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

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its eleventh meeting on Wednesday, July 27nd, 2016, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. Bill Cira, Acting Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on December 23, 2016.

I. Welcome, Introductions, and Administrative Matters

The Chair welcomed the attendees. He noted that a meeting scheduled for January 27, 2016, was cancelled because of a government shutdown due to bad weather. He reminded the attendees that all SLTPS-PAC meetings are recorded events subject to the Federal Advisory Committee Act and are open to the public. He noted that a transcript of the meeting would be made available through the ISOO website and that the meeting folders included the agenda for this meeting as well as minutes from the last meeting.

The Chair noted the departure of several members since the last SLTPS-PAC meeting: Will Pelgrin, Marcus Brown, and Clyde Miller, and thanked them for their service to the Committee. He then introduced new SLTPS members: Lee "Tip" Wight, Executive Director, Washington Regional Threat Analysis Center (now serving as the Director, Joint Strategic and Tactical Analysis Command Center, Homeland Security Bureau, DC Metropolitan Police Department), who has also been selected by the SLTPS-entity members to serve as the new SLTPS-entity Vice Chair; Sergeant Dorie Korin, a detective and supervisory taskforce officer in the Las Vegas Metropolitan Police Department; and Richard Licht, Vice President and Chief Administrative Officer of Security Operations for the Center for Internet Security and Multi-State Information Sharing and Analysis Center. He also noted membership changes from the Defense Security Service (DSS), whose new member is Keith Minard, Assistant Director of Administration and Policy Analysis, National Industrial Security Program (NISP), and whose alternate is Derrick Broussard, NISP Senior Policy Analyst. After the introduction of all Committee members and public attendees, he introduced Greg Pannoni, Associate Director for Operations and Industrial Security, ISOO, and the Committee's Designated Federal Official (DFO). (See Attachment 1 for a list of members and guests in attendance.)

II. Old Business

Updates from the DFO

Greg Pannoni, DFO, began by reminding the membership that due to federal budget constraints the reimbursement of travel expenses continues not to be possible, and encouraged future Committee participation via teleconference. He thanked Kevin Donovan for attending in person. He stated there were no action items from the previous meeting.

III. New Business

A. SLTPS Security Program Updates

Charlie Rogers, Vice-Chair, Department of Homeland Security (DHS), and Chief of the DHS's SLTPS Management Division, began an SLTPS security program update by explaining that the Division he manages is responsible for taking care of state and local security and applying Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," to the state and local environment. The office's primary focus, apart from establishing security clearances, is on fusion centers. He noted that there are 78 fusion centers, of which 52 are designated as primary. Approximately 55 of them have been granted access to the Homeland Secure Data Network (HSDN), which is a secret level system. His office also certifies the rooms, deploys the systems, and makes it possible for the states to manage both the rooms and the security environment within the centers. He pointed out that much effort is concentrated towards ensuring that there is a trained security liaison in place and functioning at each fusion center. Naturally, as there is almost constant personnel turnover, there is likewise a continual requirement for his Division to train center security liaisons and to ensure that they understand the requirements of federal policy. To that end, the DHS has established a team of people who have been assigned fusion centers, regionally, with whom they are in regular telephonic contact.

Mr. Rogers then turned to metrics for the program. He noted that his Division established a Security Compliance Review (SCR) program, which completed the first fusion center review in late fiscal year (FY) 2012. His team has completed 15 to 19 SCRs in each subsequent year, for a total to date of 70 reviews. The SCRs evaluate a center's security environment with respect to how it operates in accordance with the implementing directive and other federal security regulations. The DHS tries to identify best practices. It makes observations and mandates required actions for any discrepancy (i.e. a fusion center procedure that is contrary to a federal regulation). All discrepancies must be resolved within 60 days. Most are resolved quickly and affect normal operations only moderately.

The DHS also conducts webinars on the Homeland Security Information Network to ensure that the security liaisons are trained. The DHS began this procedure in 2013 and now conducts five to ten live on-line webinars each year. The DHS trained 81 security liaisons last year, and thus far this year it has completed seven webinars and trained 52 security liaisons. The primary goal is to train newly appointed liaisons, as well as those who require refresher training. However, the training is not limited to that, as it focuses the liaisons on a single activity in which they can ask questions and the DHS can provide information. Further, since the SLTPS-PAC was unable to hold the scheduled meeting last January, the DHS took the opportunity to host its fourth Security Liaison Workshop. It was held at the Federal Emergency Management Agency in Washington, D.C. with approximately 45 state and local security liaisons in attendance. Several federal agencies, including the Federal Bureau of Investigation (FBI) and the DHS, provided training on a range of topics, to include presentations on insider threat, operations security, foreign access management, travel reporting, construction and modification of secure rooms, and locks and containers. Mr. Rogers noted that attendance was higher in previous workshops,

which were held in Oklahoma, Texas, and New Mexico, each of which was attended by approximately 75 security liaisons.

Mr. Rogers turned to another accomplishment of the SLTPS program. He reminded the Committee that E.O. 13549 establishes the requirement for documenting and tracking the final status of security clearances for all SLTPS personnel. To that end, the Division worked with the Office of Personnel Management (OPM), which modified its Central Verification System (CVS) to create a user role for state and local personnel to allow the CVS maintain the repository of state and local clearances. In addition, the OPM worked with the Department of Defense (DoD), which provided a channel for access to the Joint Personnel Adjudication System (JPAS) through which information could be collected that would greatly benefit security clearance access. Also, in July of last year, the DHS and OPM ushered in a pilot procedure through which was established the methodology for beginning the transfer of this information, thus permitting state and local users to access CVS in order to conduct security liaison business. Essentially, this process provides a fusion center access into CVS wherein state and local security clearances can be quickly and easily validated. This process proved to be of significant value, as the fusion centers store and operate at the secret level, and they can save time and energy by simultaneously validating multiple visitors. In addition, they can now reach back to key agencies, such as the FBI and/or DHS, to discover whether or not an individual has been cleared. Finally, due to the initiative's rapid growth and broad success, last fall, the pilot was completed and the DHS began transitioning in the security liaisons. Today, the system is up and running, and Mr. Roger's partners at the Office of Intelligence and Analysis at DHS are managing the security liaison invitations and working effectively and efficiently with them.

The remaining element that the DHS now has under way is an insider threat program. Because the DHS is establishing an insider threat program for the Department, the SLTPS program has the benefit of access to established DHS policies and procedures, which it will be able to apply to state and locals. Currently there are mechanisms in place to track state and local security incidents and violation reports, and there is a training program for SLTPS personnel. Therefore the DHS is in the process of preparing to establish a robust insider threat program. Mr. Rogers does not expect this to be a big program for SLTPS entities because the number of users of classified systems at state and local level is small since even at the fusion centers that have HSDN not all cleared personnel use the system. However, there are aspects about insider threat that go beyond the system, and the program will be established for state and locals as the DHS migrates it out.

Finally, Mr. Rogers turned to clearances, reporting that the DHS has cleared over 2,000 private sector personnel and over 5,000 state and local personnel. This presents challenges in meeting the needs of such a large and ever-growing population of clearance holders. While noting that the next presentation will discuss some of the cyber security concerns of the Federal Government, he indicated that he expects the number of SLTPS clearances to rise in support of various initiatives with the private sector on cyber security.

Tip Wight, SLTPS Vice Chair, stated that he really appreciated the DHS's initiatives to expand the clearance program down to the state, local, tribal, and private sector, as this is critical for interaction. He indicated that this is especially true for cyber security, which requires getting

access to Top Secret/Special Compartmented Information (TS/SCI) material, an issue that he indicated he would raise later in the meeting.

Mr. Wight noted that the ability to maintain clearances, is absolutely essential for analysts to be able to interact with their counterparts in an environment like the National Capital Region and across the entire nation in order to effectively communicate threats down to the state and local level and the private sector. He again expressed appreciation for the DHS's efforts. The Chair then reintroduced Charlie Rogers and Greg Pannoni to discuss a new initiative that sets forth NISP procedures for sharing and safeguarding classified information with certain private sector and other non-federal entities.

B. NISP Procedures for Sharing and Safeguarding Classified Information with Certain Private Sector and Other Non-federal Entities.

Mr. Rogers explained that a few years ago, while in the process of working cyber security issues under the authority E.O. 13549, the DHS cleared some critical infrastructure subject matter experts (SME) with whom it wanted to establish much-needed partnerships. That process moved forward smoothly until partners in the DHS's National Protection Programs Directorate (NPPD) felt that they needed to sign agreements with the private sector. The initial agreement format was known as the collaborative research and development agreement (CRADA), and within it was embedded language related to providing security clearances as well as access to classified information. Since those CRADA were essentially agreements between the DHS and an industrial firm, they were thus subject to the NISP. While the authority granted under E.O. 13549 permits clearances to be provided to individuals who have special expertise and may simultaneously work for a specific company; this relationship is not with the company and is not articulated in the agreement. Further, these CRADAs between the DHS and private sector companies did not constitute classic contractual relationships in that they did not involve the reimbursement of funds for services performed. However, once the DHS and the NPPD realized that they had entered into a special relationship that would come under the authority of the NISP they began to submit these companies for facility clearances. However, some of the companies, notably those who had entered into CRADA only as a means of acquiring security clearances for the sole purpose of supplying critical infrastructure SMEs, did not desire to enter into the normal NISP processes leading to the acquisition of a facility clearance, as these processes require, but are not limited to, appointment of a facility security officer (FSO) and clearance procedures for its senior officers. Therefore, these companies withdrew from participation in the CRADA, leaving the DHS without some valuable partnerships and without access to needed critical infrastructure expertise. This condition resulted in discussions between the DHS, the DoD, and ISOO on how to solve this dilemma, but no consensus was reached. In December 2013, the Cyber Interagency Policy Committee (CIPC), under the authority of the National Security Council (NSC), challenged the DoD and the DHS to review their processes for clearing private sector entities to determine if an alternative, or hybrid, process could be developed. In July 2014, a draft document was submitted to the NSC for this purpose. Then in early 2015, Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," was written. Although this was primarily a cyber information sharing E.O., embedded in it was a revision to the NISP that appointed the DHS as its fifth cognizant security authority (CSA) and ensured that should the hybrid be implemented it would be done so by an agency within the

NISP and therefore would not represent an alternative industrial security program. The hybrid has now undergone several revisions, and ISOO sent it back to the NSC in April of 2016. While further CIPC discussions have been held, no final decision(s) have yet been forthcoming. Should the hybrid ultimately be approved substantially in its present form it would allow a private sector company to have a limited number of senior management cleared: an executive and someone with responsibility for any classified operations performed by the company. In addition, it would require that the senior manager sign an acknowledgement form stating that he/she would not interfere with any classified operations and would require the company to sign a security agreement with the DHS that would further define the relationship. It would not permit any storage or access to classified information on-site at the private sector company. Access to classified information would occur only at a federal or cleared contractor facility. Further, the company would not receive a facility clearance, would not be permitted to bid on any classified contracts, nor be reciprocally accepted as a cleared facility. However, it would have some cleared individuals. The company would not be required to have an FSO, but one of the cleared employees would serve as a security point of contact who would be required to meet NISP reporting requirements. The company would still require vetting for Foreign Ownership, Control, and Influence (FOCI). FOCI is a robust protocol that is currently completed by the DSS and the Department of Energy, and there could be one or more additional CSAs required to evaluate for FOCI, and/or to take mitigation action(s). The security point of contact would be required to receive specialized SLTPS training. The DHS would be required to assume the obligation to serve in the capacity of the FSO on behalf of the company in order to adjudicate the clearances for these select companies. Many of these cleared individuals would rotate to DHS cleared facilities and/or be detailed to work in DHS facilities. Also, the DHS would naturally incur oversight responsibilities and would have to begin by developing the oversight protocols. An additional concern is resources, which are major issue for both the DSS and the DHS. In addition, trained personnel to accomplish requirements such as FOCI and corporate structure evaluations are unique, and these activities require dedicated assets. Consequently, the DHS is in discussions with the DSS in order to build on the DSS's internal policies, standard operating procedures, and other protocols.

Mr. Rogers explained that it is not yet known how long the proposal will remain with the NSC. Mr. Pannoni responded that it could be as much as four months. However, he explained that is moving towards a deputy's committee. At some point, the DoD and the DHS will have approved the end product, which would then be presented to the principals, perhaps as early as the fall of 2016. Mr. Rogers pointed out that the DHS is operating on the expectation that the proposal would be approved and is working with the DSS to find ways to detail personnel there and is looking within the DHS to identify personnel who can be assigned to this function.

Mr. Pannoni pointed out that just as with the entity's clearance being limited to just this activity, critical infrastructure, cyber security sharing is limited. That is, the entity itself cannot sponsor the individuals within that entity that hold personnel security clearances to reach out to and become involved in other classified areas. Rather, the organization must work through the DHS. Mr. Rogers concurred, pointing out that the DHS would always serve as the FSO. The company must nominate personnel who would then be evaluated by the DHS for mission requirements. There is a lot to be accomplished, but it is important to begin to get some small number of companies through a working process so that the DHS can determine all the protocols that must

be developed in order to build the program. Mr. Rogers indicated that the DHS will always need the help of the DSS because of its databases and its expertise, but the idea is that over time the DHS would build an internal capability to do more of this independently while still consulting with the DSS. Eventually, of course, the National Industrial Security Program Operating Manual (NISPOM) would have to be revised, so that the hybrid would then be included into the policy documents of the NISP.

Mr. Pannoni then pointed out that there is currently an overall rewrite of the NISPOM, in which space has been reserved to include the procedures just discussed. Also, ISOO has oversight responsibility for the NISP, and has an implementing directive for that purpose, namely the 32 CFR, Part 2004, "National Industrial Security Program Directive No. 1," which is also being updated, and space has been reserved in it for these special procedures.

Mr. Rogers then pointed out that there were approximately 45 companies that went through the facility clearance process, and some number of them may transition into the hybrid, but others may decide, or the DHS may decide, that they are better fit for the facilities clearance model. There are perhaps 70 to 80 companies that are waiting for the hybrid to go through. Processing that large a population would constitute a monumental effort that would not happen overnight.

Mr. Wight asked at what level these clearances are contemplated. Mr. Rogers explained that the DHS Division 1 and NPPD partners observe that most of the cyber-related information is at the TS/SCI level. So, access would be at that level, but it would not occur at the facility; rather, it would be at federal facilities, and not necessarily limited to DHS facilities. He also noted that once these critical companies are cleared and have accumulated a pool of cleared employees, then other federal agencies that have cyber-related missions are likely to desire interactions with them. The Chair then called for Mark Riddle to provide and update on the Controlled Unclassified Information (CUI) program.

C. CUI Program Updates

Mark Riddle, ISOO, began by reminding the Committee that the concept for CUI originated with E. O. 13556, "Controlled Unclassified Information," a three-page document that acknowledges that something needs to be done throughout the Executive Branch with regard to the handling and protection of unclassified information. It acknowledges that the Executive Branch handles and protects this information inconsistently, not only across agencies, but also internally within agency major components. In addition, it designates an Executive Agent, the National Archives and Records Administration, a responsibility that was delegated to ISOO.

Initially the primary question being asked by practically all federal agencies was, "Why is a CUI program necessary at all? Perhaps even a cursory examination of federal agencies' handling of controlled but unclassified information would show the diverse and complex systems now employed to protect this type of information: For Official Use Only (FOUO), Sensitive but Unclassified (SBU), and Sensitive Security Information (SSI), just to name the three most prominent. As it turns out, there are in excess of 100 different designations for sensitive but unclassified information throughout the Executive Branch, and there are over 100 different methodologies employed by agencies and major components to protect this information. All

these different information types and names and all these protective measures have resulted in the evolution of some imposing information sharing barriers. Further, upon discussions with many agencies, it became instantly clear that many would resist, or at least be reluctant to share this information with other agencies due to a myriad of protective standards. Thus, the CUI program is fundamentally an information security reform initiative that establishes a baseline of protections to which all agencies within the Executive Branch will adapt in order to reach the ultimate goal of an effective and efficient information sharing posture.

Executive orders typically have an implementing directive to provide additional details on requirements and practices. In the case of the CUI program, its soon to be published implementing directive is 32 C.F.R., Part 2002, (the Implementing Directive), which takes a three-page executive order and explains exactly how CUI is going to protected under this program. It covers key tenants of the program, such as physical protection, protection in the electronic environment, safeguarding and destruction standards, and sharing procedures. One of the most frequently asked questions relative to this new directive is under what circumstances was it developed. It was envisioned and developed in consultation with many Executive Branch agencies, just as was prescribed by the executive order. Essentially what that entailed was a series of data calls, working groups, and discussions with Executive Branch agencies through which a number of questions were asked and answered, such as what information is being protected, why is it protected, and how is it protected. The answers to those questions formed the implementing directive that will soon govern the methodology for achieving the objectives of the Order. It represents a standard to which the agencies feel they can adapt, in that it provides a level of consistency throughout Federal Government agencies, which will eventually also apply within non-federal organizations. The guiding principle of the program is to emphasize the unique protections prescribed in law, regulation, and government-wide policy. There are two kinds of laws and regulations in this area: one identifies a type of information and requires that it be protected; the other identifies a type of information and states exactly how it must be protected. Therefore, the CUI program has two mission objectives: to define protection where the law or regulation is vague and to affect protection where the laws and regulations are uniquely prescriptive. For example, privacy act information is governed by a specified authority. The law is explicitly prescriptive as to how this information should be handled, and those protections, designated as "specified," remain under the CUI program.

The implementation E.O. 13556 through its Implementing Directive is not prescribed for a specific date. Rather, implementation of the CUI program takes into account that each agency has a unique mission and handles unique information types, resulting in special circumstances when it comes to implementing the program. The drafters of the executive order realized that the CUI program could not be implemented overnight. Implementation needs to occur in phases. A graphic representation of this phased implementation begins by prescribing "day zero" as the effective date of 32 C.F.R., Part 2002. ISOO expects it will be finalized sometime within the next two months; it will be released through the Office of Management and Budget (OMB) as a publication in the *Federal Register*. Implementation will be accomplished with a series of 180-day milestones that extend for two years in the future. The initial milestone is for policy. Within 180 days of the release or the effective date of the regulation, agencies are expected to develop and publish their specific policy that implements ("adopts") the CUI program. This is no easy transformation, as agencies must modify and/or rescind all unclassified information policies they

currently have so that they point to the CUI program. For example, those agencies that now use the acronym "FOUO" will, in the future it, refer to "CUI," which in turn will align with the formal definition of controlled unclassified information. The next major increment is to be training. This too will be a major undertaking, as it will touch every employee in every agency. Furthermore, it is to be an all-hands type of training event, to encompass not only awareness training but specified training as well. That is, training will cover both types of laws and regulations described previously. With regard to systems, agencies must, in the first 180 days, assess current configurations as they relate to the standards identified in the implementing directive; that is the moderate confidentiality impact value, which equates to a series of security controls on how to configure and protect a computer system. (Agency information officers and information technology personnel already understand this to be in accordance with National Institute of Standards and Technology Special Publication 853 (NIST SP-853).)

Next, Mr. Riddle provided information about the CUI registry, describing it as a catalog of information types that make up CUI. The E.O. defines CUI as any information for which a law, regulation, or government-wide policy requires some level of protection or dissemination control. The registry includes 23 main categories and 84 subcategories of information types that are considered CUI information. Mr. Riddle noted that the idea of basic and specified CUI is something that speaks to the structure of certain laws. Some are vague and some are very prescriptive, and the CUI program recognizes both. The CUI program office in ISOO will ensure that those regulations are followed. So ISOO's mission with regard CUI is two-fold, as it must ensure that all Executive Branch agencies implement the program under the Implementing Directive, as well as ensure that these same agencies follow all regulations that apply uniquely to their specific organization. The Order was created because of the myriad of inconsistencies in handling sensitive but unclassified information throughout the Executive Branch, resulting in inefficient and ineffective information sharing practices. Information sharing standards have always been linked to "need to know" in the classified world, and under CUI, this same general concept is known as "lawful government purpose." The fundamental difference between the two is that the latter leans more aggressively towards sharing.

There will, of course, be marking requirements that govern CUI information, the primary purpose for which is identification of the sensitivity of the information. ISOO is in the process of developing a detailed handbook that will show the user community—both federal agencies and non-federal entities—every conceivable CUI marking requirement. It is to be released with the publication of the Implementing Directive. Legacy information (FOUO, SBU, SSI, etc.) in the CUI environment includes everything that was marked prior to CUI and which will, during this transition, coexist with the new registry terminology. However, under CUI, legacy terminology practices and markings are to be phased out completely within five years of the release of the implementing directive. There are clear safeguarding and destruction standards included in the Implementing Directive. These and the markings for CUI were thoroughly and exhaustively debated within a CUI Advisory Council, which was composed of about 28 agencies. The agencies all offered very strong opinions on how information should be safeguarded, marked, and destroyed. The Implementing Directive is the result of the work of this group.

The CUI registry, which was initially published approximately six months subsequent to the issuance of the E.O. 13556, can be found online at http://www.archives.gov/cui. The registry is not only a catalog of CUI categories and subcategories, but it also describes what unclassified information the government should be protecting today. This is important because right now, across the Executive Branch, there are information types that are protected that cannot be linked to law, regulation and government-wide policy. That's where the work needs to be done. We need to identify what is being protected and ensure that it can be linked to this online registry and the laws and regulations that are found there.

Mr. Riddle noted that the information he provided at this meeting is a snapshot of a very detailed presentation that the CUI program office provides to Executive Branch agencies that describes the steps the agencies should be taking with regard to program implementation. The purpose of the briefing at this meeting is to set the expectation of what agency effort is going to include. From a policy standpoint, agencies will be modifying and rescinding all policies that prescribe protective measures for sensitive information. That is not as easy as it sounds because a lot of agencies probably have five to ten policies that identify an information type and indicate how to protect it. All those policies need to be aligned with the CUI program. From a program management standpoint, this means that somebody inside of an agency needs to be leading the effort to implement this program. ISOO has issued guidance to agencies which, among other things, reminds them of the requirement to designate a senior agency official and a program manager to administer the program and report implementation planning efforts.

Mr. Riddle reported that the CUI office is developing a series of training modules to be released within 180 days of the issuance of the implementing directive that will assist agencies in their efforts to train their personnel. The training will provide an introduction to the key elements of the CFR, including how to protect CUI, but that isn't going to be all inclusive. Agencies still have to include elements such as incident reporting mechanisms, key points of contact, and any marking requirements that are stipulated in their policy documents. From a physical safeguarding standpoint, agencies are generally affording sensitive information a degree of protection, described in the implementing directive as a controlled environment, wherein a mechanism is in place to prevent unauthorized access. From an implementation standpoint, agencies will need to perform an inventory of what they are currently doing to protect this information. Most are already doing so, and it is probably highlighted in some kind of policy or procedure that requires it to be secured behind a locked a door or protected using the Personal Identity Verification (PIV) or Common Access (CAC) card system to control access electronically. However, agencies need to identify this system and make certain it is highlighted it in policy as part of the CUI implementation plan. Also, agencies need to codify the number and type(s) of systems they have and how they are currently configured. Those that do not meet the requirements described in the implementing directive need to be targeted for inclusion in their implementation plan. From an incidents and violations standpoint, all agencies understand that not all their personnel are constantly vigilant in the protection of information. Both federal and non-federal entities need to investigate strengthening their incident reporting mechanisms and mitigation measures with regard to CUI information types. From a self-inspection standpoint, agencies will be required to develop a system or methodology to evaluate the effectiveness of their own CUI programs, and this self-investigatory process will include an examination of policy documents, training, incidents and violations, and every aspect of the CUI

program, so that the agencies can report these results to ISOO, which has an ongoing responsibility to report to the President on agency implementation efforts. Finally, agencies that issue contracts and agreements that relate to CUI functions will need to examine such agreements as a part of an implementation planning activity to ensure that the standards that are being conveyed to non-federal entities align to the standards of the CUI program.

Ms. Joan Harris, Department of Transportation, inquired about the status of the Implementing Directive. In response, Mr. Riddle noted that on July 1, 2016, OMB issued "OMB Circular A-11," which speaks to budgeting for the upcoming year for the Federal Government and the Executive Branch, calls for agencies to consider the implementation of the CUI program in their upcoming budgets. Although the language is not strong enough to make this a requirement, it is significant in that that's the very first time that CUI has been mentioned in the OMB circular. A lot of agencies took this as an indicator that, indeed there will be a CUI program. It is not a matter of years: it is a matter of months until when this effort will begin.

Mr. Wight asked about how the CUI program will be applied to SLTPS entities. Mr. Riddle noted that when the Federal Government shares information with SLTPS entities it is typically done via agreements. In the implementing directive "agreements" is a very broad term that can mean contracts, agreements, or sharing agreements. As part of their CUI implementation activities, agencies will need to examine all agreements wherein they identify an information type and they prescribe how to protect it. There will be some differences, and there may be a little bit of growing pains in the development of the standards that are being pushed out. For example, an information technology (IT) system that will be applied to a non-federal entity, must be protected it in a particular fashion, and, in the future, that fashion will align with the standards in the new implementing directive. For non-federal entities, NIST Special Publication 800-171, "Guidelines for Protecting CUI in Non-Federal Systems and Organizations," which references the implementing directive, provides the standards" So, if agencies have agreements with SLTPS entities that relate to housing CUI on their systems and providing some sort of service for the government, the NIST document will be referenced as the new standard. That standard is a reflection of the moderate confidentiality impact value. It is a very strong standard in that the requirements listed in the aforementioned NIST special publication cannot be tailored. This is unlike the IT standards in the government, with which federal agencies have a lot of freedom as far as what they can tailor from a security control catalog and still maintain the assertion that they're at a particular safeguarding level, as in the case of multifactor authentication. This is a requirement for federal agencies to implement, but a lot of agencies, due to funding and risk management decisions, have elected not to implement this control. However, this control, which is a very strong one, and which ensures the protection of a lot of information, is a hard requirement in the NIST Special Publication 800-171 that non-federal personnel must meet in some way. Non-federal entities are not actually being told that they have to get a PIV or CAT card. They are being told that they need to implement these measures because they are federal requirements.

Mr. Wight asked if there will be CUI training for SLTPS partners. Mr. Riddle responded that training that will be posted on ISOO's website and will be available for download by all, including SLPTS, non-federal entities, and contractors. In addition, one of the services ISOO provides both Executive Branch and non-federal entities is on-site training. So, if anyone desires

a range of training, or a special one-day session or seminar, reach out to ISOO and we will gladly visit you to provide CUI training. The Chair then opened the floor for any general forum questions or discussions.

IV. General Open Forum/Discussion

Mr. Wight then raised some issues for the Committee's consideration. First, he suggested the development of a working group to examine the question of formalizing the TS/SCI clearance process for fusion center analysts. He reminded the Committee that the fusion centers have a national asset of almost one thousand talented, critical thinking analysts at the state and local level. Many of them receive the same training as members of the Intelligence Community (IC) and some receive even more. These analysts need the same level of security clearance as their federal counterparts so they can access and share information they need and effectively perform their duties. This access would allow them to attend important meetings, such as with a Joint Terrorism Task Force, an IC group, or the National Counterterrorism Center. This access is particularly important in the realm of cyber security. He praised DHS leadership for its support for providing such clearances. He also counselled that it is also important to ensure that the process to grant such clearances continues in the future and wondered about the extent to which it has been formalized, especially as some of the primary leadership is subject to change in the not too distant future with a new Presidential administration. Mr. Wight's second proposal was to find ways to strengthen the ability to access and process intelligence information at the TS/SCI level. He noted that analysts need to be able to get accounts and have access to systems other than by being on detail to a Federal agency. While there are some workarounds for that, not every agency can afford to detail someone out and have the ability to do that. What is needed is to be able to get those clearances independent of such details or otherwise obtain the accounts and access to the information. He indicated that it was his understanding is there is no policy on this issue. Secondly, in terms of SLT analysts being able to process and share TS-level information, unlike Secret-level information where there is access via the HSDN, there is no TS equivalent. He suggested that a working group on this issue might be a proper forum in which to explore the possibilities for increased access. Finally, Mr. Wight raised a third issue: concern that the deactivation of HSDN accounts comes after a relatively short period of non-use. He understands that HSDN accounts are deactivated after they have not been accessed for 20 days. He expressed that while he can understand the reasoning for that period of time, for SLTT analysts who do not access the systems daily, the 20-day period can easily elapse (for example, if the account is not used for a week, then an analyst is out on leave for a two-week period), then the account is deactivated, and classification training—which is a cumbersome process with a significant wait-time for a class—must be retaken in order to get the account reactivated). He inquired if some mechanism could be found where we could extend that time for state and local analysts. (See Attachment 2 for the Action Items from this meeting.)

IV. Closing Remarks and Adjournment

The Chair thanked everyone for attending the meeting and for their contributions. He encouraged all to reach out to him, Greg Pannoni, or the ISOO staff with any ideas they have for topics, presentations, or areas of concern that might be added to the agenda for a meeting in the future. He then closed the meeting by reminding everyone that the next meetings of the

SLTPS-PAC would be held on Wednesday, January 25, 2017, and Wednesday, July 26, 2017, from 10:00 a.m. to 12:00 noon, here at the National Archives Building. The meeting was adjourned at 11:23 a.m.

Attachment 1

SLTPS-PAC MEETING ATTENDEES/PARTICIPANTS

The following individuals were present at the July 27, 2016, SLTPS meeting:

• William A Cira	Information Security Oversight Office (ISOO)	Chairman
• Greg Pannoni	Designated Federal Officer (DFO) (ISOO)	DFO
• Lee Wright	SLTPS Entity Representative	Vice-Chair
• Charles Rogers	Department of Homeland Security (DHS)	Presenter
• Mark A. Brooks	Department of Energy	Member*****
• Michael C. Layton	Nuclear Regulatory Commission	Member*****
• Joan Harris	Department of Transportation	Alternate Member*****
• Richard L. Hohman	Office of the Director National Intelligence	Member*****
• C. Elaine Cummins	Federal Bureau of Investigation	Member
• Leo Masciana	Department of State (DOS)	Member
• Glenn R. Bensley	Department of Justice (DOJ)	Member*****
• Bradley Johnson	DHS	Attending
• Richard Licht	SLTPS Entity Representative	Member*****
• Kevin Donovan	SLTPS Entity Representative	Member
• Mark Jay Schouten	SLTPS Entity Representative	Member*****
• Jeffery Alan Friedland	SLTPS Entity Representative	Member*****
• James Dewey Webb	SLTPS Entity Representative	Member*****
• Christopher A. Forrest	Department of Defense	Attending
• Derrick Broussard	DSS	Alternate Member
• Joshua A. Ederheimer	DOJ, Office of Tribal Justice	Attending
• Nikki Warren	Central Intelligence Agency	Attending
• James Harris	Holland & Knight LLP	Attending
• Mark Riddle	ISOO	Staff/Presenter
• Kathy Branch	ISOO	Staff
• Robert Skwirot	ISOO	Staff

***** Participated via teleconference

Action Items from SLTPS-PAC Meeting, July 27, 2016

1) The SLTPS-PAC Staff should establish a working group to explore providing JWICS access for fusion center personnel and other state, local, and tribal personnel without the requirement of being detailed to a federal agency.

2) DHS should consider extending the time period for deactivation of an HSDN account beyond the current 20-day period.

3) DHS should consider formalizing and making permanent the security clearance process.

Controlled Unclassified Information

Executive Order 13556

Shared • Standardized • Transparent

MARK.RIDDLE@NARA.GOV

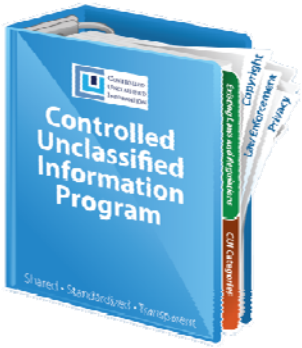
CONTROLLED
UNCLASSIFIED
INFORMATION

Information Security Oversight Office (ISOO)

Executive Order 13556

- Established CUI Program
  - In consultation with affected agencies (CUI Advisory Council)

- Designated an Executive Agent (EA) to implement the E.O. and oversee department and agency actions to ensure compliance.
  - National Archives and Records Administration
  - **Information Security Oversight Office**



- An open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy

Why is the CUI Program necessary?

Executive departments and agencies apply their own ad-hoc policies and markings to unclassified information that requires safeguarding or dissemination controls, resulting in:

An inefficient patchwork system with **more than 100 different policies and markings** across the executive branch	Inconsistent marking and safeguarding of documents	Unclear or unnecessarily restrictive dissemination policies	Impediments to authorized information sharing

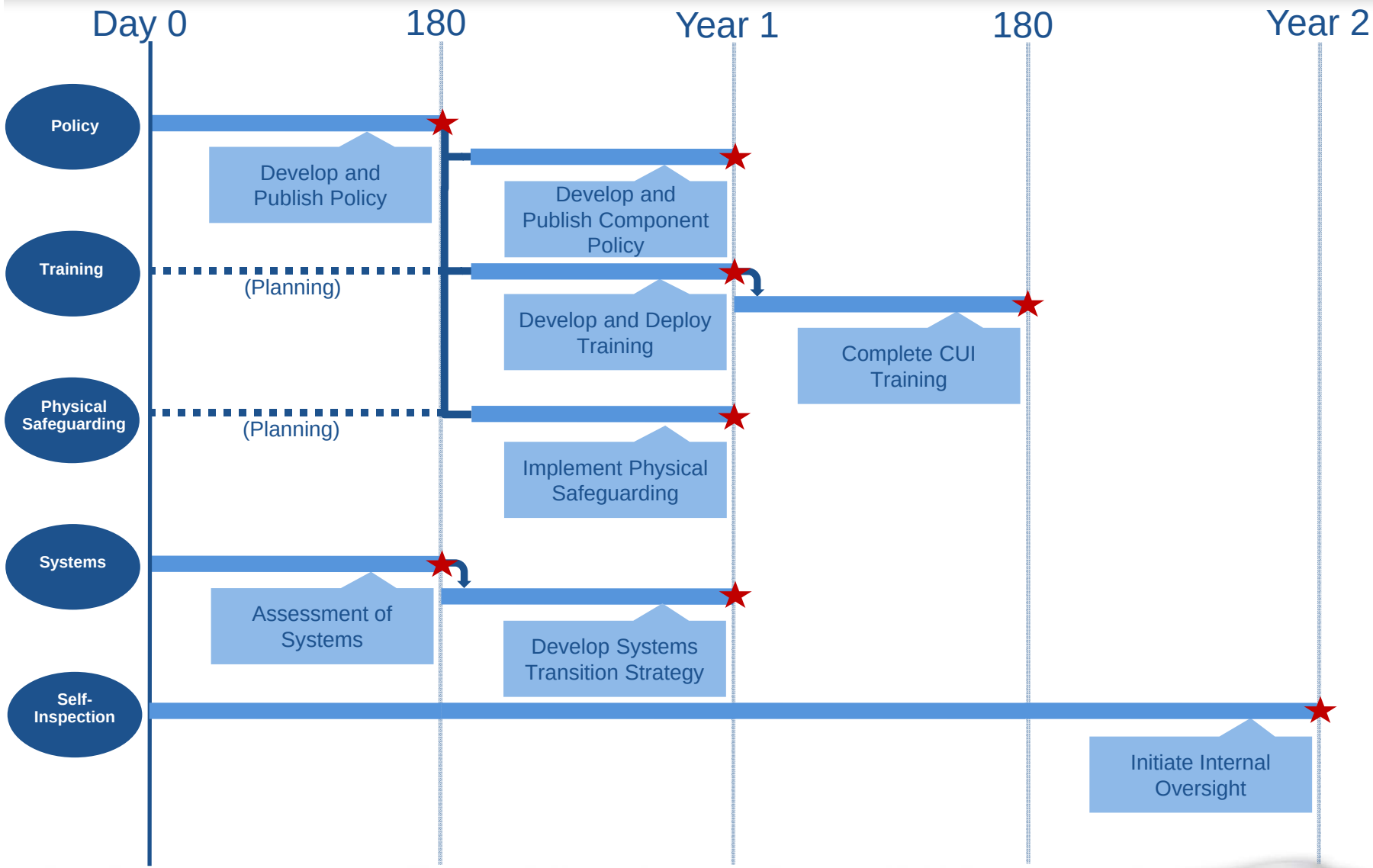
32 CFR 2002 (2016)

- Implements the CUI Program
  - Establishes policy for designating, handling, and decontrolling information that qualifies as CUI

- Describes, defines, and provides guidance on the minimum protections for CUI
  - Physical and Electronic Environments
  - Destruction
  - Marking
  - Sharing

- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)
  - These protections must continue as described in the underlying authorities.

Implementation of the CUI Program



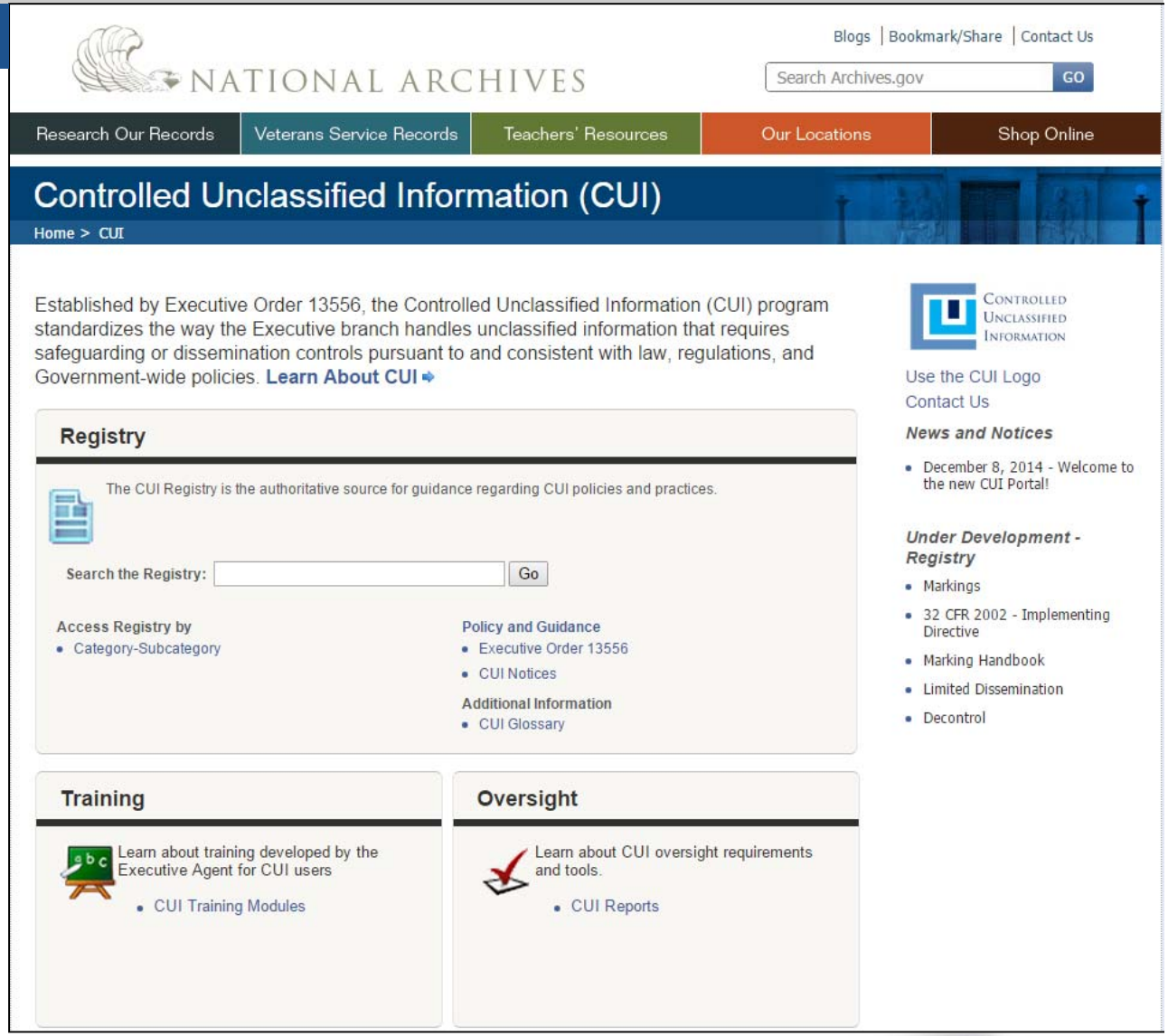
Understanding the CUI Program

- CUI Registry
- CUI Basic versus CUI Specified
  - Specified Examples
- Limitations of Agency Policy
  - CUI Specified Category/Subcategory Requirements
- Sharing and Lawful Government Purpose
- Marking CUI
  - Handbook
  - Coversheets
- Legacy Information
- Safeguarding
- Destruction

Online Registry

http://www.archives.gov/cui

- 23 Categories
- 84 Sub-categories
- 315 Control citations
- 106 Sanction citations



Recommendations for Implementation

- Policy
- Program Management
- Training
- Physical Safeguarding
- Systems
- Incidents
- Self-inspection
- Contracts & Agreements (agencies and non-federals)