STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR POLICY ADVISORY COMMITTEE (SLTPS-PAC) JANUARY 25, 2017

SUMMARY MINUTES OF THE MEETING

The SLTPS-PAC held its twelfth meeting on Wednesday, January 25, 2017, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. Mark Bradley, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on April 25, 2017.

I. Welcome, Introductions, and Administrative Matters

The Chair welcomed the attendees. He advised that he would proceed slowly and methodically at this meeting because, although he helped with the drafting of the executive order that created this committee, this was his first SLTPS-PAC meeting. He introduced himself to the participants, noting that his position as Director of ISOO is his fourth with the Federal government. He came to ISOO from the Department of Justice, National Security Division, where he worked on a variety of issues including the Foreign Intelligence Surveillance Act, intelligence community guidelines, and all sorts of boards and panels. Before that, he was Senator Daniel Patrick Moynihan's legislative director on the Hill. He took a segue for eight years as a criminal defense lawyer in Washington, D.C., and he was in the CIA in the 1980s. The Chair 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 advised them that the meeting was being audio-recorded.

The Chair noted the departure of SLTPS-entity members Kevin Donovan and Lindsey Johnson last year and welcomed new members Agnes Rainer Kirk, who is the Washington State Chief Information Security Officer, and Jessica Davenport, who is a senior management analyst supervisor with the Florida Department of Law Enforcement at the Florida Fusion Center. Both were participating via teleconference. On the Federal side, the Chair indicated that Lou Widawski, from the Department of Transportation (DOT), is retiring at the end of the month. DOT will identify a new member to the committee when the replacement for Mr. Widawski is selected. Michael Layton, of the Nuclear Regulatory Commission (NRC), will no longer be able to serve on the SLTPS-PAC, and Darryl Parsons, the NRC alternate, will continue to represent the NRC on the committee until a replacement for Mr. Layton is named. The Chair asked the attendees and participants to introduce themselves. He then 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 the attendees and participants.)

II. Old Business

Updates from the DFO

Greg Pannoni, DFO, began by reminding the membership due to budgetary limitations, it continues to be necessary to offer a teleconference capability. No funds are available to pay for travel for those who are out of the DC area. And on that point, he thanked Rich Licht for travelling from New York to attend in person. Mr. Pannoni then turned to the three interrelated action items from the last SLTPS-PAC meeting and asked Charlie Rogers, Vice-Chair, Department of Homeland Security (DHS), and Chief of the DHS's SLTPS Management Division, to join the discussion.

The first action item concerns Joint Worldwide Intelligence Communications System (JWICS) access for Fusion Center personnel and other state, local, and tribal personnel without the requirement of being detailed to a federal agency. Mr. Pannoni pointed out the executive order sets the basic threshold at the Secret level for access to classified information and for information systems that process or store classified information. Then there's a more stringent threshold essentially on a case-by-case basis with each sponsoring agency, to gain approval for access above Secret, to include Top Secret, Sensitive Compartmented Information (SCI) and Special Access Program information. The information system requirement is similar. If there is to be physical custody above the Secret level, the order speaks to having a DHS person or another federal government executive agency person full-time to manage the operations and controls of the fusion center. So, a person does not have to be detailed to a federal agency in order to gain access to JWICS, although it is a high threshold. There are much more stringent controls to access JWICS. Unfortunately, there has been transition with representation from Office of the Director of National Intelligence (ODNI), so, there has not been an opportunity to have a thorough, lengthy discussion with respect to JWICS access, which ultimately is under the ODNI's authority. Nevertheless, it is still necessary to pursue this issue because the SLTPS program is about consistent safeguarding and enhancing the sharing of classified information. Mr. Pannoni indicated that he shared the concern and understanding that there is, at least in certain instances, a need for access to higher levels above Secret, and he noted that access has happened in some instances, as Mr. Rogers has indicated. Mr. Pannoni then indicated that, unless the DNI representative wanted to comment on this—which he did not—he would turn to Mr. Rogers to continue.

Mr. Rogers began by discussing the second action item, which related to extending the length of inactivity that would prompt deactivation of a Homeland Secure Data Network (HSDN) account. The understanding at the previous meeting was that the period was 20 days. Mr. Rogers indicated that after research on this issue, he learned that the period is 30 days. He also learned that if the account is not used for 30 days, it can be reactivated for another 60 days, provided that the individual had set up challenge questions with the help desk. So, this provides the user with up to a 90-day grace period, which should be sufficient. Mr. Rogers also confirmed that this period is the same for DHS's internal SCI system. He indicated that some people may have been canceled out at 30 days because they weren't aware of the challenge questions.

Mr. Rogers addressed the third action item, which related to formalizing and making permanent the security clearance process because there were concerns if the processes were going to continue with the new administration. He noted that the Office of Intelligence and Analysis (I&A) at DHS vets and sponsors a select number of people for SCI access and his Directorate grants their clearances. I&A has formalized its processes and forms. The implementing directive for the SLTPS program, which is national policy and which was approved by this committee, sets the criteria for SCI access for state, local, tribal, private sector. The I&A nominating forms mirror the policy exactly. Individual access is on a case-by-case basis. There is a requirement that the individual identify an SCI facility (SCIF) or a location in which he or she can access the information, because state facilities cannot have SCI under their own management. They can have SCIFs, as do New York City and Chicago, but the SCIFs are managed by DHS. Another requirement is that they make an 18-month commitment. The implementing directive to Executive Order 13549, "Classified National Security Programs for State, Local, Tribal and Private Sector Entities," requires "a sufficient duration," to justify the expense, which I&A has set at 18 months. Mr. Rogers summarized that this process is articulated in policy. It's in the national policy and in the I&A policy, and I&A indicated that it is not being eliminated. Mr. Pannoni added that there is language in the directive about a "demonstrated and foreseeable need." Mr. Rogers affirmed this. He noted that there is a wide range of personnel who can get SCI access if they have a connection to homeland security and a federal counterterrorism mission and they have the ability to influence and provide expertise to the process.

Mark Schouten, SLTPS-entity member, who serves as the Director of the Iowa Department of Homeland Security and Emergency Management, asked the difference between JWICS and HSDN and whether the processes for obtaining access to each of those are similar or different. Mr. Rogers replied that JWICS is an SCI-level system managed by the intelligence community (IC) and the HSDN is a Secret-level system that DHS manages and other federal agencies access. The requirements for access to the systems are based upon the individual's clearance level and whether the individual has SCI access. So they are two separate systems with two separate requirements for access: one is an IC system; the other is a collateral DHS system. Tip Wight, SLTPS Vice-Chair added that, he has been told, the only way to get a JWICS account is to be detailed to a federal agency. He noted that this is one of the open action items and that, for state and local personnel, unless they are assigned to a joint terrorism task force or something like that, there's no way to get a JWICS account at present.

Mr. Schouten added, in Iowa homeland security, he's not so concerned about JWICS. His office would like a direct connection to the HSDN, which he assumed would be through Mr. Rogers' office and perhaps easier to get than JWICS. Mr. Rogers responded that it is relatively easy but it is not exactly through him. The HSDN requires that a secure facility be built to house the network or the system, which incurs a monthly cost just to manage it. There is a personnel cost to manage that alarmed room; so, there's a whole security overlay that goes with it. Access to these systems are basically endorsed and nominated by I&A. Because of the significant budgetary and security footprint, I&A limits the number of locations that get HSDN. For the most part, access is provided directly to fusion centers, with the expectation that people could work with the fusion centers to gain access to the network there. So getting access to the network is not that difficult. It's a matter of negotiating with I&A, having the appropriate clearance, and negotiating with the fusion center. However, to get access at your location would entail a very significant outlay, and I&A would make that decision. Mr. Schouten responded that he understands this. His office has a memorandum of understanding with the National Guard to use its SCIF. However, they are having some difficulty getting regular access to HSDN for their critical infrastructure person working cybersecurity issues. So, they are looking at alternatives in the interest of sharing information and sharing it better.
Mr. Schouten reflected that, as Mr. Wight said at the last meeting, cyber puts all of the information sharing in a different light, and it is essential to make sure that information is getting out.

Mr. Wight interjected that he agreed completely. He lamented that one of the reasons for his push for the TS/SCI access for fusion centers is because much of that cyber information is at the TS level. He added that it sounded to him like Mr. Schouten's office was not co-located with the Iowa Fusion Center. Mr. Schouten answered that they were not. He indicated that they recently pointed out to their DHS intelligence contact that not all states have their homeland security advisor under Department of Public Safety, which also controls the Fusion Center. Quite often, the fusion centers are outside of the homeland security advisor's office and there is not the automatic linkage that DHS may assume is happening. The result is that the information sharing isn't perhaps as good as it could be or as it would be if the connection were direct. Not all states are created and/or organized the same. There are, maybe, 15 states where the homeland security advisor is not connected directly with the fusion centers. Information may not be shared as well at this level in some states. Mr. Rogers agreed that there is diversity in the way in which states are configured. He added that I&A is prioritizing where the resources are going because the costs to construct, manage, and operate a room that houses HSDN are significant. He suggested that a guest speaker from I&A might be brought to a meeting to discuss this process for their field operations. Mr. Wight added that in Washington, DC, the issue was resolved, because the fusion center, which originally started in the police department, was relocated to the Emergency Management Agency, where it is now co-located with the homeland security advisor. The Chair and other members agreed that there would be value in having an I&A person to brief on the process. The Chair then turned to Mr. Rogers to provide an update on the implementation of the SLTPS security program.

III. New Business

A. SLTPS Security Program Updates

Mr. Rogers began by noting that in the SLTPS security program, there is a big emphasis on the fusion centers. There are different aspects to the program to ensure that we're providing the support we need to provide and that classified information at those locations is protected sufficiently. DHS has a compliance review program to oversee that this occurring. The program was implemented in late 2012. The SLTPS Management Division performs the compliance reviews and also makes special visits on other occasions. I&A also conducts assistance visits. There are about 15 compliance reviews each year, but the number has varied from a low of 11 to a high of 19. Since the program was implemented, Mr. Rogers' division performed a total of 76 compliance reviews with the fusion centers. So, it's a pretty robust program.

In another aspect of the SLTPS security program, in accordance with the implementing directive, fusion centers are required to appoint onsite security liaisons who have responsibility for managing the classified program and managing the secure room at their location. There is an ongoing training program to ensure that the security liaisons maintain an appropriate level of expertise to carry out their duties. There are several elements to this training program. There is a webinar program, which includes about two hours of training. It provides an opportunity to go over the policy and procedures and to answer questions. Mr. Rogers' division does about 10 of those a year. In 2015, they did 10 webinars and trained 81 security liaisons, and in 2016 they also did 10 webinars and trained 80 security liaisons. Compliance reviews provide another opportunity for training, although it is web-based training, not in-person training. There is also another training program that is funded by I&A and consists of quarterly training events that bring newly appointed security liaisons to DHS headquarters for about two and a half days of training. The Office of Security, I&A, and other offices within DHS participate in this training. Although, due to a funding issue, there were none of these events in 2016, one has already been held in 2017 that brought in four liaisons for training.

Mr. Rogers turned to personnel security. He reported that DHS has issued approximately 2,100 private-sector clearances under EO 13549. These are subject matter experts who have been primarily granted Secret clearances. There are another 5,500 state and local personnel who are cleared through the program. The current combined private sector and state and local clearances is about 7,500 people. Over the years approximately 2,200 clearances have been deactivated through separation, or because the individual is no longer eligible or no longer works for the company or in the infrastructure that the company represents. These personnel have been debriefed.

Mr. Pannoni inquired regarding the number of SCI clearances. Mr. Rogers responded that the number of state, local, and private sector SCI clearances stands at 370. Mr. Wight noted that that number would not represent all the state, local, tribal, or private sector personnel that are cleared to the SCI level. That's only through DHS. There are personnel like him who are cleared through the Federal Bureau of Investigation (FBI). So, there are other sources. Mr. Rogers agreed.   He stated that under the executive order, agencies are able to clear whoever they need to. The DHS is not solely responsible for all state and local clearances. FBI frequently clears personnel and also has a clearance turnover and debriefing process.

Mr. Schouten added his perspective from a state like Iowa where the security liaison is part of homeland security and emergency management, not part of the fusion center. The security liaison there is a former NSA employee. Mr. Schouten's office works with its personal security assistant (PSA) to do the private sector clearances, and particularly now, with cyber, they are reaching out to the lifeline critical infrastructure folks and talking with their PSA, trying to get higher level clearances for them. He indicated that he is inclined to agree with Mr. Wight that the Secret clearance is probably not enough for some of them. He spoke of a utility representative who is part of the Kansas Fusion Center and has Top Secret/SCI. Mr. Schouten expressed his belief that, from the cyber standpoint, if you're really going to be getting into the attack analysis, then SCI is probably necessary. Mr. Rogers affirmed that the PSAs do nominate a lot of private sector personnel. There are two nominating activities in DHS: one in I&A and one in the National Protection and Programs Directorate (NPPD), which has the private sector infrastructure protection mission. So there are two nominating elements that feed into the Office of Security, which vets and validates the requirements.

Mr. Schouten continued that from his standpoint in Iowa his office has taken the approach that they need a number of people with clearances, but they request them judiciously, particularly among the 300 to 400 municipal utilities there are in the state, so that one or two would represent that sector or the gas systems or the water and wastewater reclamation systems. His office talks to the organized groups for these sectors and asks for one or two people to nominate with the PSA to get a clearance, because they think merely giving them a nondisclosure agreement at the time of an incident is probably not going to be adequate. If they are to be prepared, it is necessary to provide them some classified threat information. Critical infrastructure protection changed after the Russian hack of the power grid in the Ukraine at the end of 2015. He noted that before Ukraine, his office was not nearly as sharply focused on lifeline critical infrastructure as they are now. Having the knowledge that an attack like this is possible, they want to increase these persons' awareness of the threat, and perhaps give them more information about the nature of the risk. But to do so, it is absolutely necessary that they be cleared at, at least to the Secret level to make it worth their time to hear the briefing. Mr. Rogers indicated that Mr. Schouten could contact him and he would try to connect him to the critical infrastructure people in DHS, since it is necessary to establish a relationship with them in order to facilitate any sponsoring of clearances. The clearances would have to have a nexus to a DHS mission and that is what the critical infrastructure people are involved in. They're involved in infrastructure and cyber. Mr. Rogers provided his e-mail address so that he could help facilitate this. Mr. Schouten indicated that this was consistent with what his office is doing. The PSA is handling it. There are maybe four or five clearance requests in process. There will not be more than six. He does not want to burden the system, but he thinks -- and the PSA agrees -- that they will be adding a lot of value to the state by having select members or representatives of critical lifeline industries with clearances so they can hear the nature of the risk. Mr. Rogers and the Chair agreed that this all makes sense. Mr. Schouten added that his office will see how these clearances are processed, noting that he has an idea of how it should be done. The DHS plays a critical role, and information sharing is paramount. He believes that so far it is working really well and that they are taking steps to add significant value to what they do.

The Chair thanked Mr. Rogers and noted the Mr. Pannoni will be joining Mr. Rogers for the next presentation, which will provide an update on the status of an initiative that sets forth the National Industrial Security Program procedures for sharing and safeguarding classified information with certain private sector and other non-federal entities. This is an update to their discussion on this topic at the last meeting.

B. Update on Additional National Industrial Security Program (NISP) Procedures for Sharing and Safeguarding Classified Information with Certain Private Sector or Other Non-Federal Entities

Mr. Pannoni began by noting that he would not recount the discussion from the last meeting on what had occurred to that point with the classified critical infrastructure protection program (CIPP) under the NISP, as it is documented in pages four through six of the meeting minutes. Since then, the President signed the implementation procedures on December 28, 2016, and that's the beginning of implementation. There is a considerable amount of work to be done with responsibility mostly on the DHS side, for the DHS secretary, but also working with Department of Defense (DOD), through the Defense Security Service (DSS). The procedures are designed to streamline the process for sharing and safeguarding classified CIPP information. The vetting, reporting, and oversight mechanisms under this program are less stringent than they are under the traditional NISP program, and that was done deliberately to increase involvement from both parties. They are operating under cooperative research and development agreements (CRADA), which is a contract, and because of this, the process falls under the NISP. With that Mr. Pannoni turned to Mr. Rogers to continue the discussion

Mr. Rogers provided a brief overview of this hybrid program. He indicated that DHS was tasked by the National Security Council, which directed DHS and DOD to work together and to develop an alternative program to facilitate classified information sharing with the private sector. A number of people at this meeting, including Kathy Branch, Keith Minard and Mr. Pannoni, were involved in the long process of negotiation and writing to develop an alternative process that lessened the burden on companies while retaining some of what was determined to be essential safeguarding requirements of any classified information sharing with the private sector. So, the White House did sign it. It has a long name, "Additional National Industrial Security Program Procedures for Sharing and Safeguarding Classified Information with the Private Sector Infrastructure Entities," but it is referred to as the hybrid. Some of the key elements that are waived for this program are that the private sector companies who will eventually get access to classified information would not be required to get a facility security clearance, would not be able to bid on any additional classified contracts, and would not be permitted to store classified at their location. But once they met all the requirements of the program, they could get security clearances that would enable the sharing of classified information. Some of the things that are required to be in place for this classified information sharing to take place are relatively simple, like creating security agreements between DHS and the company. Some are complex, such as establishing a foreign ownership, control, and influence (FOCI) information collection and evaluation process. Mr. Rogers admitted that he does not fully understand all of the complexities of the process and noted that it is going to be a challenge to stand up a full capability in DHS.

Mr. Rogers noted that DHS had internal meetings on December 29, 2016, the day after the hybrid was signed. DHS met with the DSS on December 13 and is working with them to help gain an understanding of what is involved in establishing this capability in DHS. The two agencies have signed a Memorandum of Understanding for this. DHS has detailed a person to DSS to begin to acquire that knowledge. DHS also assigned three other people to meet intermittently with people at DSS and collect documents. There are ongoing conversations on this. DHS also plans to meet with the Nuclear Regulatory Commission (NRC), because it has a program from which they can learn. Mr. Rogers added that, in order to implement this program, DHS had to become a cognizant security agency (CSA) under the NSIP. This was facilitated by EO 13691, “Promoting Private Sector Cybersecurity Information Sharing,” February 13, 2015, and the DHS had been waiting since then for the hybrid to be approved.

Mr. Minard, DSS, indicated that DSS is collaborating with DHS to help them through the process. He noted that it is going to be a long process to understand FOCI analysis and mitigation. There are a lot of procedures that are required to be put in place, such as information collection approvals from the companies or entities that they are going to oversee and provide access to classified data. Also, a key point, as Mr. Rogers mentioned, is working with the NRC. The NRC has some FOCI and mitigation processes that might be more similar to what DHS needs to do, so DSS is making sure that they connect DHS with the right communities along the way to start understanding the processes.

Mr. Pannoni asked Mr. Rogers to give the group an understanding of the approximate size of the program today and where we project to be in a few years. Mr. Rogers indicted that there are about 165 companies who have signed these cooperative agreements with DHS with the expectation that they will eventually be able to enter into the program, and certainly there’s a backed-up momentum or backed-up expectation. These companies urgently want to get in the program. We’ve all been waiting for a couple of years for its approval, but we couldn’t build a program without being a CSA, and without having the hybrid process. He expressed that there are approximately 200 companies that are in the background, but the program office in DHS has about a dozen that they urgently would like to be brought into the program. So the plan is that DHS first has to build the capability as quickly as possible to allow them to get some of these companies in the pipeline. He recognizes that DHS cannot put them in the pipeline until they are able to appropriately vet them and appropriately do all the requirements that are necessary for the hybrid. DHS has funding in the 2018 budget—both money and requests for personnel—to supplement this program, but there is no funding for this year and its costs are being borne by other DHS programs. DHS is getting assistance from partners in other CSAs. Mr. Rogers promised an update on progress at the next meeting. The immediate need is to understand all the things that need to be accomplished in order to implement the program, and it is most urgent now to understand the information collection process, the forms, and the FOCI evaluation. There will eventually be an oversight program associated with it, but the focus right now must be on the front end.

Mr. Pannoni added that it is important to know that this is very much insular, these facility security clearances or entity eligibility determinations are restricted to this program, so there’s no reciprocity by which an entity can take the fact that it has been granted this eligibility and start bidding on other contracts that require access to classified information. The entity would have to enter the traditional NISP process in order to do that. Mr. Rogers agreed and noted that the real purpose of the program is to facilitate classified cyber information sharing. The plan is to enable DHS and other federal agencies to share threat and risk information and to mitigate risk with companies by having classified information sharing. The companies would not store classified information, but they could have six, eight, 10, or 12 people cleared so that they could get the information they need to protect their networks and to provide expertise to the federal community. DHS is working to bring this about now that it has the approvals to move forward.

The Chair indicated that this is a good start. He then introduced Mr. Wight, the SLTPS entity Vice Chair, to make a presentation on the National Network of Fusion Centers. Colonel (Retired) Lee "Tip" Wight is currently the director of the DC Metropolitan Police Department's real-time crime center. He was the Director of DC's fusion center from 2013 to 2016 and also served as the vice president of the National Fusion Center Association (NFCA) from 2014 to 2016. His briefing, entitled "Fusion Centers and National Strategy, National Asset, Local Resource," describes state, local, tribal, and territorial fusion centers and the National Fusion Center Network.

C. Fusion Centers and the National Strategy: National Asset, Local Resource

Mr. Wight started by noting that many people do not understand what a fusion center is or that a network exists among all 78 of them. He noted that many do not know how to leverage these resources and are unaware that there is a national strategy for the fusion centers. The intent of the strategy is to standardize the delivery of this capability to state, local, tribal, territorial, and private sector entities as well as allowing the federal government partners to leverage the capacity. So, the purpose of the briefing is to increase the understanding of all of these things. Mr. Wight explained that when the presentation uses the term "local resource" the intent is not just local entities. It encompasses the whole umbrella of state, local, tribal, territorial, and private sector.

Mr. Wight observed that there are a lot of misconceptions as to what a fusion center is. They are not federally owned or controlled. Rather they are very much owned by state, local, tribal, or territorial entities. They conduct regional intelligence and information sharing. Each one is unique, although some of the things such as the national strategy and the FEMA grant program, and the requirements under DHS I&A for reporting and evaluation have standardized them to some degree. They are unique because each jurisdiction wants to tailor the service to its local needs. Some will have an investigative role, such as the Boston Regional Intelligence Center. Mr. Wight's former center, the Washington Regional Threat Analysis Center (WRTAC) in DC, had no investigative capability and was under the rubric of an emergency management agency. All fusion centers are multi-agency but the composition in each is unique. In DC, there were about 50 partner agencies that had a variety of different kinds of relationships, from having a full-time liaison officer detailed to it to virtual connectivity through which conversations were held every couple of weeks at a staff meeting at the end of a phone line. This too varies across the national network. What the fusion centers are focused on will also depend on the jurisdiction. The terms "all crimes," "all threats," and "all hazards" are commonly used. A threat is manmade, and a hazard is something naturally occurring, such as a hurricane or an earthquake. When a center professes to be all-crime, such as the WRTAC did, it is not possible for the center to have an analyst for every possible crime. But, among the 900 trained analysts in the fusion center network, the expertise does exist, and personnel throughout the network reach out to others and benefit from their expertise. Mr. Wight then noted that fusion centers do not duplicate the mission of joint terrorism task forces (JTTF). A JTTF is owned by a federal agency and has a single mission, counterterrorism, whereas a fusion center generally looks at all threats and all hazards, with the exception that some are just law enforcement and homeland security.

Mr. Wight then turned the National Strategy for the Network of Fusion Centers. He noted that after 9/11 and the recognition of the need to share information among federal, state, and local partners, more fusion centers were being established and a variety of reports and guidelines were issued, including various Congressional documents. He traced the origin of the National Strategy to 2013, when Congressman Peter T. King made an assessment of fusion centers that recognized that fusion centers have come a long way since 9/11 and are performing well, but he observed that there was no strategy for them. This assessment led to the NFCA to begin work on the National Strategy, which was issued in 2014. A copy of the National Strategy can be found on the NFCA website (NFCAUSA.org). The NFCA worked with partners at the National Governors Association, Major County Sheriffs Association, Major City Policy Chiefs Association, and other agencies including Fire Service and Emergency Management. The strategy had broad circulation and support as it was developed.

The intent of the document was to define the strategy of the national network, to identify a path forward for it, to discuss its effectiveness, and to demonstrate what an asset it is. The mission of the network is to use the unique capabilities that are available. Many of the 900-plus trained analysts are former federal IC personnel that have either retired or decided to work closer to the mission at the state and local level and to be able to leverage their skill set. Mr. Wight returned to a point he previously made about TS/SCI clearances, insisting that it makes no sense that when someone takes off the federal hat with a TS/SCI clearance and goes to work for a state and local agency, the next day the individual is only cleared to a Secret level. The strategy is aimed at helping to protect the homeland and discusses this in terms of receiving, analyzing, disseminating, and gathering threat information and intelligence in support of the state, local, tribal, territorial, and private sectors as well as the federal efforts to protect it.

Mr. Wight reported that this national network has become a multidisciplinary, all-crimes, all-threats, all-hazard, information sharing network that protects the nation's security while safeguarding the privacy, civil rights, and civil liberties of our citizens. He noted that this last point is something that is really key. The network is a decentralized, distributed, self-organizing national asset. Mr. Wight emphasized that it is self-organizing. There is no federal directive that all these entities participate together, but they do, and the network functions quite well. There are 78 fusion centers, including three in federal territories: the US Virgin Islands, Puerto Rico, and Guam.

Mr. Wight turned to the four goals of the National Strategy. The first goal is to uphold public confidence, which involves protecting the information, privacy, civil rights, and civil liberties, and it is key to all the work that the fusion centers do. The second goal is to support engagement and expand the network of each fusion center. When Mr. Wight was at the WRTAC, he had 50 partner agencies. Trying to expand the breadth and depth of each fusion center's individual network is the focus of goal two. Goal three is to strengthen the integration and interconnectedness of fusion centers. It is about enhancing the national network. And, goal four is to increase the overall connectivity between fusion centers and the federal government. It is the vertical piece of connecting with the federal partners and strengthening the information sharing efforts that go along with that.

Mr. Wight then discussed the objectives to be attained in reaching the four goals. Of the 37 initiatives that support this strategy, he highlighted some of the key objectives under each of the four goals. Under goal one he cited objective 1, “privacy, civil rights, and civil liberties protections;” objective 2, “enhance and sustain a trusted network;” and objective 3, “promote fusion center accountability and transparency.” Each of these objectives talks to an aspect of upholding that public confidence. Under goal two, he highlighted just a few of the six or seven objectives that fall under it: objective 1, “identify opportunities for continued outreach and engagement with state, local, tribal, territorial, and private sector;” objective 4, “advocate for visibility of local homeland security priorities;” and objective 5, “improve the information sharing enterprise within fusion centers’ areas of responsibility.” These concern providing opportunities for better outreach and engagement with state, local, territorial, and the private sector to ensure that there is visibility for local homeland security priorities in the fusion center. They aim to improve information sharing within each of the areas of responsibility of these fusion centers. Goal three addresses the whole, overall network again.

Mr. Wight cited several of the objectives under goal three: objective 2, “develop centers of analytic excellence;” objective 3, “promote the development and interoperability of fusion center information sharing and intelligence management systems;” and objective 4, “develop a rapid response or augmentation capability to physically and virtually support fusion centers.” Because each agency is unique and each has unique contracting and procurement practices and differences in availability of funding, some of the systems at the fusion centers end up being different, and they are not all interoperable or interconnected. This can be a challenge when sharing information or having analysts from one center come to support another one. For example, if personnel from Maryland come to the fusion center in DC, they wouldn’t have any ability to log in and use the systems and really leverage that talent there. The question becomes, how to develop that kind of capability and interoperability. That ties to objective four. Mr. Wight cited two of the objectives here: objective 4, “collaboration and formalized production of joint products;” and objective 6, “improve smart practices regarding JTTFs.” Mr. Wight noted that leveraging these partnerships for information sharing between the federal partners and the fusion center network has come a long way through collaboration and the formalized production of joint products. Many of these initiatives are already completed in the federal framework. In fact, the WRTAC just did one for the inauguration, a joint threat assessment, with DHS, FBI, and National Counterterrorism Center.

Mr. Wight touched on several of the other 37 objectives. He discussed standardized training and noted that I&A has helped a lot with this. He spoke to the development of a baseline set of fusion center common technology services. He noted that it is not possible to specify what a jurisdiction must use, but it is possible to develop a rating system or identify best practices and generate a list of the systems that work better than others. There have been discussions about the possibility of holding some licenses at the NFCA level that can be used for some of these systems by the individual centers. With regard to the initiative to improve the collection of information and intelligence from correctional facilities, he observed that different rules apply, and there is a great deal of intelligence there. Improving cyber strategies is an initiative that is still a growth area. Concerning the initiative to develop comprehensive fusion center intelligence requirements, Mr. Wight noted that, unlike a federal intelligence agency where collection can be tasked, it is not possible to task at the state and local level. It is possible to pick up the phone and ask a center to share intelligence. The objective is concerned with having collection requirements and standing intelligence requirements and about refining them and keeping them current. Another objective is cross-training analysts between fusion centers. Mr. Wight pointed to the fact the WRTAC had an exchange program with the Maryland center, through which the WRTAC send analysts to spend a week at the Maryland center, and Maryland send analysts to DC. The Maryland analysts were given logins and passwords and gained an understanding of WRTAC systems and products and processes. There are efforts to do this in a broader context within regions, because, if the DC center is overwhelmed, Maryland probably is, too; so, it may be necessary to reach up to Connecticut or elsewhere for help.

Mr. Wight turned to the federal framework that complements the national strategy, and noted that there were 40 projects identified with that. He reported that 37 have been completed and three are in progress and an MOU has been developed and is awaiting final signature. So, it is almost complete. There are four goals for the federal framework that mirror the goals of the national strategy. The first is, again, continuing to safeguard information while protecting privacy, civil rights, and civil liberties. The second is to standardize partnerships between the Federal government and the fusion centers to increase analytic and information sharing capabilities. The third goal for the federal framework is to expand fusion center engagement with Federal and state, local, tribal, territorial, and private sector partners. It aims to ensure that the Federal agencies are able to leverage all the talent in the network, because there is a lot of information at the state and local level that federal agencies do not have. Mr. Wight noted that Mr. Rogers just provided a great summary on some of the key projects that are in the federal framework to support the strategy, such as enabling TS/SCI clearances for state, local, tribal, and territorial analysts. He commented that, while it is probably not yet as smooth as it could be, it works. Another project is the fusion center assessment program, done annually by DHS. Initially, it was quite cumbersome, with over 300 questions. With the support of Francis X. Taylor, former Under Secretary for Intelligence and Analysis, DHS, it was revised to about 10 metrics, including five key ones for which the fusion centers had to collect the data and five for which DHS collected data from existing sources, such as products that are posted on the Homeland Security Information Network (HSIN). This reduced the requirement while still managing to show the effectiveness of the network, tell the fusion center story, and explain why federal money is being used to support them. Another project is to define where fusion centers fit in the cyber mission space. Since DHS has the requirement for that cyber defense mission nationally, it has an interest in figuring out where fusion centers fit, identifying common technology requirements and common analytic training standards, and refining and improving analytic training centers. Mr. Wight noted that there is an initiative to develop a national mission cell, which is to imbed a DHS analyst from I&A and an FBI analyst into a fusion center and produce products on site that address national mission priorities like counterterrorism.

Mr. Wight then turned to fusion center network collaboration successes. He praised the HSIN, noting the value of the situational awareness from the HSIN SitAware, whereby the centers across the nation could see what was going on in DC because both the police department and the fusion center were posting the information in the situation room. Similarly, he noted that there is an awareness room, HSIN CinAware, for sharing cyber security information. A lot of these things, especially in the cyber world, are not local issues. Somebody may be in a local area, but they're attacking, internationally or nationally as well. So, often, issues, such as ransomware, that occur in one area will pop up elsewhere. Having that ability to share information instantly about an attack and provide that information through the HSIN CinAware network is a great thing.

Pointing to a specific example, Mr. Wight discussed a collaboration between Alabama and Chicago fusion centers. Somebody in Alabama who was looking at social media and got concerned about some postings called the local fusion center. The Alabama fusion center inquired and found that the individual was traveling to Chicago where he stated he was going to kill some law enforcement people. Alabama passed the information to the Chicago fusion center, who tracked this individual down and found that he had a basement full of weapons and his own shooting range where he was training for and planning the attack. The subject was arrested. Mr. Wight explained that this kind of collaboration occurs daily across the national network, noting that looking at success stories like this and realizing what things have been prevented, demonstrates how much value there is in the fusion center network. He noted another example that shows there is value to information shared across the network even for centers that are not involved in an incident. The Northern California center was supporting a network of partners with an event in San Bernardino. In DC, they could see in real time what was happening in San Bernardino, and, as interested observers, were trying to determine if and how it could affect the local area. The first question that the senior leaders would always ask about a high profile events like this is whether there is any nexus to DC? Number two, is it part of a broader plan, and, number three, is it coming this way? It is valuable information that can support an investigation.

Mr. Wight then touched on the centers of analytic excellence and noted that the idea is to share tradecraft. Since some fusion centers are blessed with some great skills in certain areas but other centers may not have that access, the idea is to explain how centers built up a capability, how they crafted the products, how they trained analysts, and how they put that information out for centers to access. He lauded another great initiative, the fusion center cyber pilot, which he described as a toolkit, a cybersecurity program in a box. It can be accessed on the DHS HSIN, as well as on NFCA website. This is particularly important because many fusion centers are getting into the cyber realm and need to hire cybersecurity analysts. They must learn how to develop a requirement to hire them, to determine what skill sets they are looking for, how to get them trained, the career path, and certifications. All this and other information is available, and it has been very effective. Mr. Wight also mentioned the cyber- intelligence network, noting that there are six regions, each with a coordinator and a deputy. There is the HSIN CinAware where more than 300 cyber professionals share information. Plus, there is the real-time situation awareness room, the HSIN SitAware. Mr. Wight ended his presentation by advising that contact information for the fusion centers can be found on the HSIN or through the NFCA.

Rich Licht, SLTPS-entity member from the Center for Internet Security/Multi-State Information Sharing & Analysis Center asked if it was correct that there is not a funding stream for the 37 key initiatives and projects. Mr. Wight affirmed this and explained that the fusion centers themselves—76 of the 78—receive some form of federal grant funding. Some receive a lot, like DC, which is 100% grant-funded, and some such as Louisiana and Alaska receive none. For the others, the funding varies, although it’s a relatively small portion for most of them. So, while there is grant funding, there is none specifically earmarked for the 37 initiatives. Mr. Licht then inquired about DHS standardization of technology. Mr. Wight replied that standardization is one of the initiatives being worked by DHS and the Program Manager for the Information Sharing Environment, ODNI, to provide technology services and recommendations. Part of the challenge is there are different rules and different funding availability, but there are analytic tools on the HSIN. This is one of the initiatives. These tools are made available on HSIN that anybody can use.

Josh Ederheimer from the DOJ Office of Tribal Justice inquired regarding the participation of tribal law enforcement. He indicated that he was aware that it is working fairly effectively in New Mexico and Arizona but was not sure about other places. Mr. Wight responded that there is participation in the national network. Certainly, Arizona has tribal representatives that are a formal part of the center. Across the national network there is participation in varying degrees. It's individual. It's localized. There's no standard level of participation. It varies by region. He noted there is no directive that anybody has to participate. It is a voluntary, self-organizing network. The individual jurisdictions see the value in participating or are aware of it. Mr. Wight reported that one of the things he did as a fusion center director, was constantly conduct outreach briefings saying, "Hey, your local fusion center is here. Here is what we can offer you. Please partner with us and share information with us." But no one can be forced to do that, and it's that way with the tribal entities. Some participate and see it as a great value added. Others, for whatever reason, do not. But, the network does receive tribal information.

Mr. Rogers, observing that the strategy ends in 2017, asked if work was being done on the next version. Mr. Wight replied that he was recently discussing this with the executive director of the NFCA and observed that everyone has taken a breather with the administration change. The NFCA director said his first priority is to assess where we are on this and then see where we need to go.

Dr. C. Elaine Cummins, SLTPS member from the FBI, remarked that she really enjoyed the presentation. She noted that she was engaged in this effort at the policy level, recalling that she and Russ Porter, ODNI met over the fusion center guidelines as they were working to write that first version. She reflected that with policy you get to put stuff in place, and you have to move on and do some other policy.

The Chair complemented Mr. Wight for another high note. He then introduced Dr. Patrick Viscuso, Associate Director of Controlled Unclassified Information (CUI), ISOO, to provide an update on the status of the implementation of the CUI program.

D. Controlled Unclassified Information (CUI) Program Status

Dr. Viscuso noted that the CUI staff has worked with state and local entities in the past and that he recognized some of names of people on the phone and in the room. He said that he would like to work more closely with them in the future. The CUI program needs the valuable input of this community in order to form guidance that makes sense when it comes to the handling of this type of information, which is highly valued by this community.

He began by describing the current problem in the executive branch. For information that is unclassified and that law, regulation, and government-wide policy tells the executive branch to control or protect, there are over 100 different systems for protecting this information within the executive branch, and this is reflected in over 100 different markings. Often, there is not even agreement on what information should be protected, and certainly there is no agreement on how to protect it. That is not a good situation, and it can lead to a lot of problems in information sharing. And where information sharing does take place, because many of these agency policies are not widely available, it can lead to either under-protection, putting the information at risk, or overprotection, restricting the information in terms of its sharing. Now, if this is the problem within the executive branch, one can only imagine what may be going on when this information is shared with nonfederal partners, law enforcement, state law enforcement, and others.

Dr. Viscuso continued, reporting that to address this problem, several administrations have attempted to come up with solutions. There were solutions under the Bush administration, and there was a solution that was developed under the previous administration. The major partners in the executive branch and major partners in the state, local, tribal, and private sector community participated in the development of an executive order.

He stated that, in place of over 100 different systems, Executive Order 13556, "Controlled Unclassified Information." established one system. It established the CUI program. It designated the National Archives as the executive agent, and ISOO was delegated the responsibilities of the executive agent. The executive order established the criteria of what needed to be protected based on what the law, a federal regulation, or a government-wide policy said to protect. The problem is that, often, the law, regulation, and government-wide policy did not dictate how to protect it, so well-meaning agencies developed their own policies on what it meant. This is why there are over 100 different systems in the executive branch right now for doing this, and, consequently, you have the problem we have now. For example, there is the marking FOUO, and a number of agencies mean different things by "FOUO" and have varying sanctions for what happens if FOUO is released in an unauthorized manner. So there's a problem. The CUI system is meant to fix this problem. So, now there is one scope of information, one criterion for that scope of information, and the CUI office, as executive agent, was charged with the responsibility of establishing a registry.

Dr. Viscuso related that the executive order wanted to make clear to the entire executive branch and its partners what needed to be protected. So the idea was to establish an online public registry of all the categories and subcategories of CUI that everyone was required to protect. There was a data call to the entire executive branch that asked them, "What do you protect now on the basis of law, regulation, and government-wide policy? How do you mark it? What are your policies?" Over 2,200 submissions were received, which the CUI staff evaluated based on the criteria in the executive order. They sifted through them and came up with 23 categories and 84 subcategories, and they linked each one of those categories and subcategories to the law, regulation, and government-wide policy that established them. They also listed the sanctions that were associated with each one of those categories and subcategories, a very important point if you are establishing one system for the entire executive branch

Dr. Viscuso reported that, after establishing what needed to be protected and completing the registry in December of 2011, it was necessary to come to an agreement as an executive branch on how to protect the information and what the unitary, standardized system would look like. After five years of work, this was accomplished in the 32 Code of Federal Regulations, Part 2002. It was developed through three years of informal coordination with the key agencies of the executive branch that would be affected by this regulation—28 major agencies that constituted most of the federal budget—which included input from state, local, tribal, private sector, and others, as well. There was a council, whose composition was based on the Chief Financial Officers Council, and the CUI office consulted with them three years. We asked them key questions: How do you protect this information right now? How do you safeguard it? How do you share it? How do you destroy it? How do you control it? How do you mark it? How is it protected in the physical and electronic environments? It was important to incorporate the electronic requirements because most of this information exists within the electronic environment. They were instructed by the President and the executive order to be consistent with the Federal Information Security Management Act (FISMA), with National Institute of Standards and Technology (NIST) guidelines and standards, and with Office of Management and Budget (OMB) policy. They were not to create a parallel electronic set of requirements but to be consistent with those that already exist for protecting information that law, regulation, or government-wide policy requires to be protected.

Dr. Viscuso reported that an agreement was reached. This was followed by the OMB public rulemaking process. After three years of informal coordination, there were two years of OMB-managed public rulemaking. The result was the 32 CFR 2002, which underwent public comment, including many comments from state, local, tribal, private sector community, and, in addition, many from industry and academia. The CUI staff held numerous meetings during the public comment period, and also during the formal-informal development. They received between 1,800 and 2,000 comments and proposals, which were considered in the crafting the 32 CFR 2002 to establish a baseline for protection.

Dr. Viscuso recognized that there are many things that would be of interest to the SLTPS-PAC group. Due to the limits of time, he had to pick one. He chose the cyber-security requirements, because he recognized that this is a big-ticket item for the state, local, tribal, and private sector community. How does a tribe upgrade its security, its IT system, in order to receive government information? This was considered very carefully. Dr. Viscuso described how the problem was approached. He began by returning to the purpose of this program. While there are many elements, ultimately, the purpose is to make sure the information can be shared, but undergirding this is its common protection, its common marking, and the common definition of what that information actually is. Part of that is uniformity and consistency in the definition of protection. Based on the requirement to be consistent with the OMB policies, the FISMA, the NIST standards and guidance, a safeguarding standard was prescribed. That safeguarding standard is no less than moderate confidentiality. Confidentiality relates to safeguarding. The term “moderate” is a key one. If the law tells us to protect something, it means to go beyond how things are normally treated. In other words, if the minimum that any system is treated within the executive branch is low, when the law says, “Protect it,” it probably means something more than low, hence moderate. And most government agencies do have a moderate baseline for the protection of information that the law says to protect, particularly privacy information. Privacy information is protected at a minimum of moderate.

Dr. Viscuso indicated that prescribing in the federal rule no less than moderate as a standard for all the information that the law, federal regulation, government-wide policy said to protect poses a very important problem for the state, local, tribal, and private sector communities, and also for contractors to the government who will be receiving federal information for a lawful government purpose, which is the standard by which this information will now be shared. This was defined in a particular way. Dr. Viscuso read the definition, because this is important to this community: “Lawful government purpose is any activity, mission, function, operation, or endeavor that the US government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of nonexecutive branch entities such as state and local law enforcement.” So there is a clear recognition of the needs of the SLTPS community to share the information for lawful purposes within the scope of its legal authorities. The question to be asked is if you are sharing this information for that reason, to fulfill a lawful government purpose, does this mean when you receive the information that you now are required to build a federal information system. The requirements for building a federal information system are specified in NIST Special Publication (SP) 800-53, which is about 500 or 600 pages long. It contains controls organized according to families. This is basically a blueprint of how to build a federal information system. It is divided according to low, moderate, and high controls, and if you have something at moderate it assumes you have built all the controls that are at the low. It’s very complex. It is based on a lot of sources including congressional legislation. Some of the congressional requirements are not related precisely to security but are related to other concerns. There are detailed requirements such as whether you should set your computer to Greenwich Mean Time or not.

Dr. Viscuso reported that the first thing that had to be done to solve the problem was to reference the FISMA to distinguish what is a federal information system and what is a nonfederal information system. A federal information system is one that is operated by someone on behalf of the government. It is operated by a contractor, for example, on behalf of the government. It can be an email system, a payroll system. It can be an IT system that's built by a contractor. A nonfederal information system is one in which, for example, someone has received information incidental, for a contractor, to provide a service or product to the government that's not processing. It can also be a tribal organization that has received the information for a lawful government purpose. They are not operating an information system on behalf of the government. Simply by receiving the information you're not operating a federal information system. Dr. Viscuso related that the CUI staff recognized this. They teamed up with the NIST and developed NIST Special Publication 800-171. They went through the entire catalogue of controls in the NIST SP 800-53 and eliminated those controls that weren't related to safeguarding, that were specific to federal concerns or, for example, may have been based on political concerns, like some that were enacted by Congress and have nothing to do with safeguarding. The result was not a set of controls but a requirements document, an objectives document, organized according to 14 families that are related to the definition of what good information security is in terms of safeguarding. It set out objectives that could be met in a variety of ways, and there is flexibility built into the document. The latest revision is December 22, 2016, which sets out the requirement that the nonfederal entity following this document would have a security plan that could set out where it was in terms of meeting the objectives of good information security, so they could say, "We're 40 percent there," in that document and then set out a plan by which they could mete out the other 60 percent. This is important because the government partner then could make a risk management judgment on sharing the information. Dr. Viscuso made two important points about this. The NIST SP 800-171 is an objectives document, a requirements document, that sets out goals for nonfederal entities. It allows them to build into it a security plan that captures where they are right now and where they want to go. In both instances, there's plenty of flexibility for a judgment to be made by a government entity in terms of whether to share the information or not. They can determine whether they've actually met those objectives and how, and whether that's sufficient for them to share the information.

Dr. Viscuso next provided a sketch of the direction this is going for contractors. One of the intentions of the program is standardization, and the CUI office intends to propose a federal acquisition regulation rule this year that will be incorporated into procurements by the executive branch. He discussed what would be some of the considerations in addition to levying the requirements of the program for protection of this information on nonfederal partners. He indicated that some of the considerations that will be addressed will include how to identify the information sufficiently on the government side so that everyone knows what needs to be protected and, at the same time, highlight anything that's not standard in law that the nonfederal partner must follow in order to adequately protect the information and not break the law. There will also be a way to capture information necessary for oversight, at least for contractors. This is an immense population. Current government systems will be used to do this, to track who is holding CUI among the contractor world. Currently, in the System for Acquisition Management, (SAM) which is the system in which all contractors must register, there are 350,000 registrants. These are contractors, grantees, and licensees. If only two-thirds of them hold CUI, that would be more than 200,000.

The CUI office intends to leverage that system in order to track who has CUI today so that decisions can be made about who needs to be examined more, particularly for oversight questions.

Dr. Viscuso then turned to the implementation of the program for the executive branch. The CUI staff negotiated deadlines with OMB and with the CUI advisory council, deadlines according to which this program will be implemented. The deadlines are captured in a notice that's online, CUI Notice 2016-01, which sets out some basic things that seem very common sense development of policy first by agencies. These are very large organizations, so they must develop their internal policy to be consistent with the CUI program. Then, they have to train their employees. At the same time, they have to assess their information systems, because some of them are not at moderate confidentiality. Some of them are at low, and no doubt everyone in this room knows the problem of data breaches in the executive branch. So what is called for is an inventory of those systems and then a plan by which those systems will be brought to moderate confidentiality.

Dr. Viscuso indicated that the physical security requirements of protecting this information are not burdensome. If it is in paper, physical form, it is one physical barrier, and the CUI rule explains what that means. What is anticipated is a soft interim operating capability at year one that will mainly deal with the physical, and the division and development of policy and training. Then, by year two, optimistically, there will be the full implementation of the program. Flexibility has been built into this timeline. These are very aggressive timelines that were shortened from the initial ones that went to OMB. Dr. Viscuso indicated that, in actuality, if we are flexible with these timelines, it will take longer for agencies to develop their policy, to train all their employees, and to inventory their systems. He thinks a more optimistic view is five to six years to implement this program in the executive branch.

Dr. Viscuso then turned to the main elements in terms of implementation, remarking that he thought they had some relevancy for this community. He opined that everyone who is involved in information security and management must know that, in order to do it effectively, you have to have policy. You have to have someone that manages the program. You have to have training. You have to address physical safeguard systems. You have to have some provision for reporting incidents. You have to inspect yourself. He stated that we know that state, local, tribal entities and agencies will be modifying their agreements and contracts to reflect the new program. This will occur when the agencies themselves have begun to implement the program in a meaningful way internally. Then, they will modify their agreements, because it would make sense if they're going to, for example, use the CUI markings, which are online, they would have to be using them themselves, first, before they began to require others outside of their agency to use them.

Dr. Viscuso then provided additional details of the registry, noting that there are some things here that he could discuss in some detail. He indicated that he would be more than happy to take some time to do this, but he thought his time was limited. So he spoke to a couple of things that might be wondered about in terms of legacy information. Particularly for state and local entities, if you deal with a major database that's online that has thousands upon thousands of PDFs, it's probably running through your mind, "If it's going to go under a new system of marking, how will they remark all of those?" And so, flexibility has been built into this rule based on input from the agencies and from the state and local partners that we can do these things in a much more creative manner. We can put a flash screen up and alert people that the information is CUI without having to remark every PDF. Legacy information in general, agencies have a great deal of flexibility in determining whether it should be remarked or not. The general rule of thumb is that if you're reusing the information, putting it into a new document, you should re-mark it.

Dr. Viscuso noted that his briefing normally lasts an hour and a half because the CUI staff is trying to give people an orientation to the program. In addition, they have several virtual briefings that anyone can attend. There is one the day after this meeting (January 26, 2017), from 10:00 to 12:00. There is one on February 14th and one on February 22nd. The times are listed on slide 12 of the presentation. There is a large in-person briefing scheduled for January 27, 2017, in the William McGowan Theater, in the National Archives Building. Anyone can attend this. You will get the same information at all of these briefings, but, in particular, we are inviting nonfederal partners to the February 14th and February 22nd briefings. The content is the same. The questions are the same. This program is meant to be shared, and the guidance on it is meant to be open. He invited everyone to attend any of these briefings, as they can be very informative. Dr. Viscuso added that they have a number of briefings that he can provide electronically. He reported that they have a plan to post a video of one of the larger briefings on their website, which should be very soon. Mr. Porter asked how the nonfederal partners are going to be notified about the February 14th and 22nd presentations. Dr. Viscuso indicated that this is where he needs some advice. Mr. Porter indicated that he would be happy to help, and Dr. Viscuso responded that he would be delighted to have it. He added that if there is anyone listening in on this phone call that has any ideas how we may obtain greater input from this community, he asked that they look to the end of the briefing, on slide 13, for his contact information and for his leads for implementation and oversight. He told everyone to feel free to contact him directly. He expressed his eagerness to hear their input and insights and most of all to understand their needs and concerns so that future policy guidance can address them.

The Chair then turned to the open forum discussion.

IV. General Open Forum/Discussion

Mr. Wight returned to the issue of TS/SCI access for state and local, in order to be clear on what are the next steps on that. He indicated that he understands at the TS/SCI level it's got to be a federally-managed facility to have the physical machines in it that can process that information. He understands that this might be possible in New York City and Chicago and some of the other major cities later. But to help Iowa and places where that may not be as easy, the real challenge is just getting the analysts the ability to get a JWICS account once they get the clearance. So they then can go into that sponsoring SCIF and, at least, log onto the machine and share information and actually process the TS/SCI. Right now the clearance will allow you to attend a meeting and read a document, but you can't process it. So that's the real challenge, being able to do it without being detailed to a federal program. Maybe it is as simple as changing the definition of what "detailed" means. If that means I go over there once every two weeks and that counts as being detailed, that is fine. However, there is a lot of pushback in that. Mr. Rogers added that E.O. 13549 talks about the operating level being "Secret," and then TS/SCI is granted at the discretion of the agency. It also says access to classified systems are in accordance with agency policy, so we have to go back to the agencies that are managing the TS/SCI networks in order to understand what exactly their policies are. That is the key, because the executive order does not direct the agencies. It says they still govern their system and policies. Mr. Wight added that, in terms of getting the access itself, you have to have a SCIF owner sign off on the access and do the read-ins. When this initially came out through DHS, it said, "It can't be DHS," which did not make a lot of sense. He indicated that at the

WRTAC, they were able to find another federal agency, but in a lot of cases, for our partners out there across the nation, the DHS facility may be the only one. He speculated that it may have just been the newness of the issue and the interpretation, but thought it would have made a lot of sense to be able to go, “Well, OK, DHS, I&A, how about sponsoring it?” But the response was, “No, no, it can’t be us.” He indicated that he was not sure if that was a miscommunication or something is actually written down, but it was something that was encountered at the WRTAC, and other agencies may have had that problem. Mr. Rogers indicated that he was not aware of this. Mr. Pannoni added that it seems like if DHS accredited the SCIF, they should be able to grant access. Mr. Wight agreed and indicated that he did not know what that was, but the WRTAC was told it had to be an other-than-DHS facility, so that’s something that we may be working on. Mr. Rogers said that he could ask about that. (See Attachment 2 for the Action Items from this meeting.)

V. Closing Remarks and Adjournment

The Chair reminded everyone that the next SLTPS-PAC meeting would be held on Wednesday, July 26th, 2017, 10:00 a.m. to 12:00 noon, in the National Archives. He thanked them for coming, noting that he thought the meeting was worthwhile and that this is an incredibly important board, especially after hearing the briefings. The meeting was adjourned at 12:07 p.m.

Attachment 1

State, Local, Tribal, and Private Sector (SLTPS) Policy Advisory Committee (PAC) January 25, 2017, Meeting Attendees and Teleconference Participants

Bensley, Glenn R.	Department of Justice (DOJ) Member	Teleconference
Bradley, Mark A.	Chair, Director, Information Security Oversight Office (ISOO)	Attending
Branch, Kathy	ISOO	Attending
Cooper, Harry	Central Intelligence Agency (CIA) Alternate	Attending
Cummins, Dr. C. Elaine	Federal Bureau of Investigation (FBI) Member	Attending
Davenport, Jessica	SLTPS Member	Teleconference
Ederheimer, Joshua A	DOJ Office of Tribal Justice	Attending
Friedland, Jeffery Alan	SLTPS Member	Teleconference
Harris, Joan	Department of Transportation Alternate	Teleconference
Kirk, Agnes	SLTPS Member	Teleconference
Koren, Dori	SLTPS Member	Teleconference
Licht, Richard	SLTPS Member	Attending
Locklear, Lydia	DOJ Observer	Attending
Manley, Gary	Office of the Director of National Intelligence (ODNI) Observer	Teleconference
Masciana, Leo	Department of State Member	Attending
Minard, Keith	Defense Security Service Member	Attending
Parsons, Darryl	Nuclear Regulatory Commission Alternate	Teleconference
Pannoni, Greg	Designated Federal Officer, Associate Director ISOO	Attending
Pekrul, Mark	Department of Energy Alternate	Teleconference
Porter, Russ	ODNI Observer	Attending
Richardson, Benjamin	Department of Defense Member	Attending
Rogers, Charles	Vice Chair Department of Homeland Security	Attending
Schouten, Mark Jay	SLTPS Member	Teleconference
Skwirot, Robert	ISOO	Attending
Vinciguerra, Robert	Department of Transportation Observer	Attending
Viscuso, Dr. Patrick D.	Associate Director, ISOO	Attending
Webb, James Dewey	SLTPS Member	Teleconference
Wright, Lee (Tip)	Vice Chair SLTPS	Attending

Attachment 2

Action Items from SLTPS-PAC Meeting, January 25, 2017

1) Continue to explore the issues related to fusion center and other state, local, and tribal personnel seeking to obtain JWICS access without the requirement of being detailed to a federal agency

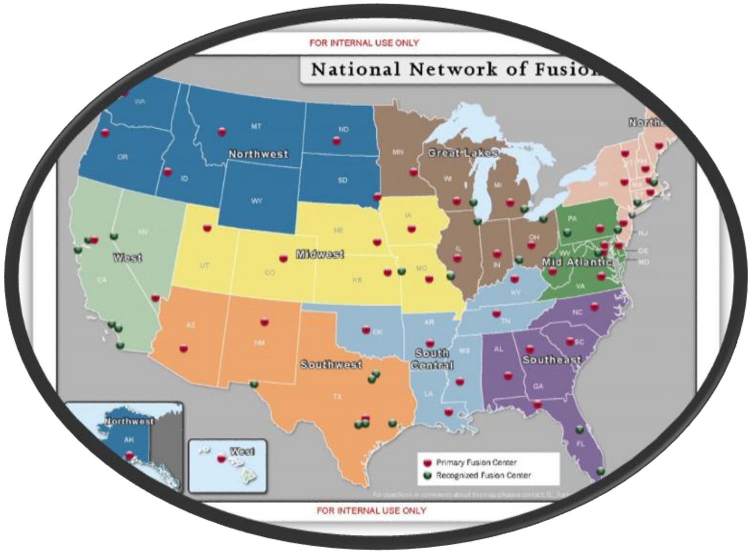
2) DHS to invite a guest speaker for the SLTPS-PAC meeting from Office of Intelligence and Analysis to discuss the process to prioritize Homeland Secure Data Network deployment for their field operations.

3) DHS to provide an update on the implementation of the hybrid (Additional National Industrial Security Program Procedures for Sharing and Safeguarding Classified Information with Certain Private Sector or Other Non-Federal Entities)

Fusion Centers and the National Strategy: National Asset/Local Resource

Lee “Tip” Wight, Vice President Emeritus NFCA

WHAT IS A FUSION CENTER?



SLTT(P) Entities

Regional Intelligence and Information Sharing

Multi Agency/Functional Composition

Multi Mission Focus ("All Threats/All Hazards")

NOT:

Federally - owned

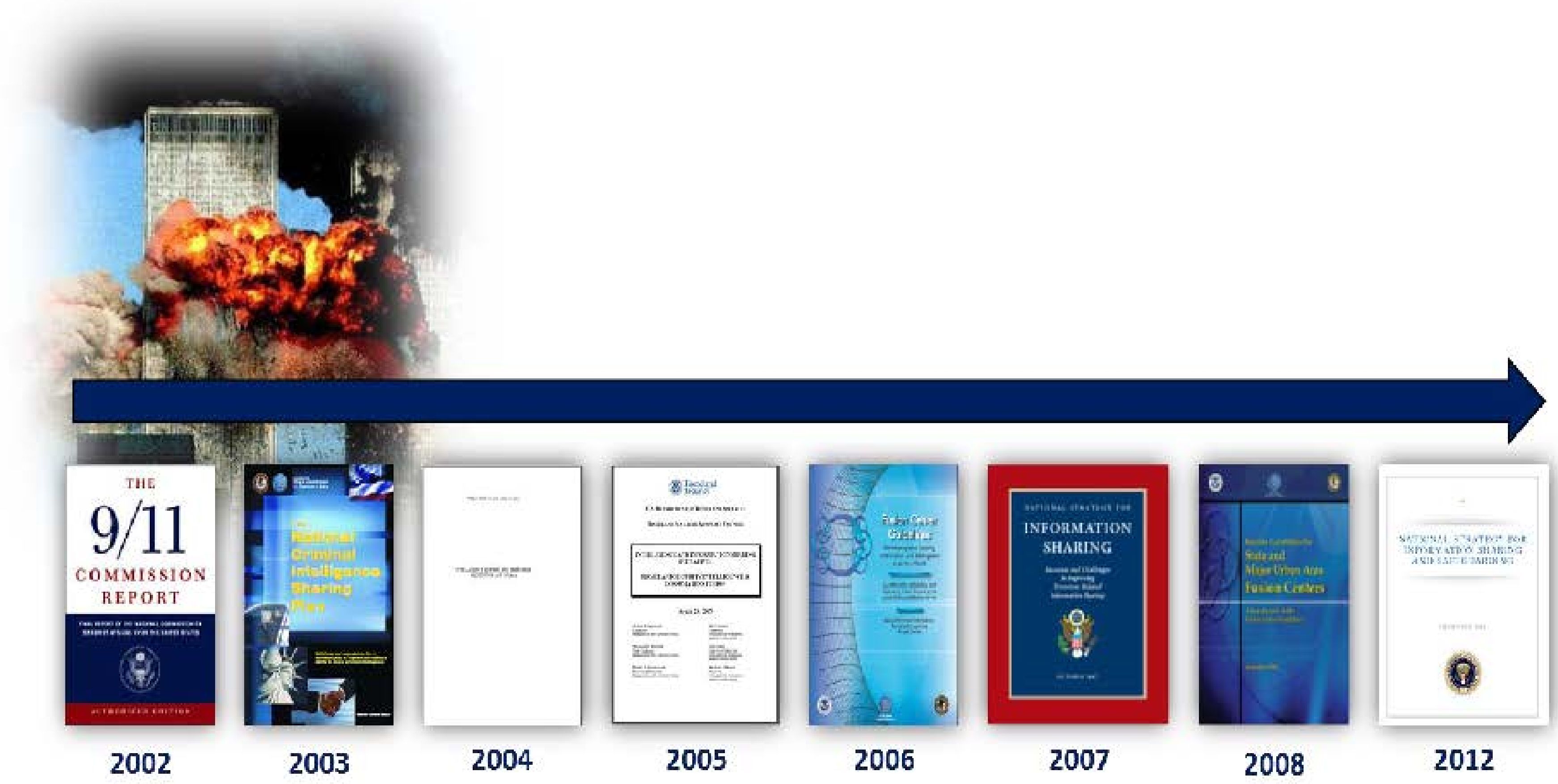
JTTFS, HIDTA, RISS Centers

Crime Centers, Local LE Units

Emergency Management Programs

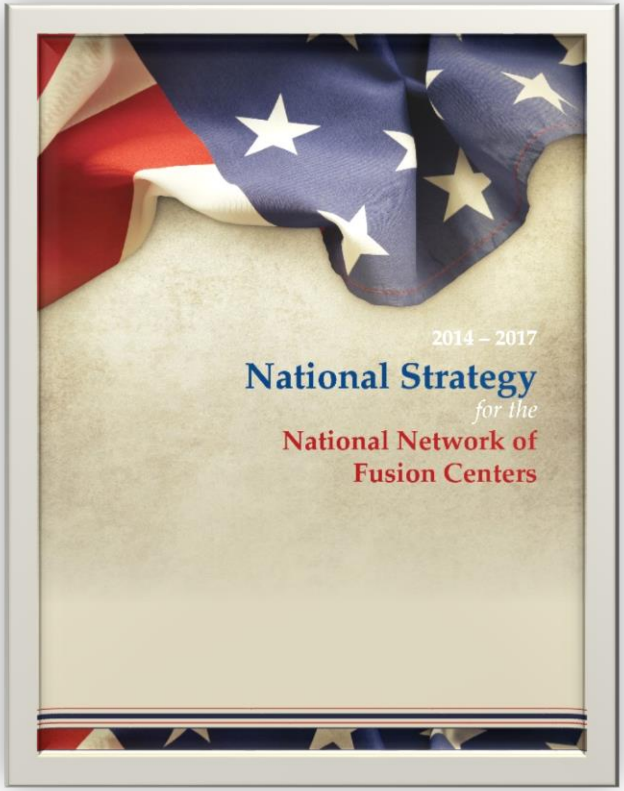
All the Same

History of Fusion Centers


THE 9/11 COMMISSION REPORT
National Criminal Intelligence Sharing Plan
Fusion Center Guidelines
NATIONAL STRATEGY FOR INFORMATION SHARING
State and Major Urban Area Fusion Centers
NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING
2002
2003
2004
2005
2006
2007
2008
2012

2014 – 2017
National Network of Fusion Centers National Strategy

- Vision
- Mission
- Values
- Narrative to Provide History and Context
- Goals
- Objectives
- Initiatives



2014 – 2017

National Strategy

for the

National Network of Fusion Centers

Contributing Organizations

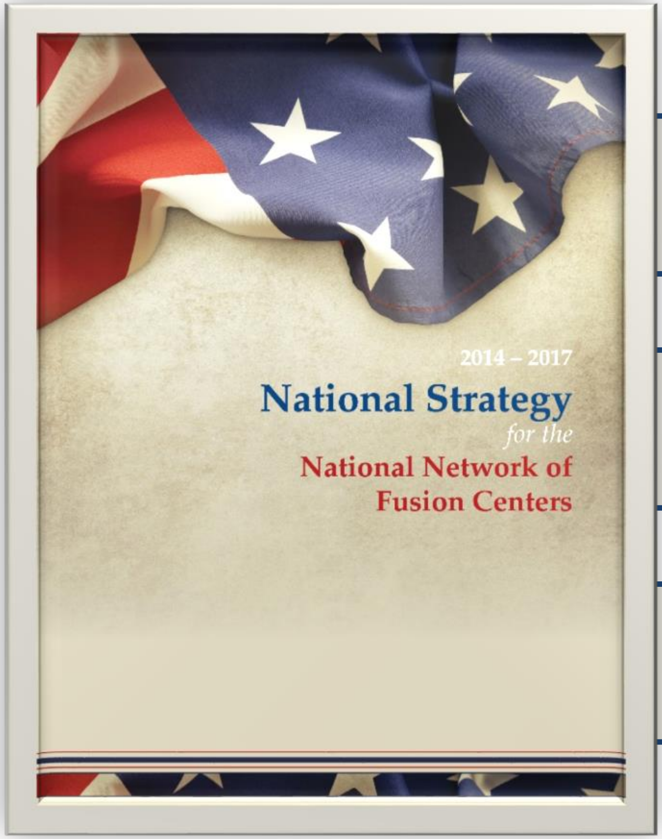
The Regional Information Sharing Systems

Major County Sheriffs Association

The High Intensity Drug Trafficking Areas Investigative Support Centers

In addition, representatives from the fire service and emergency management sectors were instrumental in the development process.

Purpose of the Strategy



2014 – 2017

National Strategy

for the

National Network of Fusion Centers

Define National Network Strategy

- Mission, Vision, Goals, Objectives

Identify Expectations

- Articulate path forward

Demonstrate Effectiveness

- Support and enhance the value of fusion centers

Key Components

Mission: The mission of the National Network is to **use the capabilities** unique to the NNFC and the state and major urban area fusion centers included in the National Network **to receive, analyze, disseminate, and gather threat information and intelligence** in support of state, local, tribal, territorial, private sector, and federal efforts **to protect the homeland** from criminal activities and events, including acts of terrorism.

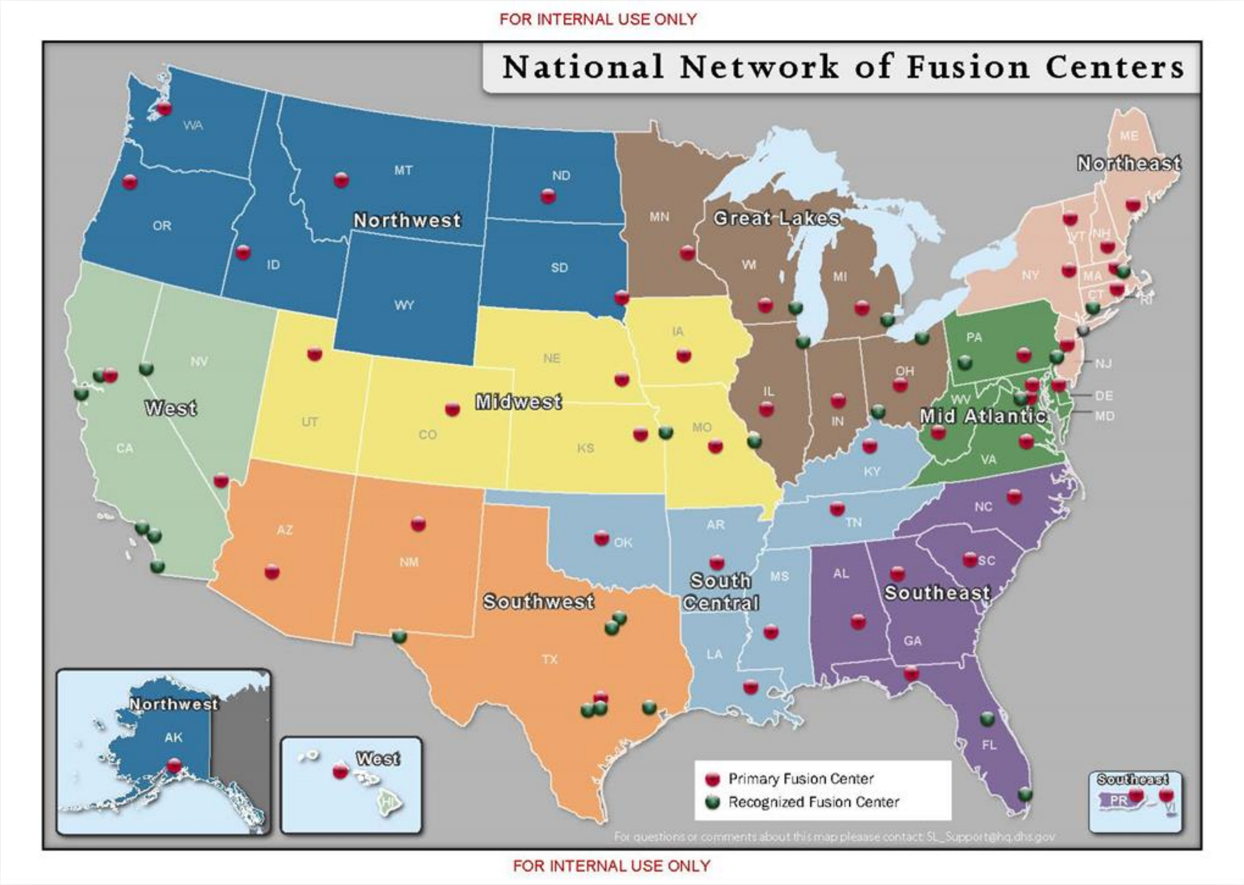
Key Components

Vision: The vision of the National Network of Fusion Centers is to be a multidisciplinary, all-crimes/all-threats/all-hazards **information sharing network** that protects our nation's security and the privacy, civil rights, and civil liberties of our citizens.

Key Components (continued)

- Values:
  - Respect—Individually and as a National Network, we respect the privacy, civil rights, and civil liberties of all.
  - Integrity—We are accountable and demonstrate impartial service to the law.
  - Professionalism—As leaders, our behavior is ethical and our information is safeguarded

DEFINING THE NATIONAL NETWORK



- Decentralized
- Distributed
- Self-organizing
- National Asset
- SLTT and major urban area fusion centers and networks

Today, there are 78 state-and locally-run fusion centers in operation across the nation

Function of the Network

"Help keep people safe by producing intelligence and sharing information"

Collaborate across jurisdictions and sectors to effectively and efficiently detect, prevent, investigate, and respond to criminal and terrorist activity.

Goals of the National Strategy

- ★ **Uphold public confidence** *(Protect information, privacy, civil rights, civil liberties)*
- ★ **Support engagement and expand the network of each fusion center** *(SLTT, private, federal, field-based information sharing)*
- ★ **Strengthen the integration and interconnectedness of fusion centers** (*Strengthen the Network itself*)
- ★ **Increase the overall connectivity between fusion centers and the federal government**

GOAL ONE AND KEY OBJECTIVES

Goal 1: **Uphold public confidence** through the safeguarding of information and the protection of the person and the privacy, civil rights, and civil liberties of citizens.

- Objective 1: …. **privacy, civil rights, and civil liberties protections**….
- Objective 2: **Enhance and sustain a trusted network….**
- Objective 3: **Promote fusion center accountability and transparency**…

Goal Two and Key Objectives

Goal 2**: Support fusion center engagement** with state, local, tribal, territorial (SLTT) partners, private sector partners, field-based information sharing programs, and federal partners, to enhance decision making and resource allocation, improving the information sharing environment within fusion centers' areas of responsibility.

- Objective 1**: Identify opportunities for continued outreach and engagement with SLTT and private sector…**
- Objective 4: **Advocate for visibility of local homeland security priorities** …..
- Objective 5**: Improve the information sharing enterprise within fusion centers' AORs**

GOAL THREE AND KEY OBJECTIVES

Goal 3**: Strengthen the integration and interconnectedness of fusion centers** to share and leverage information, analysis, and expertise.

- Objective 2: **Develop Centers of Analytic Excellence**

Objective 3: **Promote the development and interoperability of fusion center information sharing and intelligence management systems**

- Objective 4**: Develop a rapid response or augmentation capability to physically and virtually support fusion centers**

GOAL FOUR AND KEY OBJECTIVES

Goal 4: **Increase the overall connectivity between fusion centers and the federal government** to strengthen analytic and information sharing capabilities and enhance situational awareness through collaborative efforts to protect the homeland.

- Objective 4: …. **collaboration and formalized production of joint products.**
- Objective 6: …..**improve smart practices regarding Joint Terrorism Task Forces (JTTFs).**

Implementing the Strategy: 37 Initiatives

Fusion Liaison Officer (FLO) training programs

Annual threat assessments within AOR

Develop comprehensive FC intelligence requirements

Develop baseline set of FC common technology services

Enhanced annual exercise program

Cross-train analysts between fusion centers

Improve information/ intelligence from correctional facilities

Improve cyber strategies

Create centers of analytic excellence

Federal Framework

Federal Framework for Support to the National Network of Fusion Cent

>90% Complete

40 Projects

- 37Completed
- 3 In Progress

Federal Goals

- Continue to safeguard information and **protect privacy, civil rights, and civil liberties (P/CRCL)**
- **Standardize** partnerships between Federal Gov't and FCs to **increase analytic and info sharing capabilities** and enhance SA in the homeland
- Develop and **expand FC engagement w/Federal & SLTTP partners** to enhance FC core capabilities & improve SA in FC AOR
- Improve/increase Homeland Security Enterprise ability to **leverage National Network information & expertise**

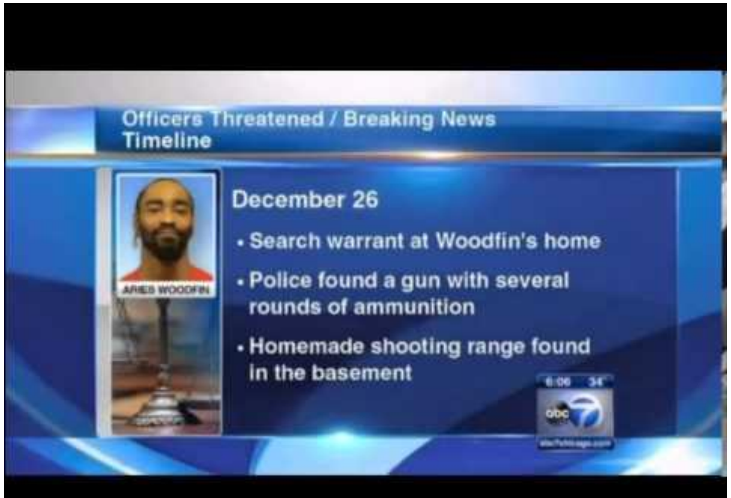
Key Projects

- TS/SCI Clearances for SLTT Analysts
- Revised Fusion Center Assessment Program
- Cyber Strategy/Define FC Cyber Mission Space
- Baseline common technology requirements
- Develop common analytic training standards
- National Mission Cell

NETWORK COLLABORATION SUCCESS STORIES

- Boston Marathon
- DC Navy Yard
- Alabama-Chicago
- San Bernardino
- HSIN SitAware
- HSIN CinAware

Alabama/Chicago Collaboration



Officers Threatened / Breaking News Timeline

December 26

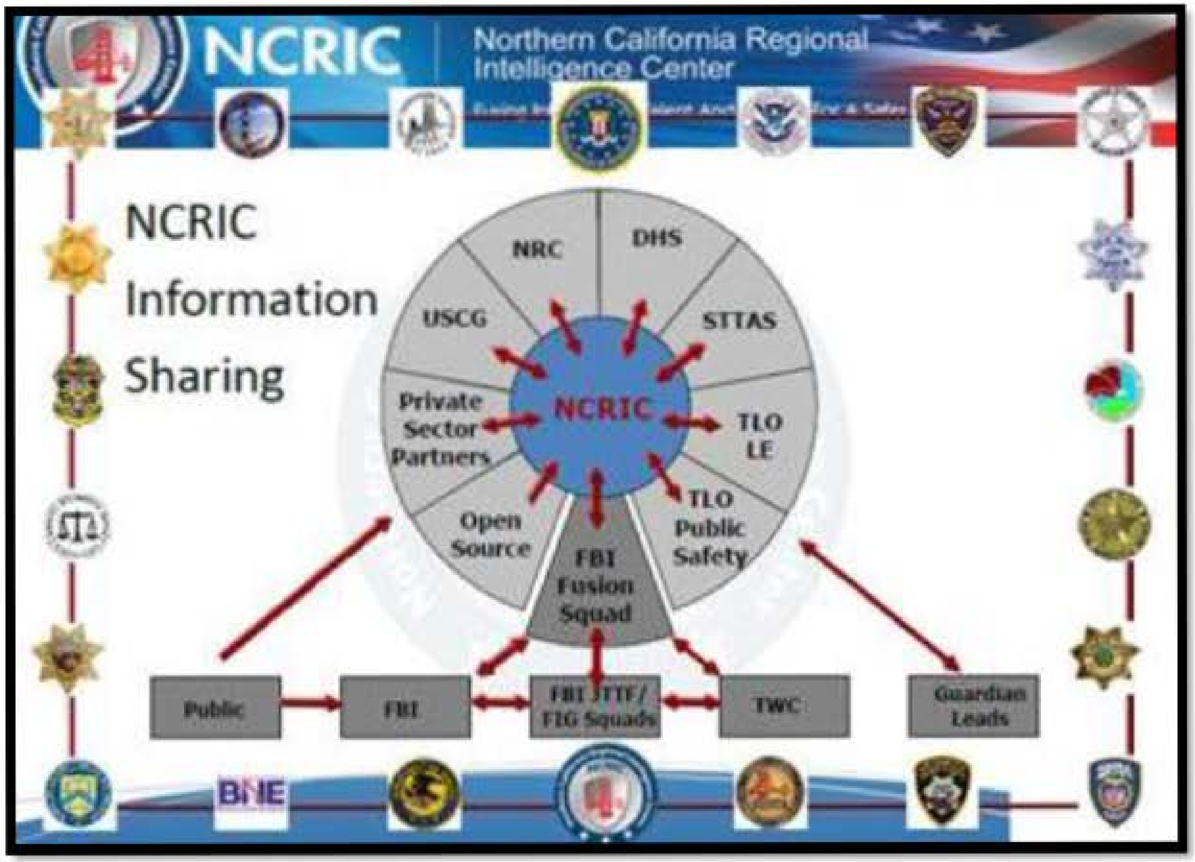
- Search warrant at Woodfin's home
- Police found a gun with several rounds of ammunition
- Homemade shooting range found in the basement

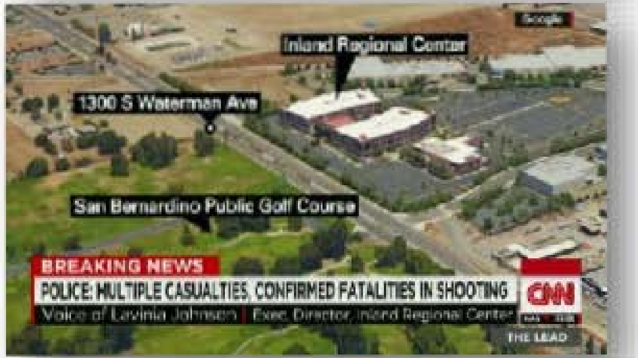
UNCLASSIFIED

- On 8 December 2014, the Alabama Fusion Center (AFC) received a call from an Alabama citizen alarmed by an individual's social media posts related to killing civilians and law enforcement.

- On 26 December 2014, the subject was located and stopped.

San Bernadino




Google
Inland Regional Center
1300 S Waterman Ave
San Bernardino Public Golf Course
BREAKING NEWS
POLICE: MULTIPLE CASUALTIES, CONFIRMED FATALITIES IN SHOOTING
Voice of Lavinia Johnson | Exec. Director, Inland Regional Center
CNN
THE LEAD

KABC
San Bernardino, California
12:05 PM PT
BREAKING NEWS
POLICE, FBI, ATF AT SCENE OF MASS SHOOTING
CNN
NEWSROOM

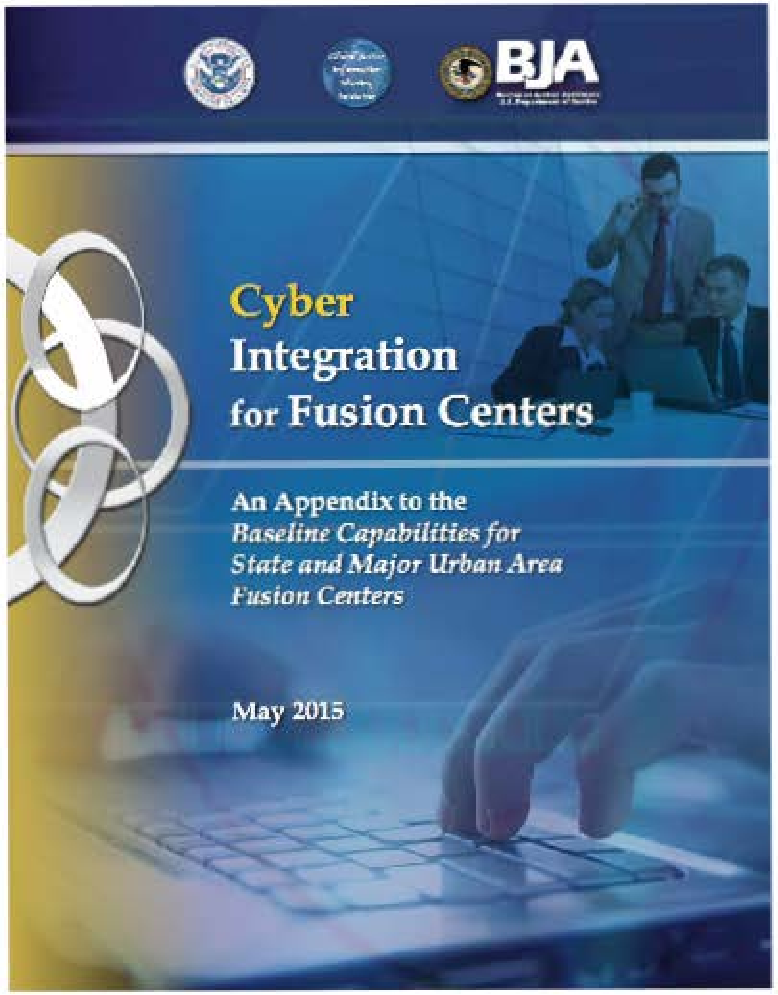
Centers of Analytic Excellence (CoAE):

Sharing Resources, Best Practices, and Expertise Toward a Stronger Network

- Collaborate, access resources, and learn how FCs add value to national security and crime reduction
- NFCA coordinating mechanism and "force-multiplier,"

- Capabilities, activities, examples:
  - Policies and procedures
  - Resources and methods
  - Decryption, language translation, and data reduction
  - Tradecraft and product information
    - Analytical Tradecraft Community of Interest (AT COI)

FC Cyber Pilot



Cyber Integration for Fusion Centers

An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*

May 2015

TOOLKIT

Sample Job Descriptions

NFCA-CIN

Cyber Intelligence Network

"Connect, collaborate, coordinate, share information and resources with the National Network of Fusion Centers."

- Share information rapidly.
- Coordinate & prevent the duplication of efforts.
- **Leverage skills and resources across the entire National Network of Fusion Centers (force multiplier.)**

NFCA-CIN
Cyber Intelligence Network

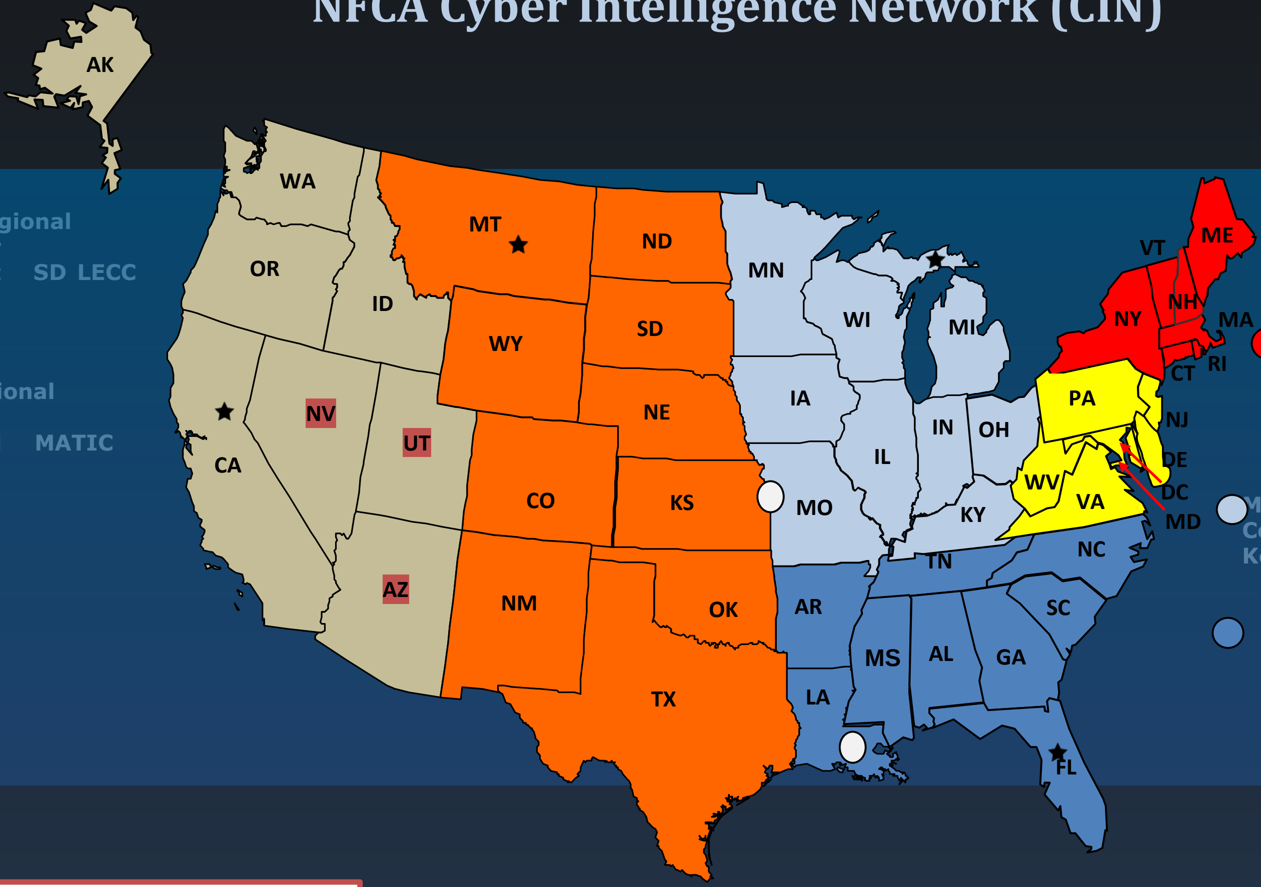
- 6 regions each with 1 Coordinator and 1 Deputy
- Implemented NFCA-CIN portal on HSIN
  - 50 agencies
  - 40+ states
  - 300 Cyber professionals
- Implemented Cyber Situation Awareness Room (CINAWARE) on HSIN.

NATIONAL
FUSION CENTER
ASSOCIATION

NFCA Cyber Threat Intelligence (CTI) Subcommittee

● Troy Campbell – Co-Chair – KCTEW
Devin King – Co-Chair – LA-SAFE

NFCA Cyber Intelligence Network (CIN)



● Western Regional
Coordinator
Will Mondet SD LECC

● Central Regional
Coordinator
John Burrell MATIC

● Northeast Regional
Coordinator
Brett Paradis (CTIC)

● Midwest Regional
Coordinator
Kelley Goldblatt (MC3)

● Southeast Regional
Coordinator
Heather Perez (CFIX)

Non-Voting/Associate Advisory Members

- Chad Holmes – Private Sector Cyber Intelligence SME
- Andrea LeStarge – DHS I&A SLPO Support SME

QUESTIONS ???

Controlled Unclassified Information

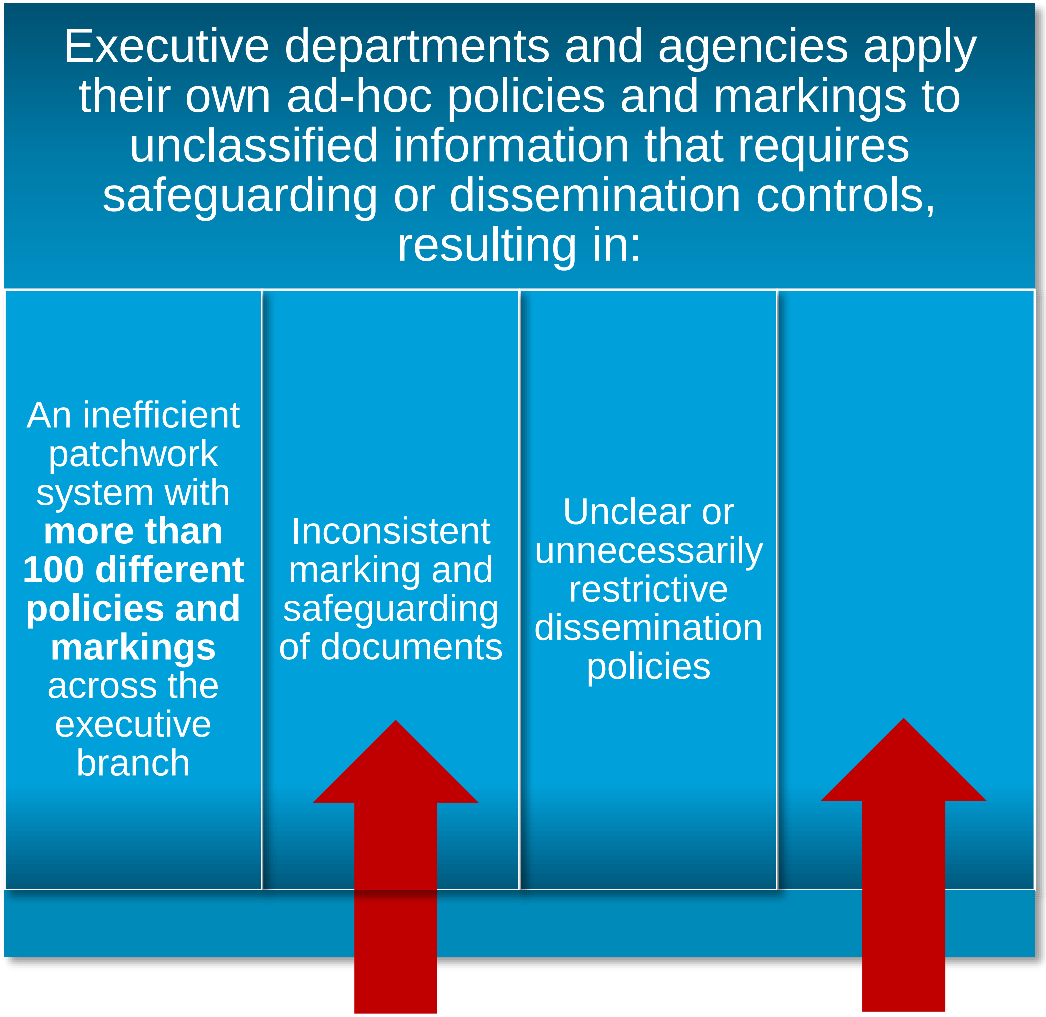
Executive Order 13556

Shared • Standardized • Transparent

Controlled
Unclassified
Information

Information Security Oversight Office (ISOO)

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

Executive Order 13556

68675

Federal Register
Vol. 75, No. 216
Tuesday, November 9, 2010

Presidential Documents

Title 3—

The President

Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose.* This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Sec. 2. *Controlled Unclassified Information (CUI).*

(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. *Review of Current Designations.*

(a) Each agency head shall, within 180 days of the date of this order:

(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

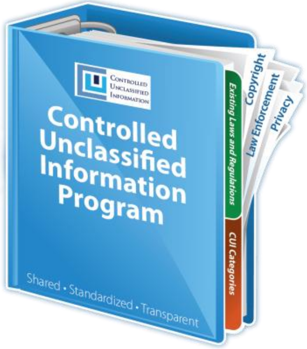
(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

Sec. 4. *Development of CUI Categories and Policies.*

- 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**


Controlled Unclassified Information
Controlled Unclassified Information Program
Shared • Standardized • Transparent
Existing Laws and Regulations
Copyright
Law Enforcement
Privacy
CUI Categories

- 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

CUI Registry

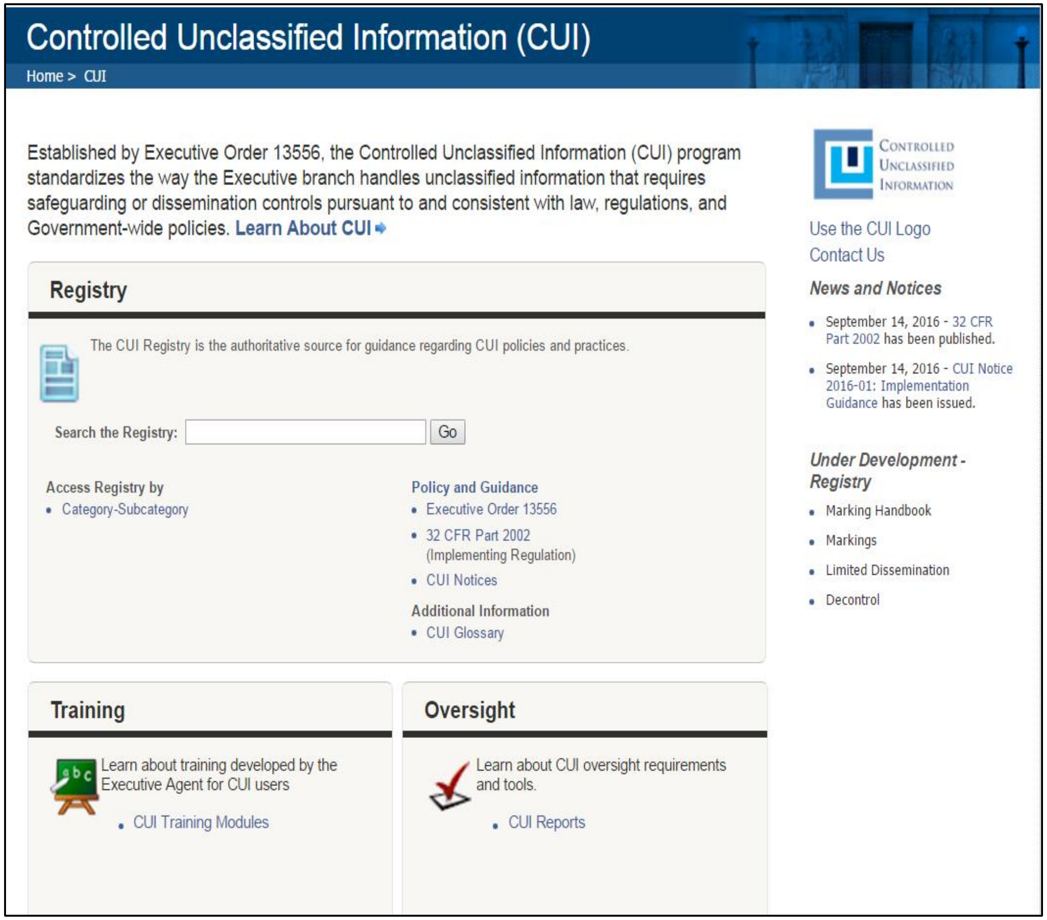
EO 13556 called for a review of the categories, subcategories, and markings currently used by agencies.

Agencies submitted over 2,200 authorities for controlling many types of information.

Information types were grouped together, legal authorities were examined, and a CUI Registry was published.

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

www.archives.gov/cui



Controlled Unclassified Information (CUI)

Home > CUI

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Learn About CUI ➡

Registry

The CUI Registry is the authoritative source for guidance regarding CUI policies and practices.

Search the Registry: [ ] Go

Access Registry by
- Category-Subcategory

Policy and Guidance
- Executive Order 13556
- 32 CFR Part 2002 (Implementing Regulation)
- CUI Notices

Additional Information
- CUI Glossary

Training

Learn about training developed by the Executive Agent for CUI users
- CUI Training Modules

Oversight

Learn about CUI oversight requirements and tools.
- CUI Reports

Controlled Unclassified Information

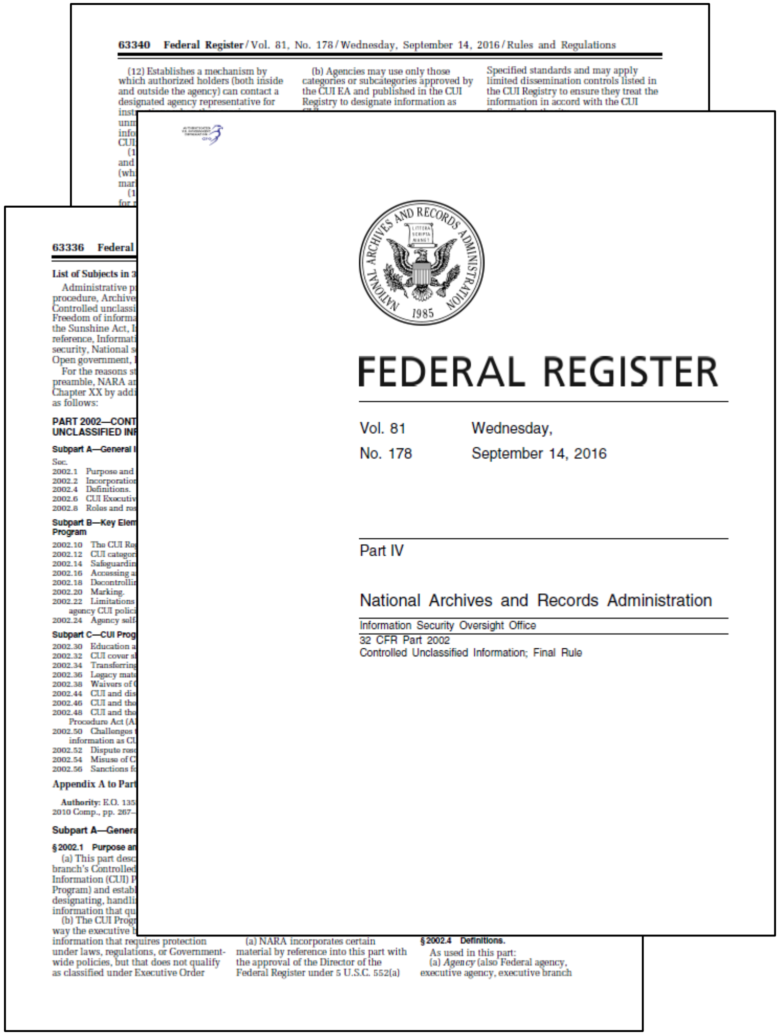
Use the CUI Logo

Contact Us

News and Notices
- September 14, 2016 - 32 CFR Part 2002 has been published.
- September 14, 2016 - CUI Notice 2016-01: Implementation Guidance has been issued.

Under Development - Registry
- Marking Handbook
- Markings
- Limited Dissemination
- Decontrol

32 CFR 2002 (September 14, 2016)



63340 Federal Register / Vol. 81, No. 178 / Wednesday, September 14, 2016 / Rules and Regulations

(12) Establishes a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for

(b) Agencies may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as

Specified standards and may apply limited dissemination controls listed in the CUI Registry to ensure they treat the information in accord with the CUI

FEDERAL REGISTER

Vol. 81 Wednesday,
No. 178 September 14, 2016

Part IV

National Archives and Records Administration

Information Security Oversight Office

32 CFR Part 2002
Controlled Unclassified Information; Final Rule

information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order

(a) NARA incorporates certain material by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a)

§ 2002.4 Definitions.

As used in this part:

(a) *Agency* (also Federal agency, executive agency, executive branch

- Implements the CUI Program
  - Establishes policy for designating, handling, and decontrolling information that qualifies as CUI
  - Effective : November 14, 2016 (Day 0)

- Describes, defines, and provides guidance on the minimum protections (derived from existing agency practices) for CUI
  - Physical and Electronic Environments
  - Marking
  - Sharing
  - Destruction
  - Decontrol

- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)

Controlled Unclassified Information

Information Systems and CUI

- Purpose of the CUI Program is to provide a uniform and consistent system for protecting CUI throughout executive branch.
- Baseline standard for protecting CUI is no less than moderate confidentiality.
  - Such protection is greater than low, the minimum requirements for all systems under the FISMA
  - Most agencies already configure their systems to Moderate for protection of information falling under the scope of the CUI Program.

NIST Special Publication 800-171

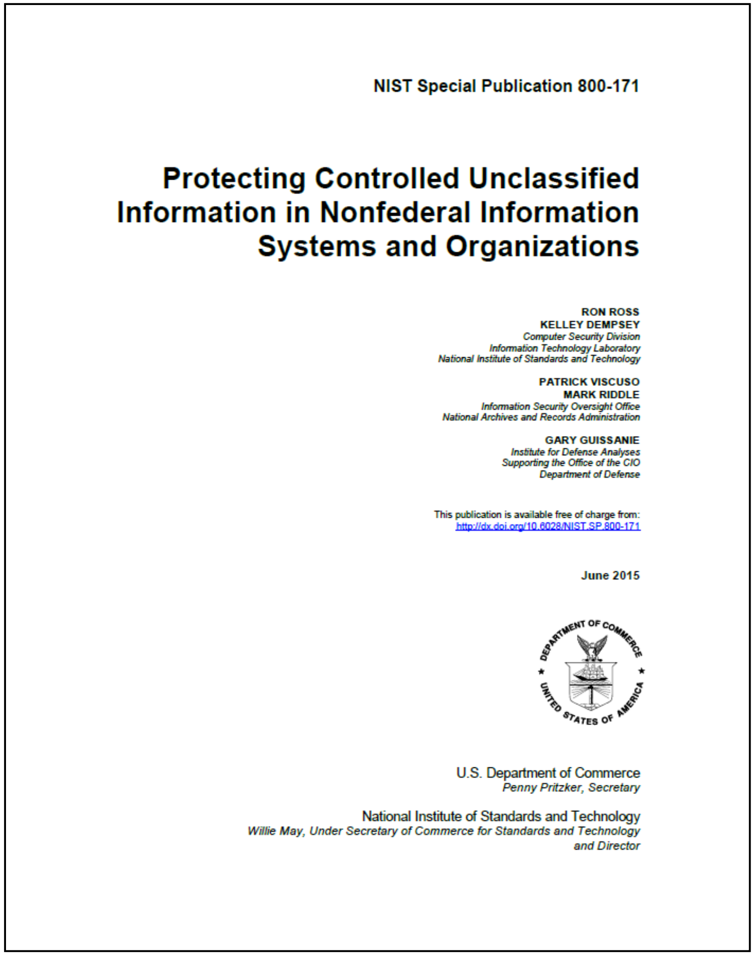
- Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems.

- The NIST 800-171 is intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations.

- Establishes requirements for protecting CUI at the Moderate Confidentiality Impact Value.

- Non-tailorable requirements

- Flexibility in how to meet requirements



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

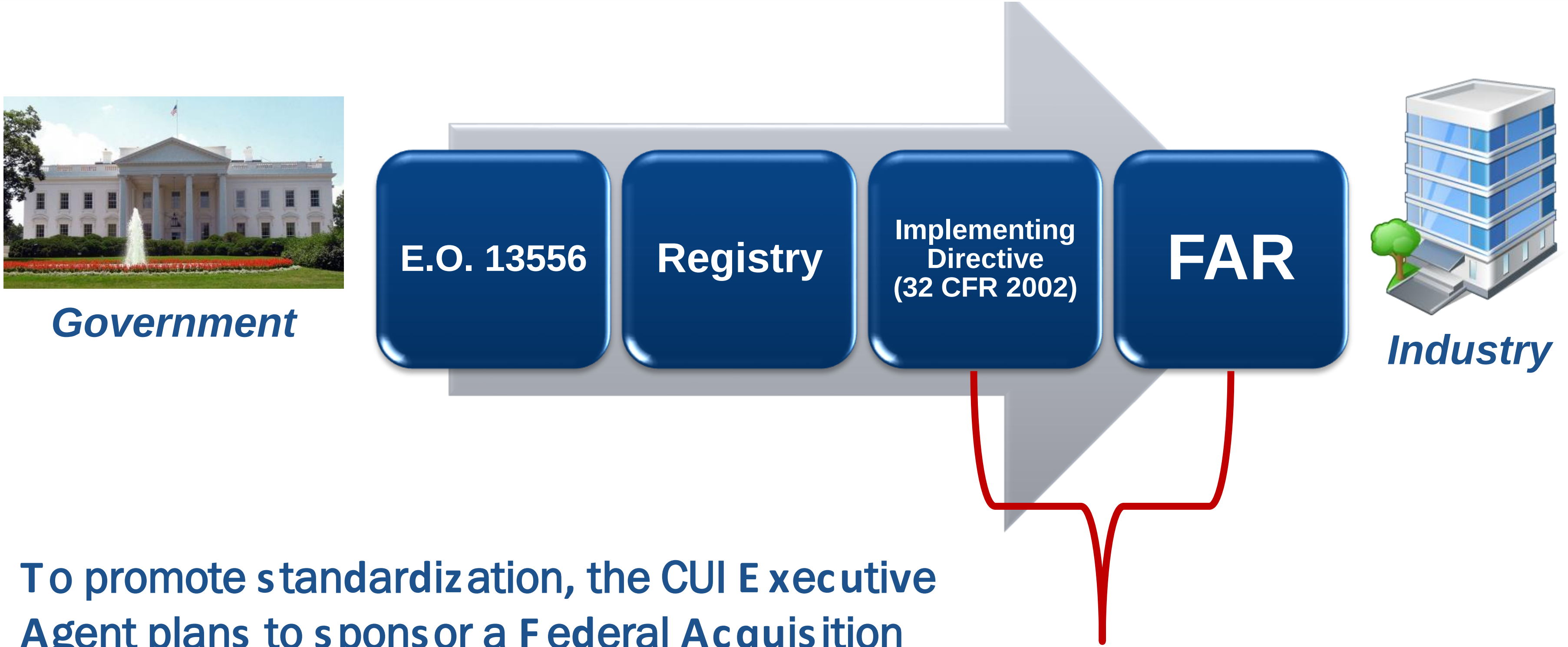
GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

June 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director



Government

E.O. 13556

Registry

Implementing Directive (32 CFR 2002)

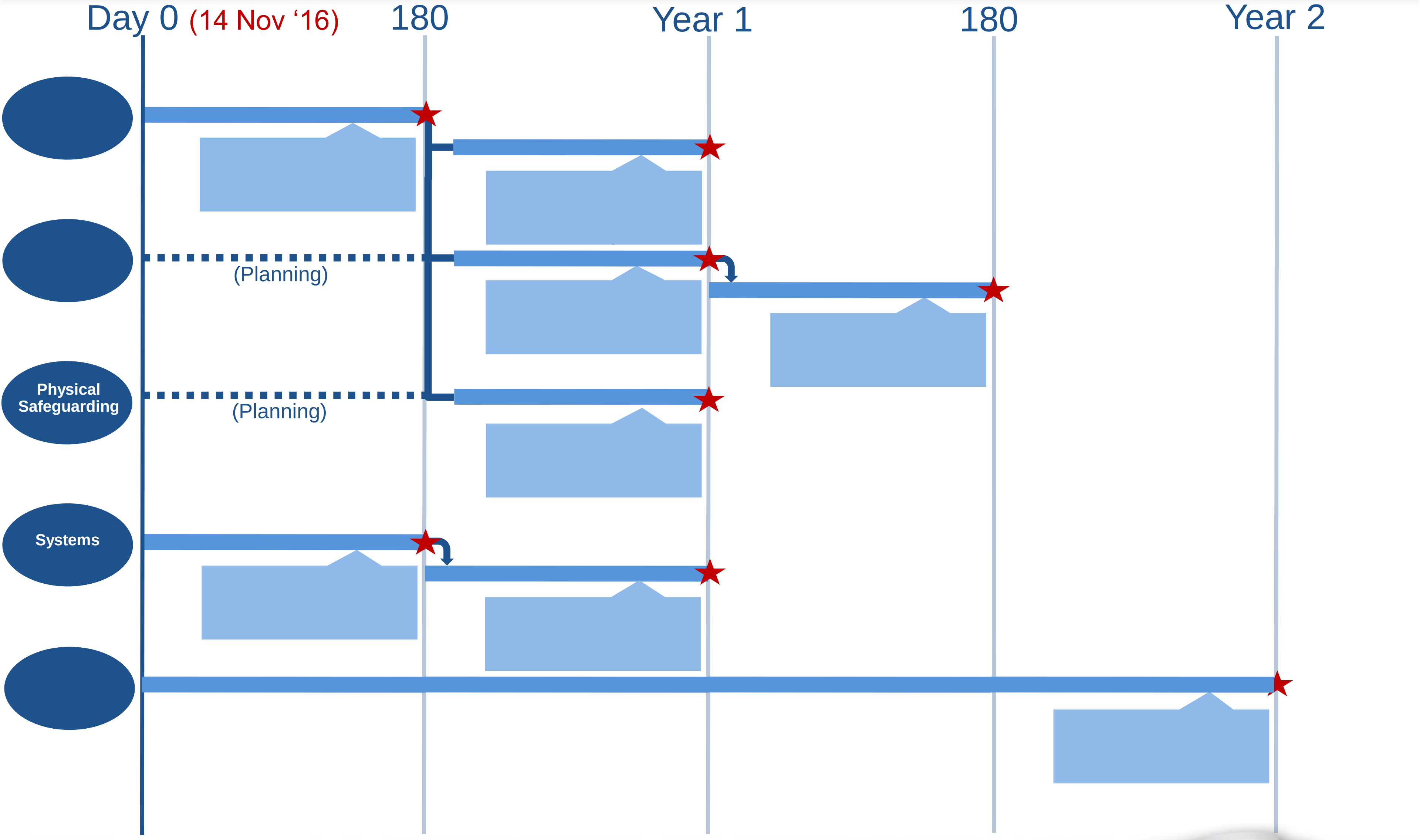
FAR

Industry

1 Year

To promote standardization, the CUI Executive Agent plans to sponsor a Federal Acquisition Regulation (FAR) clause that will apply the requirements contained in the 32 CFR Part 2002 and NIST SP 800-171 to industry.

Implementation of the CUI Program



Recommendations for Implementation

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

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

Briefings on CUI and Implementation

- Information Security Oversight Office will be providing briefings on the Controlled Unclassified Information Program. RSVP to mark.riddle@nara.gov

Virtual briefings:
Date: January 26, 2017
Time: 1000-1200
Date: February 14, 2017
Time: 1000-1200
Date: February 22, 2017
Time: 1000-1200

Additional information (i.e., call-in information and web links) will be forwarded to the attendee(s) prior to the event.

In-Person briefing:
Date: January 27, 2017
Time: 1000-1200
Location:

William G. McGowan Theater
700 Pennsylvania Avenue, NW
Washington DC

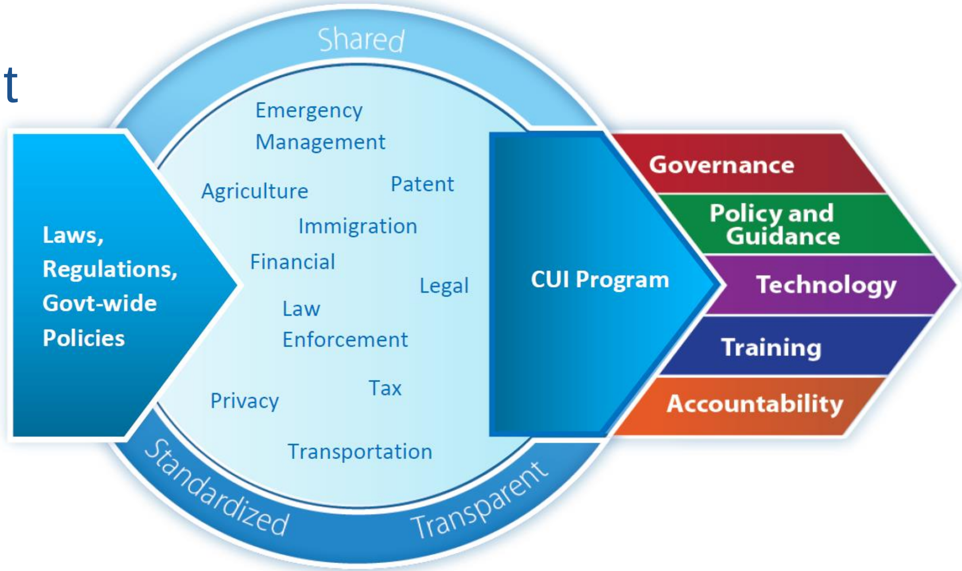
Attendees should enter through the “Special Events” entrance on the Constitution Avenue side of the building.

Questions?

Patrick Viscuso (202-357-5313)
Associate Director
Patrick.viscuso@nara.gov

Mark Riddle (202-357-6864)
Lead for Implementation and Oversight
mark.riddle@nara.gov

Devin Casey (202-357-6867)
Implementation and Oversight
devin.casey@nara.gov


Shared
Standardized
Transparent
Laws, Regulations, Govt-wide Policies
Emergency Management
Agriculture
Patent
Immigration
Financial
Legal
Law Enforcement
Privacy
Tax
Transportation
CUI Program
Governance
Policy and Guidance
Technology
Training
Accountability