out of, what, 30? I know where it is. My son lives in Anchorage. But I didn’t want to go to Fairbanks. There’s nothing in Fairbanks. Except this provider. They got hit with a ransomware attack, and they lost over $44k. Not in dollars, PII. That’s crushing to someone like that. Because that’s probably one of the single source of health care for that area. And that’s a big deal. That’s not only just money out the window, but it’s also a lot of people that could potentially get hurt. Your business (inaudible) compromise in your [web face defacement?], which don’t happen too, too often anymore. But they still do. Who are the targets? The gist of this slide is everybody’s a target. I see [C-17, MH-370?]. What else do I see? Government, US government computers, military, health systems, missiles. Super value breach, what is that? So the gist is everybody is a victim -- or everybody’s a target. So you want to call the FBI. By the way, that’s me on the lower left. I’m kidding, that’s not me. So the gist is on this, the FBI will come in. They’ll help. Every field office has their own threshold and their own way of sort of doing business. They work in concert with the US attorney’s office. So to set a expectation right now, if there’s a dollar loss, let’s say, that is -- it may or may not rise to the level of what the threshold is for that specific area, as set by the US attorney’s office. Example being, the dollar loss threshold will be lower in, let's say, Jackson, Mississippi than it would be in New York or Los Angeles. So we understand that the victims are the victims. We don't want to drag anybody's name through the mud. We have no desire to do that. We want to go in, get the information we need. We will work with the local IT staff to determine what steps were taken to either stop the attack or prevent the attack, or what steps have been taken up until that point. We'll meet off site if necessary to avoid any sort of public display of the FBI. You're probably envisioning the FBI rolls up in the big blue jackets with the FBI on the back. And they have boxes and pelican cases with them, and they run inside with 30 people. It's -- hopefully it won't be like that. But that's really victim specific. If there's a concern to that, the FBI will work with you to address that. We'll need images of the servers. We typically don't go in and take all -- we're not going to go in and scoop out all of your server and dismantle your network and say, "Thanks a lot," and we'll come back later and leave you out of business. That's not -- we're just not going to do that. We're going to go in. We're going to image -- we'll take time, depending on the size of your servers and the amount of data that was taken and moved or you have in-house. And we’re only interested in the information that affected the breach. So a lot of times we hear some concerns about proprietary information that maybe on the system. We have no interest. If we find it, we segregate it. And then -- having communications and very good open communications between the FBI field office that’s responding and the victim company is going to be very critical. And please remember, it takes time. The investigation takes time. Because that’s not -- you’re not the only victim in many cases. But the amount of data that has to be sifted through is pretty substantial. So it takes a while. And just like any other government agency, we’re limited on resources. But also, in the event that there’s a significant event or there’s a large scale event, then not only in your company -- or in your AOR -- contact the bureau early is very beneficial. Because we can help mitigate any losses. Or we can at least get in on the front end. And we can -- it helps us better see who the actor is. And we can trace it back and hopefully put somebody in jail. The biggest threat you’re going to find out in the market right now is a business email compromise. There’s a variety of mechanisms to -- for an actor to use BEC as a mechanism to compromise your network or a network. It’s done mainly through phishing emails and-or social media -- or social engineering. I can tell you this. A BEC actor is -- they’re sophisticated. The large networks that go after the big, big dollars, these folks are very, very sophisticated. They’re going to do their homework. They will know everything there is to know about a particular company that they are targeting. They’re going to know how they do business. They’re going to know how they transfer money. They will probably even know what thresholds you have in place. A lot of -- I hear -- oh my god, if I’ve heard it once, I’ve heard it a million times. You know, a company goes, “The guy was just so nice on the phone. And he knew exactly what to say. He knew that our threshold was $15,000. Anything above that, I have to get concurrence from an upper management to send that money. And he asked for $14,950.” OK, that is below the threshold. They know. Or they target social media pretty heavily. Because they’re looking to see what the C-suite level is doing, how they’re moving. Are they away? Are they on vacation? Are they on a big business trip? Is there a pending merger fixing to happen, and how they can exploit those -- that gap, I guess, in between merger to full integration. I have a good, good friend of mine who was an investigator out in our Manassas office. He has a large BEC case, where the actors were targeting an extremely high-profile but very wealthy company. And they took the time to groom a person inside that company who was in a wire transfer-ish type department. They took six months to groom this person, befriend her, talk to her, get her to understand, and just be comfortable with -- recognize the number, recognize the voice. “Hey, it’s me.” They sent her gifts. They knew everything there was to know about her, because she was a prolific social media user. So they knew everything there was to know about her. And they used that information against her in the long run. But to give you an example of how sophisticated and what they will do to get to their endgame, not only did they take the time to groom her and get her set up for the, quote-unquote, execution of the transfer, but they hired an actor, a real actor, to impersonate the CEO of the company. The CEO was [out of pocket?]. Thanks to social media, they knew he was out of pocket. And they hired somebody that looked like him, sort of, kind of. Looked like him, close enough. And they trained this person up on some of the lingo he used. And they put him in a suit. And they put him on a Skype, but the room was kind of dimly lit. They knew that the CEO was out of pocket in a foreign country that probably didn’t have the best -- or the assumption is they didn’t have the best infrastructure. So the connection was kind of sketchy, which was done by design. So this lady is looking at a Skype, a live Skype, talking to whom she believed to be the CEO. Looks like him-ish, but the connection is kind of bad. So, OK, he’s saying all the right things. And he starts in on her about, “I need you to transfer $15 million to this account. I’m working on a deal. Nobody knows about it. But it’s done. I want it solid today. I want that money today.” “Well, I can’t” -- and what do you think? Now, this is the guy that he has been talking to -- she was talking to the CEO. But the person that she had been groomed by enters into the room and says, “Hey, it’s me.” She’s like, “Oh my gosh, is this for real?” He’s like, “Of course it is.” And then what’s -- what do you think he does? Now, six months he’s been talking to this lady. Just super nice to her, sends her gifts, talking to her on the phone, asking about her cats. Who knows? But what do you think he did to convince her to send the money ASAP?

BRADLEY: (Inaudible) [blackmail?]?

PARMELEE: He got mad at her. He got mad at her and starts to berate her. And she was so devastated that her buddy, her friend, the guy that sent her gifts, and knew everything about her, and was talking to her, and was her friend was so angry with her for not sending the money -- because here sits the CEO, and gosh dang it, he wants that money. Why are you doing this? And he starts in on her, starts yelling at her. He goes, “If you don’t ever -- if you don’t send this money, I’m not going to talk to you again. And we’re not friends.” And she was like, “Nope, not going to have it.” Hits the button. Money’s gone. That’s a very extreme example, but that happens a lot. And it happens easier than you think, especially with social engineering. These guys are very, very good at talking the talk. So what can you do? You can train your employees to understand -- don’t be click-happy on every email you get. Not every link is a cool link to get. But also understand that thresholds are in place for a reason. If business -- if you’re asked to send money or any sort of atypical business practice that is inside your company, it’s OK to question that. I would encourage them to question that. If I was the CEO of a company, I really can’t imagine that I would be upset with the lady in accounts payable or accounts transferable who wants to question sending $30 million of my company’s money somewhere. I should give her a bonus for at least questioning it. To give an example of how bad it really is, this is numbers that were collected by IC3. They received over 300,000 cyber crimes complaints and fraud complaints in 2017 alone. Over $1.4 billion in losses. And BEC was the number one cause of that loss. Now, these numbers that you're seeing up here are all general best-guess numbers. Because we can only report about what we know about. A lot of compromises and a lot of BEC-type compromises are not reported. The more we know, the more effective we can be, not only as a law enforcement agency, but also as the United States government in combating these threats. Update your policies in your companies. As you go back out and you reach out to your constituents in your areas of responsibility, encourage them to make changes. Look inside their companies. Look inside your respective agencies, and look for ways that you can improve your security. Train your employees. Question unusual business practices, any sort of vendor that calls you and says, "Hey, we're changing our bank account information. Can you send it to this one?" If that's done via email or fax, folks, that's a clue. Pick up the phone. Because my guess is, particularly for those vendors that may be on the phone, or if you have a relationship with a company, my guess is a company's going to have a fairly substantial relationship with a vendor, particularly ones that they do business with all the time. So my guess is going to be that the person at Company A who's responsible for sending money to the vendor, Company A is going to know that person on the other end. Pick up the phone. “Hey, did you just send me a fax? Or did you just send me an email about transferring money to a different account?” That, unfortunately, doesn’t happen as often as it should. And it would probably end up preventing a fair amount of losses. Facebook is the devil. So as I stated earlier, Social media is -- it’s good in its own way, but it’s bad in its own way. Have your folks and have your family and friends, and your employees, and your constituents understand that -- you’ve got to take a couple seconds to think about what you’re doing. What are you talking about? What are you posting about? I’ve seen some stuff on Facebook, that I just -- my family -- I’ll call them up and it’s like, “You can’t do that. You can’t do that. You can’t talk about that kind of stuff. You can’t put that out there.” I mean, it’s -- you -- every person in this room has probably seen something on Facebook or a social media site, and you shake your head, going, “Oh my god, what were you thinking?” Right? Again, just go back. And sometimes its repetitive. But it’s just one of those things where you have to constantly remind folks to be diligent in what they are posting out in the public. Real quick, so internet of things. That’s another viable attack vector. That’s a growing problem. I don’t remember, but about two years ago, maybe three, there was a power outage on the East Coast. It’d be more than that probably. But there was a large scale power outage on the East Coast started with a compromise of an IOT device. Ensure that it’s updated and patched. Every time you get an Amazon request to update Alexa, do it. Because -- and your phone, same thing. Because those security patches are extremely beneficial to your devices. If you can keep an IOT device off your main network or segregated somehow from your main network, that would also be probably a good practice. So your final thoughts. Develop a relationship with your local ISAC and your sector specific agencies, in addition to the local field office, FBI field office, and-or secret service field office or DHS office. Consider being a member of InfraGard, or at least look into what benefits are from being a member of InfraGard. Have an incident response plan. And test that plan. Just because you have one doesn’t mean it necessarily works. Test that plan. And I would encourage you to do it at least minimum twice a year. I’ve talked to companies that do it every 90 days. That’s excessive, but it’s also very effective. The time to trade business cards is not over a command post table. Do it before anything happens. Patch management. Classify and segregate your very critical data. Use multi-- consider using multi-factor authentication. Don’t -- have passwords change every 90 days, 60 to 90 days. Strong passwords or passphrases are extremely helpful. The NIST, the National Institute for Science and Technology -- thank you -- they have a very good website as well that gives a lot of very good information about preventative maintenance and best practices for cyber hygiene. And they have some pass phrases and schematics -- or not schematics -- but nomenclature that you can adopt. Here’s contact information if you need. Like, I said, if you have any issues with a local field office or you just need guidance with either inside the FBI or outside the FBI, I’m happy to help. I can point you in the right direction. Or I can at least recommend you to talk to somebody else, at a minimum. And if you want to be part of the PIN FLASH distro list, please shoot me an email. And with that I’ll answer any questions if you have any.

MASCIANA: Leo Masciana, State Department. Among the organizations that you walked us through was a action team, I think it was.

PARMELEE: Cyber Action Team.

MASCIANA: I was just wondering if they have an international scope or just domestic in the -- say an attack on Estonia type scenario, would they go out and assist an ally?

PARMELEE: They can. There has to be, obviously, a lot of moving parts put into place. That has happened before in the past. They can't take that initiative on their own. There has to be a formal request. And through the embassy in our [ALAT?] -- yes sir. We -- so for those of you who don't know, cyber division has a presence across the over -- there's 65 assistant legal attachés that are cyber-specific in the embassies across the globe. We're trying to expand that presence to every embassy if we can. And that person's responsibility is to interact with the local government much like the counterterrorism ALAT would be. But they're doing on a cyber-centric -- and cyber investigations. And that could be one of the mechanisms that the local host country can ask for assistance that way. Good question. Anybody else? OK.

BRADLEY: Thank you so much.

PARMELEE: I have some examples. I'll leave them up here or I'll put them out on the table over here. But there's some examples of -- like a ransomware pamphlet that we have. And InfraGard information as well. So I'll leave them on the back table here for you all. Thanks.

BRADLEY: Thank you again for an outstanding presentation. Our last speaker of the day will be Mark Riddle from my office who will be providing a briefing on the NIST Special Publication 800-171, protecting controlled and classified information, non-federal information systems and organizations. Ron Ross was supposed to do that, but he was called away. So we impressed Mark here. Mark, please.

RIDDLE: Thank you. (Inaudible) I'm going to turn out the lights again. Hopefully everybody stays with me, right? You can go ahead and turn on that screen there. Let me get that clicker from you. Hi, again. Mark Riddle again with the Information Security Oversight Office. I work in the CUI part of ISOO, which serves as the executive agent for the CUI program. I was actually one of the co-authors of the NIST Special Publication 800-171 and its various revisions. I'm here filling in today for Ron Ross. And I understand this briefing is going to give you a nice overview of what CUI is, the purpose of the NIST SP 800-171, the various families, how to use it, regardless of whether or not you have a contract or agreement with the federal government. First things first, of course, CUI. The title of this document is protecting controlled unclassified information in non-federal systems and organizations. What is CUI? First and foremost, CUI is information that we protect. It’s more importantly information that we protect because there’s a law, regulation, or government-wide policy that calls for this information to be protected. CUI is not the new FOUO. FOUO and SBU is a broad term that could mean almost anything. Oftentimes within agencies, for official use only is tied to FOIA exemptions. The CUI program is a lot more narrow in focus. If you were to take -- everybody knows what a word cloud is, right? It’s a -- basically if you can imagine that wall over there just covered with words, that’s kind of what information security looks like today. The government is trying to protect everything on that wall. The CUI program is a picture frame. We’re putting a black picture frame on that wall, and we’re going to say, you know what? We’re only going go focus our attention when it comes to protection on everything that falls within that picture frame. That’s the CUI program. We are a house cleaning effort that narrows the focus of protection to only those information types that can be linked to laws, regulations, and government-wide policies. What that means is that as agencies implement this program, there are going to be some things that fall off the protection grid, because there’s no basis to protect it in laws and regulations. The CUI program has been rattling around for a number of years. It finally got some steam back in November of 2016 when our implementing regulation hit the street. We'll talk a little bit more about that in just a moment. Now, of course, we have an executive order that was issued under President Obama in November of 2010. Now, this executive order, you can see it as a line in the sand moment, as far as our executive branch is concerned. This was the acknowledgement by the administration that information security practices surrounding sensitive information needed an overhaul. We reached a boiling point inside of the executive branch where something needed to be done. It wasn't an initiative that started with President Obama. It actually had some roots inside of the second Bush administration. But it finally got steam under President Obama. He issued the executive order and said, OK, enough's enough. There needs to be a program to standardize how we protect this information. Because you guys know this term, the wild west, right? If you were to go out right now, from agency to agency to major stakeholder, it is the wild west. You don't know what they're calling sensitive information. And you also would be surprised on how they were handling and protecting that information, be it in a physical environment and also in the electronic environment. So something needed to happen.

So to form the CUI program, of course, the executive order appointed the national archives and records administration as the executive agent for the CUI program. And that was of course delegated down to the director of the Information Security Oversight Office. What we were charged with doing was developing a program, taking existing practices and folding them into something that everybody could wrap their arms around and say, you know what? That is security. The speaker before me was talking about all these things that are happening to information security in the state, local, tribal environment, and also inside of the executive branch. And everybody wants to know what are we going to do about it? How are we going to shore up our information security protections, not only in the executive branch, but also in the non-federal environment. The NIST SP 800-171 is an answer to one of those questions. It defines security when CUI is entrusted to non-federal entities on systems. Now of course, the NIST SP 800-171 applies to non-federal organizations. So we have federal contractors, state, local, tribal governments, and also colleges and universities. Now, these folks through contracts and agreements will start to see some of these requirements from the NIST SP 800-171 come through from federal agencies. So as agencies implement the CUI program -- and we’re about a year and a half into implementation -- once agencies modify their policies, train their workforce, one of the things that they will be doing is modifying all of their contracts and agreements to make reference to CUI standards, including the NIST SP 800-171. Right now, if you guys are doing business with the executive branch, various agencies, that conversation or that agreement usually reads like this. If you want to do business with Agency X, my agency, you have to call it what I call it, and you have to protect it the way that I protect it. And those protection measures that agencies give to non-federal entities is oftentimes inconsistent. With the CUI program, that conversation once this program is fully implemented is going to be a little different. There’s going to be a lot more clarity on what you’re actually supposed to be protecting, what you’re going to be calling it, and especially how you’re going to be protecting it. Now, inside of the CUI program we have something called a CUI registry. Now, this is a catalogue of information types that make up the CUI program. Earlier when I first introduced the term CUI, I brought down the -- that high level definition, which means information that requires protection because there’s a law, regulation, or government-wide policy that needs -- that calls for it to be protected or shared in a very particular way. Now, that term is really fancy. And it almost means nothing to nobody, right? You can't implement an protection program around that term. So we needed, too -- ISOO and an interagency group called the CUI advisory council -- we needed to bring that term down to the ground level so that way the implementers, the people who are actually working with this information would know exactly what was expected of them when it came to protection. So the CUI registry operates a lot like a security classification guide. In the classified community, a classification guide tells you what is classified. In the CUI world, the CUI registry breaks down what CUI is. There's about 25 different categories of information now. And of course, the usual suspects of information types that can be found there, like federal tax information, law enforcement sensitive information, unclassified intelligence information, critical infrastructure information. The usual suspects of what you would normally be protecting under this program can be found on the CUI registry. A number of other things can be found there, because this is a tool for implementers of the CUI program. About the CUI registry, it is something that isn't created for the average bear at an agency. We don't expect agency personnel to go to the CUI registry to understand how to protect CUI. Just the same thing, we don’t expect state, local, tribal folks to go to the CUI registry to find out how to protect CUI that they’ve been entrusted with. They have to go -- agency personnel go to their agency policies, which will be modified in accordance with the standards of the CUI program. Contractors and state, local, tribal folks, you guys will use those agreements to protect information. So one of the things that agencies will do as they implement is they will modify all those agreements to identify the specific information types that you as non-federal entities are expected to protect and handle in association with the federal government. I will have time for questions at the end. I know this is kind of like drinking from a fire hose. It comes at you pretty fast. But we have a lot of resources on the CUI registry that you can use to help educate the workforce and also help increase your understanding of the CUI program. We have a number of policy guidance documents for agencies. And we have a number of training modules that we have there to help you train the workforce and also help you understand the program. Also, if anybody in the room or if we have a line open would like a special briefing on the program, my office is actually available to provide that to you. We also offer a quarterly briefing to stakeholders. If you subscribe to our CUI blog, of course you -- the next one is August 15th, 1:00 to 3:00, Eastern Daylight Time. You'll get the latest and greatest of what's going on in the CUI program in regard to the products we're developing, the initiatives that we have underway, like the development of the federal acquisition regulation, which I'm going to talk to you in just a moment. So actually, just on this slide. So the first thing's first. We have our 32 CFR part 2002. This is the implementing regulation for the executive order for the CUI program. This regulation, of course, became effective in November of 2016. And this was the -- it is the implementation regulation for agencies. As agencies move to implement this program, they're going to be using this regulation to modify all of their policies and procedures. And while we're here on this big picture slide, we have to talk about why is it necessary for agencies to modify their imple-- or their policies and agreements to align to this standard. Because if you go back to where maybe 20 years ago, when agencies started to really develop all of their policies in regard to information security, they started out with laws, and regulations, and government-wide policies. These things told them that certain information types needed to be protected. The issue, of course, is that these regulations failed to say how. So they put agencies in the driver's seat as far as defining what they were going to call this information and how they were going to protect it in the federal space and also the non-federal environment, through contracts and agreements. So this freedom that was given to agencies kind of gave rise to terms like FOUO, SBU, SSI. Those terms were created because there was no oversight entity to reel those agencies in. So that's why it reached a boiling point under President Obama that something needed to be done. So when this rule became effective, it essentially took agencies out of the driver's seat when it came to defining protections for information, how to protect that information. The CUI program, this regulation will fill the void. So if most regulations never speak to how to protect information in the electronic environment, the CUI program draws a pretty hard line in the sand for how that should be done. In the NIST SP 800-171, those tech standards are actually conveyed to the non-federal environment. The moderate baseline. What you're looking for inside of the NIST SP 800-171, or what it is, is a reflection of the moderate confidentiality impact value. This is the standard that agencies have decided is appropriate for the protection of CUI and also appropriate when we share it or we ask a non-federal entity to protect information on our behalf. So we actually -- this is a statement by Ron Ross. We actually are doing the exact same thing once we're fully implemented. We aren't asking non-federal entities to implement security controls that are drastically different from what we're doing internally. There's consistency in practice. Now, the last element in this big picture, the three part plan for the CUI program, is the federal acquisition regulation. This is something that ISOO has been working with an interagency group to develop. We've been at this for a couple of years now. Ever since our CFR became finalized back in November of 2016, we've been working with GSA, NASA, DoD, and a number of other agencies on developing a FAR. Now, why is a FAR important? Because again, the conversation that usually happens with agencies in regard to non-federal entities is it breeds inconsistencies. Agencies are saying, "Call it FOUO." Then another agency says, "No, call it SSI." And everybody's saying, "Protect it X, Y, Z way." And it doesn't look the same. So the Federal Acquisition Regulation, once it's finalized -- and as the CUI program is fully implemented in probably about two to three years -- this regulation, the FAR, will standardize the way that the executive branch communicates safeguarding guidance to non-federal entities. So all of a sudden, now executive agencies will actually appear to be on the same page. They’re going to say, OK, you have to protect sensitive information, it’s CUI. It’s this particular category. These are the standards that you have to use to protect it, whether it be on a regular company system or a cloud-based system, which we’ll talk about in just a moment. Now, again the purpose of the NIST SP 800-171 is to convey this requirement for how agencies protect sensitive information. We don’t want a two-state solution here. Now, this being said, of course, we wanted to make sure that agencies or that non-federal entities were not given requirements that were uniquely federal. So as we were developing the NIST SP 800-171, we took the moderate baseline, after we knew where we were going to go with how information should be protected. We needed to strip through the moderate baseline to strip out all of those requirements that were uniquely federal. So things like continuity of operations, continuity of government, some documentation that the government loves to maintain. Those are the types of things that were kind of stripped out. And of course, the NIST SP 800-171 has a laundry list of the controls that are contained in the moderate baseline and the ones that didn’t make it to this document. Now, also I forgot to mention on the very front end, the -- of course the 171 has gone through a couple of changes over the past couple of years. It was originally issued in June of 2015. There was a revision one in December of 2016 and yet another [rather?] change also in June of this year. So if you were to go to the CUI registry page, go to our policy and documents, you can actually pull up the latest and greatest version of this. Another document that was created by NIST just recently and published in June is something called a NIST -- it's the NIST Special Publication 800-171-A. It's an assessment guide for the 171. This is issued in final form, and it'll be something that agencies use to assess compliance to these standards. But also non-federal entities can use the 171-A to conduct their self assessments. You basically have the questions that you will be asked in regard to how your system is configured. Also, the 171 and the 171-A were modified to include an expanded explanation of each security requirement. One of the things that you'll notice about the NIST SP 800-171 is that we have, of course, 14 families. These are the same 14 families that we use inside of the executive branch to protect systems. The issue, or the golden -- the great thing about the 171 is that as non-federal entities implement these security requirements, you don't have to do it the way that the government does it. Now, what that means, of course, is that you still have to satisfy every one of these requirements. Let’s take the control of multi-factor authentication, which is -- in the federal government, we satisfy the control of multi-factor authentication by using our ID cards. That’s something we have. And then we punch in a password, the something you know. That requirement extends to the non-federal environment. But you don’t have to do it the government way. And that’s kind of the whole theme inside of the CUI program, is that there are security requirements and standards that have to be met. But you don’t necessarily have to do it the exact way that the government does. So these are some of the families that are inside of the 171. And you can kind of zero in on each one of that. I’m not going to go into a whole lot of detail on each on of these controls. But things like escort requirements, training records, physical security protections, the whole idea of encryption in transit. These are concepts that are conveyed in here. And then of course, there’s a detailed table that explains each one of these security requirements. Again, since this has been rattling around out there since June of 2015, most non-federal entities, especially in industry, have adapted most of these security requirements to their systems when there’s a connection to the federal environment. So the NIST SP 800-171 is broken down into basic security requirements and derived security requirements. Basically, these high-level statements about how to configure a system that contains CUI. And they’re pretty broad. There’s a difference inside of the IT world on what a security requirement is and what a security control is. Inside of the federal environment, we pretty much use security controls. We like to do it a very particular way, like our ID cards, which satisfy multi-factor authentication. A requirement gives flexibility to the non-federal community on how to satisfy those requirements. Now, inside of the NIST SP 800-171 there is a requirement for non-federal entities to maintain a system security plan, something that describes how you’re satisfying all of these requirements. And then of course, upon request, federal agencies can ask for that system security plan. Because again, they are the keepers of that information, and they want to make sure that you’re doing it in accordance with these standards. And of course, as they go to evaluate your systems, the use of the NIST SP 800-171-A will be rolled into the mix. There’s a couple of important appendices to the NIST SP 800-171. The first one of course is a mapping table. Now, the 171 is based off of the NIST SP 800-53, which is the playbook for how federal agencies configure their computer systems. And one of the most common questions that I get when I get out there and talk to folks is, “What the heck is the difference between the NIST SP 800-53 and the NIST SP 800-171?” The short answer is about three inches, right? So one document, the 800-53, if you were to print it out end to end, it’s about 450 to 500 pages long. If you were to print out the 171, you’re looking at 100 pages or so that explains these requirements. The reason for that is the 800-53 contains every control in the low, moderate, and high baseline. So agencies, as they’re configuring their systems, they kind of pick which controls they’re going to use depending on how they’ve elected to configure those systems. What we’ve done with the 171 is we’ve extracted every moderate control that matters to protect the confidentiality of information and put it into a document. So a lot of agencies actually use the 171 to explain to senior leadership on what are these controls that are residing in the moderate baseline to protect confidentiality. And of course, the tailoring criteria is in there as well. Now, at this stage in the game, Ron usually has some very poetic words to say about information security, which I will spare you. Because I don’t think I could ever quote him quite right. But believe it or not, this is a philosophy. It is an ongoing thing. Whenever you get out there and start looking at your computer systems, it’s more than just the systems itself. I think the guy who was speaking before me was talking about developing a security program. And that’s actually the CUI program. As we move into this age of this reform, which is the CUI program, you’re going to see more defined security requirements in the way of systems. You’re also going to see greater and more defined physical standards in that environment, and also training requirements. There’s also going to be a greater focus on internal security. Once we put up these barriers to prevent the outsiders from getting access to our electronic infrastructure and our physical infrastructure, we have to start paying attention to who inside of our organization has access. I heard this term earlier today about, “We don’t want to give anybody the keys to the kingdom.” This is a true statement. And the CUI program was built to prevent that. We want to make sure that when somebody has access, they don’t have too much access. When we’re talking about CUI, right now we don’t have terms in the CUI program like Snowden, Manning, and Winner. It’s because we never had a program that was looking, and we never had an oversight entity that was aggressively identifying these issues related to an insider who had too much access. In probably the next five years, we will have a name, because we’ve had a program in place, and we would be looking. Now, a lot of people have a question about the cloud. How do I configure my systems? Or how do I protect information that’s maintained on the cloud? You can lean on the FedRAMP moderate standard. You can just actually type in FedRAMP.gov into any search engine, and you’ll see the laundry list of controls that exist for -- if you’re using a cloud-based system. Now, also in the Federal Acquisition Regulation that we’re drafting, we’re talking about a lot of information systems. Agencies are not just going to be using these static systems where the 171 would apply. Most organizations, agencies included, are moving to a cloud-based solution. So how are we going to protect it? We have a standard that’s already been well-established. The FedRAMP site has templates, sample system security plans, spreadsheets that break down the various controls that matter in that environment. Now, I think that takes me right up to the end. Here’s our contact information. Pat Viscuso in our office recently retired. If you have any questions regarding the CUI program, please feel free to send them my way. Of course, Ron Ross and Kelly Dempsey are co-authors of this document as well. They get out there on what Ron calls the speaking stump in engaging with folks on these standards and what’s coming next. I can speak to a couple of things that NIST is working on. Of course, in relation to the CUI program -- so of course, the NIST SP 800-53, which is the playbook for agencies when they configure systems is also going to be modified, if it hasn’t been modified already, to include direct references to the CUI program. Now, in the past, agencies have always been given the option of how to configure their computer systems if sensitive information was contained on it. When the CUI program hit the streets, there is a firm line in the stand. When CUI is present on a system, federal or non-federal, the moderate confidentiality baseline is the way it must be configured to. So in addition to the 800-53 being modified, the NIST SP 800-60 will also be modified to include some of these standards. And a slew of other publications as well. I think with that, does anybody have any questions for me? Yes sir.

MASCIANA: On your moderate risk controls -- let me just preface this by saying that what I’m familiar with on network security for sensitive and classified networks is perimeter border firewall encryption, and probably IDS as well, as standard. Questions have been arising from our CIO concerning CUI requirements for messaging at Assessing

Security Requirements for Controlled Unclassified Information and also encryption at rest for storage within a network. So specifically, is that required? NIST-compliant encryption in those two situations?

RIDDLE: So yes. There are specific requirements in the moderate baseline for encryption in both circumstances. Now, one of the things that different inside of the federal space versus the non-federal environment is agencies inside of the executive branch have the ability to make risk-based tailoring decisions. Now, this is something that's actually hardwired into the CFR. So a chief information officer at an agency still has the ability to make a risk-based tailoring decision regarding any of the controls in the moderate baseline. The thing that you have to think about, though, as you tailor out certain controls, especially certain things like encryption based off of the risk -- you're entitled to do that -- is that what are the compensatory controls that you have in place to mitigate that risk? And are those acceptable? And then is everybody on the same page? Now, the idea of encryption inside of the federal government is a tricky one. And we actually -- I run a working group that talks about various issues related to implementation. And one of the topics, of course, is encryption. Everybody does it right now when they’re sending certain information like privacy information. The issue, of course, is that if you have 20 agencies that you’re sending it to, and you’ve encrypted it, and you hit send, some of those agencies will legitimately not be able to open it. And then what happens more often than not, the mission has to continue. And we end up sending that information in the clear. We don’t want that. So we have to find a way to tackle this encryption problem. Right now NIST maintains a site that has a list of companies, I guess, that have been evaluated to meet the standard that’s referenced in the CUI program and in NIST, which is the FIPS 140-2. The issue, of course, is these things are not necessarily compatible. But the compatibility of encryption software is something that needs to be addressed, not just by the CUI program, but generally by CIOs. So one of the things that we’re hoping to do at the CUI advisory council level is trying to identify the best practices and the issues so maybe we can find a way to solve the issues related to encryption.

MASCIANA: Well, as we move to a cloud, this becomes an even more acute problem. And for those data architects who are trying to engineer this into at least the messaging side, what sort of deadline are you looking for for compliance?

RIDDLE: Oh, that’s a good question. So the deadline in regard to compliance for IT systems is actually pretty soft. Right now, we are asking agencies to report to us on the status of their implementation efforts. In regard to systems, we’ve asked that you develop a plan for this transition to the CUI standards. We haven’t set a firm date in the sand to say you must do it by 2022. But you have to have a plan in place to get you to the point where all of your systems are compliant. In regard to systems architecture, one of the things that you probably are already doing that you probably have to dive into a little bit deeper is the idea of the compartmentalization of data. Putting up those electronic barriers so that way when somebody is accessing your systems, whether in a cloud or whatever, that they don’t get access to the entire world. But in regard to the implementation of the requirements, there is flexibility. Every agency at this time -- on November 1st, we’re going to ask agencies to report to us again. The main questions that we ask for agencies is that -- where are you at in the development of your -- the transition of your IT systems. Have you completed it? Are you assessing? And then we ask another question, just two questions. What day do you expect all of your systems to align to the standards of the CUI program? And with that, as long as you don’t say that it’s going to be 20 years or something, then we’re not going to push back. But whatever date that you have in place, one of the things -- it should be tied back to some sort of a transition strategy. And I think that -- I’ll stick around afterwards for any other questions. But I’ll turn it back over to Director Bradley.

BRADLEY: OK, yeah, let’s wrap this up. Just quickly, does anybody have anything to say at all? This is the open forum section, so.

SACHS: I know I need to be real brief. (Inaudible) We can do this offline later. But I’d love to pull the chain a little bit on the tear lining of very, very sensitive information that’s time-based. So a lot of the cyber stuff that comes out might start off TSSCI. But a system administrator’s not cleared. We’ve got to be able to get indicators to those sys admins real quick. And that’s -- again, we can talk about that later. But if there’s anything else we can do to help make that, we’re standing by to help out.

RIDDLE: You’re on board, right.

MASCIANA: On that same thing, I had discussed it earlier, but I would like to propose that discussion for the classification as potential barrier to be part of our future business and enter into some of the discussions we’re already having about access. And just to add that it’s already identified in the National Security Strategy as a barrier. So the group, I think, should take an initial look.

BRADLEY: Agreed. We will do that. All right. Let me just wrap this up. The next SLTPS-PAC meeting will be held on Wednesday, January 30th, 2019. And the one after that will be Wednesday, July 24th, 2019. Ten o’clock to twelve o’clock here at the National Archives. All right, with that I’m going to adjourn the meeting. (Bangs gavel) Thank you. (overlapping voices; inaudible)

END OF AUDIO FILE