MEMORANDUM FOR:	Judge William Webster, Chairman for Homeland Security Advisory Council
FROM:	Erin O'Connor, Executive Director, Homeland Security Advisory Council
DATE:	July 23, 2014
SUBJECT:	Review June 5, 2014 HSAC Meeting Minutes – Open and Closed Sessions

Purpose

Under Federal Advisory Committee Act (FACA) requirements, the Homeland Security Advisory Council (HSAC) is provided a period of ninety days to make meeting minutes—certified by the Chair for accuracy—available to the public.

Please find attached for your review and approval, both the open and closed session minutes of the June 5, 2014 meeting the Homeland Security Advisory Council. If these minutes meet with your approval, please date and sign in the space marked "Approve." If further discussion is required, please contact me at 202-447-3151.

Please let me know if I may be of assistance.

Recommendation

Approve the attached minutes.

Attachments

Approve: _____

Date: 7-28-14

Homeland Security Advisory Council (HSAC) Meeting- Open Session
U.S Coast Guard Headquarters
Washington, D.C. 20528

EXECUTIVE SUMMARY

1:45 to 4:15 p.m.
Thursday, June 5, 2014

Welcome by HSAC Leadership

Erin O'Connor, Executive Director of the Homeland Security Advisory Council (HSAC), introduced herself and welcomed HSAC members, speakers and members of the public to the meeting. After brief administrative remarks, she introduced Judge William Webster, who is the Chairman of the Homeland Security Advisory Council. Judge Webster has been a member of the Council since its inception in 2003.

Judge Webster introduced himself and welcomed the HSAC members, Department of Homeland Security (DHS) personnel, and members of the public. He informed those in attendance that the role of HSAC is to provide organizationally independent advice to the Secretary of the Department of Homeland Security and the Department's senior leaders. Judge Webster gave out the HSAC e-mail address (hsac@hq.dhs.gov) so members of the public could provide comment to the HSAC. He then introduced HSAC's Vice Chairman, Bill Bratton. He then invited the HSAC's Vice Chairman to make remarks.

Vice Chair Bratton thanked Judge Webster, greeted the Council members, and introduced himself as the Police Commissioner of the City of New York. He said he was excited to be with the Council in a new capacity since the last HSAC meeting, and was looking forward to engaging the Department to utilize the Council.

Judge Webster then addressed the Council, informing the body that Secretary Johnson would join the meeting later in the afternoon. He said the Council was fortunate to have Deputy Secretary Alejandro Mayorkas participating in the meeting. Chairman Webster then informed the Council that DHS is undergoing a series of changes and transitions, and reminded those in attendance that the HSAC is at the Secretary's service to provide organizationally independent advice and guidance to top leadership to help the Department of Homeland Security in all future endeavors. He concluded by introducing Vice Admiral Peter Neffenger, Vice Commandant of the United States Coast Guard (USCG) to address the HSAC.

Remarks by Senior Leadership

Vice Admiral Neffenger welcomed guests to the new United States Coast Guard headquarters building, the Douglas A. Munro Headquarters Building, named in tribute to a United States

Coast Guard Medal of Honor winner from the battle of Guadalcanal. Vice Admiral Neffenger informed guests that the Conference Center where the meeting was taking place is named after Ray Evans who earned the Navy Cross during the same battle of Guadalcanal. Following Vice Admiral Neffenger's remarks, Chairman Webster introduced Deputy Secretary Mayorkas and invited him to lead the first discussion.

Homeland Security Strategic Environment Discussion and Performance Improvement Discussion-DHS Business Process Reengineering

Deputy Secretary Mayorkas greeted the Council and spoke briefly about the Quadrennial Homeland Security Review (QHSR). He stated that given the breadth and expanse of the Department and the myriad responsibilities that we have, the Department must maintain its focus on the reason why DHS was created. That reason is to counter the terrorist threat and ensure the safety of the homeland. That is a principle point that Secretary Johnson has articulated very clearly both externally and within the Department. The landscape on which the Council operates is evolving with increasing rapidity, and is more dynamic that ever before.

Deputy Secretary Mayorkas discussed the differences in responding to a natural disaster verses a terrorist or cyber threat. The tools the terrorists or cyber actors have access to are increasing in sophistication. Their means and methods of operation are changing dramatically as are their capabilities and composition. He said the Department needs to be more agile today than ever before. It is an area of intense focus not just of the Secretary, but of all of the Component agencies that drive the operations of the Department. Deputy Secretary Mayorkas underscored the imperative of the department to adjust its operations based on a rapidly changing threat landscape. This new challenge is more acute, but creating greater opportunities for and drivers of organizational change as well. He invited member's into the discussion and turned the meeting over to Judge Webster. Judge Webster thanked Deputy Secretary Mayorkas and asked the members if they had comments or questions for him.

Mr. Augustine asked how the United States has been able to go a dozen years without another 9/11, and about what lessons could be learned from this experience. The Deputy Secretary answered over a number of years, we have learned a number of lessons from particular incidents and our responses to those incidents. He described the threat as imminent, and more accurately present. The threat activity is ongoing. The Deputy Secretary said our intelligence capabilities, as well as the dedication of the people is remarkable. Our technological capabilities are advancing continuously. He said that there is not one particular reason; but he emphasized the importance of an all government approach. There are sister Departments and agencies, such as the Department of Defense, that have extraordinary capabilities that have led to the safety of this country.

Ms. David talked about how the original founding of DHS was specifically to address terrorism threats. In the aftermath of Hurricane Katrina, there was a shift to an all-hazards approach. She

asked the Deputy Secretary to speak more about how the Department would achieve an appropriate balance between addressing the terrorist threat and the all-hazards approach.

Deputy Secretary Mayorkas responded by saying that the Department will maintain an all-hazards approach, and has become much more sophisticated in its disaster response capabilities. Deputy Secretary Mayorkas referred to an example previously described by Administrator Fugate of the Federal Emergency Management Agency (FEMA) regarding the Boston Marathon bombing. He said the traditional response for first responders would have been to evacuate all persons from the danger zone immediately. From a lessons learned approach, the exact opposite was carried out. The area was roped off and everyone was required to stay within the danger zone; this change led to the saving of a multitude of lives. This allowed for citizens who had health care skills to attend to those in the danger zone, while also enlisting citizens – some not medically trained – to assist in the application of tourniquets and other services. Many people who would have lost limbs or otherwise bled to death were saved by this evolved and advanced response.

The Deputy Secretary also made remarks regarding the Heart Bleed incident and the partnership between DHS, other government agencies, and other partners to ensure systems were patched in a rapid fashion, ensuring damage was minimized.

The Deputy Secretary finished by discussing how Department is putting forth a unity of effort when looking at problems that the Department encounters. The Department does not merely look to the operating Component that would most naturally respond to a problem, but rather brings to bear the comprehensive capabilities and authorities of the Department in ensuring Components are acting in concert, complimenting one another, and duplicating effort when duplicating is not a needless redundancy but actually brings greater operational strengths when resolving a problem.

Deputy Secretary Mayorkas then turned the meeting back over to Judge Webster who introduced Suzanne Spaulding, the Under Secretary of the National Protection and Programs Directorate (NPPD), to give a presentation on cybersecurity.

Cyber Discussion: Improving Security and Resilience of Cyberspace and Critical Infrastructure- Engaging Private Sector

Under Secretary (U/S) Suzanne Spaulding, National Protection and Programs Directorate (NPPD), provided an overview on how NPPD is instituting the Department's unity of effort initiative in cybersecurity. Within the Department, NPPD works closely with Components including Intelligence and Analysis (I&A), U.S. Secret Service (USSS), Immigration and Customs Enforcement (ICE), the Transportation Security Administration (TSA), U.S. Coast Guard (USCG), the Office of Privacy (PRIV), Civil Rights and Civil Liberties (CRCL), Office of General Counsel (OGC), as well as the Chief Information Officer (CIO) and Chief Security

Officer (CSO) within NPPD in efforts pertaining to cybersecurity. Each Component must work together and bring a unique perspective and set of skills to the mission of cybersecurity.

She then briefly talked about the Executive Order on Cybersecurity (EO 13636) and Presidential Policy Directive 21 (PPD 21) issued in February of 2013. PPD 21 specifically introduces the Secretary's responsibilities in critical infrastructure and promoting a unity of effort in this area.

She said it is fitting that Secretary Johnson and Deputy Secretary Mayorkas have brought a real unity of effort focus to the overall activities of the Department. Attention was then turned to the mission of NPPD. U/S Spaulding identified the overarching mission of NPPD as to strengthen security and resilience of critical infrastructure. She stressed how cybersecurity is a part of this mission. This mission cannot be looked at through stovepipes; integration is essential. She mentioned that this is one way NPPD brings unity of effort through an integrated approach.

Integration between physical and cybersecurity is the first critical piece of integration. The other important form of integration is between the government and the private sector. Unity of effort involves not only all aspects of the government across the country, including state, local, territorial, and tribal government, but also the private sectors. The traditional risk management framework begins with identifying threat. Although the government may have great insight into threat actors, the private sector has the best insight to the threats they face and the threats they are seeing in cyber space. Once the threat is identified we do a vulnerabilities and consequences assessment to ensure the resiliency of the potential target.

Dr. Phyllis Schneck, Deputy Undersecretary for Cybersecurity for NPPD, comes from the private sector and provides credible insight that needs to be utilized in order to make the private sector comfortable with sharing threat information with the government. The private and public sectors need to work together to take this information and make sure it is appropriately presented to a wider audience across the community. This has been a substantial challenge that is being worked on each day.

The private sector works closely with NPPD on cybersecurity efforts at the National Cybersecurity and Communications Integration Center (NCCIC). This combined efforts work to gain situational awareness and to develop mitigation measures. Additionally, on many occasions, cleared private sector personnel are called in to look at intelligence with the Department. Those private sector personnel offer a unique insight that government personnel do not necessarily have. They work with DHS to develop actionable unclassified intelligence products that the government can put out more broadly across sectors or throughout the affected sector so that appropriate responses can be made to the intelligence. Having private sector entities serve as true partners has been an invaluable relationship.

Other partnerships include working with the Secret Service, which has great insights into the threat environment and works to protect law enforcement equities while getting information disseminated in a timely fashion to the private sector for action. Valuable intelligence comes

from DHS Intelligence & Analysis (I&A). The Department disseminates this valuable information through sector coordinating councils and additionally the Information Sharing and Analysis Centers (ISAC), which traditionally focus on the cyber piece. The information dissemination through such entities helps break down the stovepipes.

Vulnerabilities are a place where the Department sees physical and cybersecurity inextricably intertwined. The Federal Protective Service (FPS), a part of NPPD, is responsible for facility protection, which includes a developed network of surveillance cameras which is vulnerable to cyber-attacks. Another example of the intertwined and interlinked nature of physical and cyber vulnerabilities are physical server rooms. An organization that fails to appropriately lock the physical door to the room where all their servers are stacked now has both physical and cyber vulnerabilities. Dr. Schneck stressed the importance of bringing Chief Security Officers (CSOs) and Chief Information Officers (CIOs) together to discuss security.

In order to help the private sector identify its vulnerabilities, the Department established the Critical Infrastructure Cyber Community (C^3 VP) Voluntary Program. It is used to help implement the cybersecurity framework. The C^3 Voluntary Program will assist stakeholders with understanding the use of the framework and other cyber risk management efforts.

NPPD performs continuous diagnostics and mitigation (CDM) that assists to identify and prioritize vulnerabilities in the .gov domain; NPPD has the lead in the .gov domain and coordinates support in the .com world. In U/S Spaulding's opinion, the area of assessment is neglected most in cybersecurity conversations.

U/S Spaulding stressed that NPPD must prioritize their actions in an overwhelming threat and vulnerability landscape to understand where consequences could be greatest. There needs to be an understanding as to what consequences should be most worried about in the event of a cyber-attack.

In order to understand interdependencies between cyber and physical, and potential cascading consequences, NPPD has taken personnel with years of experience analyzing physical consequences to create a level one/level two list of critical infrastructure assets around the country. NPPD has leveraged the extensive experience of its team by partnering with industrial control system cyber experts to look at consequences that could be caused through a cyber-event.

NPPD has responded to the President's directive to develop what they call the Section Nine List. This list is one which contains entities that a successful cyber-attack would cause consequences of catastrophic proportion. NPPD is working with the entities on this list to develop ways to mitigate those consequences.

Reducing risks across the physical and cyber domains continues to be an important priority. NPPD has learned that testing potential vulnerabilities is one of the most cost effective ways to mitigate consequences of a cyber-attack. To that effect, the electrical grid is not quite as

vulnerable as previously thought. The typical electrical industry infrastructure has more redundancy built in for cyber-attacks due to the relatively recent date of its construction. As such, cyber dependencies are often efficiencies that are built in. Within the electrical sector, there are many physical redundancies that are in place for electricity generation and transmission.

Finally, U/S Spaulding discussed the importance of enabling 'market drivers' to improve cybersecurity in this country. NPPD has spent time talking with CEOs from across various sectors, including electrical, and also with groups of individuals, such as venture capitalists, to improve cybersecurity. Through these partnerships, NPPD has developed very robust and collaborative working relationships and plans among and between the CEOs. Dr. Schenck has spoken to many venture capitalists, stressing the importance of how adequate cyber security is essential to protecting investments in companies. U/S Spaulding has been working with the American Bar Association (ABA), urging them to ensure that their stakeholders have adequate cybersecurity in order to do due diligence for clients. U/S Spaulding stressed that this is a unity of effort between the governmental sector and private sector to push effective cybersecurity. She went on to state how they need the best and brightest individuals from across the country and the support of the HSAC to ensure cybersecurity. U/S Spaulding closed by sharing her appreciation for the opportunity to update the Council on NPPD's efforts on cybersecurity.

Chairman Webster thanked U/S Spaulding and then asked if she felt if the Department was doing enough to engage the corporate leadership in adequately protecting their own infrastructure. U/S Spaulding responded that the Department works to engage corporate America at all levels, but they always welcome any suggestions from the Council. In addition to direct involvement with CEOs, CIOs, and CSOs, the Department is working with organizations such as the Chamber of Commerce and the Business Roundtable, who often have broader reach than the Department can have alone.

Mr. Magaw commented that private sector and public sector partnerships are of key importance. Hiring individuals from the private sector into the public sector is good progress. He said the other challenge is trust. Historically there is a sense of lack of trust between the private and public sectors. Mr. Magaw briefly discussed the credit card problem and the hesitation of the private sector to discuss the crisis with the government due to a lack of trust. He stated he was pleased by the efforts of U/S Spaulding and feels they are steps in the right direction.

Ambassador Jones asked about the status of the hiring and training of cyber experts (600 personnel), especially with the fact that the private sector can incentivize people with higher salaries then the government. U/S Spaulding replied that since the government cannot compete with the private sector in terms of salaries, the government must attract the best and brightest with its mission. The Department has established pipelines into community colleges, starting in high schools all the way up to PhD programs, such as Georgia Tech. In each of these locations, the Department attempts to convey a sense of excitement for the mission and hopes to attract

candidates on that basis. Additionally, the Department is disadvantaged in hiring within the government, due to the nature of its hiring authority. The Department has been working closely with Congress to improve the hiring authority, seeking more flexibility and expediency. Dr. Schneck echoed U/S Spaulding's sentiments about needing to attract people to the government with its mission, and also felt that the hiring process needs to be improved, so that it does not take as much time. Revised hiring authorities would better enable NPPD to compete with the private sector and with other governmental entities for this talent.

Ms. Lute stated that the Task Force on CyberSkills workforce, co-chaired by Jeff Moss, and now under the direction of Deputy Secretary Mayorkas, has highlighted the ways in which we should look at cybersecurity responsibilities distributed in the workforce. The first group is comprised of the highly specialized cybersecurity experts; these are the 600 people that Ambassador Jones mentioned previously. The second group contain professionals who are not cybersecurity experts but specialists in other areas such as electoral engineers, gas and oil specialists, health IT, or law enforcement IT professionals. These individuals need a degree of education and competence on cybersecurity, without having to turn them into cybersecurity experts. The Department has been working with Departments in the Federal government and partners in the private sector. The rest of the employees comprise the third group. These employees need a level of cybersecurity awareness and engagement only. The Department approaches these employees through the National Initiative for Cybersecurity Education (NICE) and others. A lot of that traces its work back to this Council and the Task Force on CyberSkills. In her opinion, Deputy Secretary Mayorkas, U/S Spaulding, and Dr. Schneck are working diligently on the development of these workforce efforts.

Congresswoman Holtzman asked U/S Spaulding to elaborate on the sixteen sectors of critical infrastructure. Specifically, Congresswoman Holtzman inquired whether goals and timetables, for each of the sixteen areas, had been developed to determine how vulnerable we are now and where we want to be six months or a year from now.

U/S Spaulding responded that such goals and timetables haven't existed, in any formalized or methodical way, for all sixteen sectors. In accordance with President's Policy Directive 21 (PPD 21), an updated National Infrastructure Protection Plan (NIPP) for the year 2013 was issued. One key action of NIPP 2013 was to work with each of the 16 sectors to develop strategic plans and joint priorities with defined tasks and milestones. Congresswoman Holtzman followed up by asking U/S Spaulding when this action would be accomplished. U/S Spaulding stated that it is her hope that by the end of the year, after collaboration with our private sector councils, this action could be achieved.

Mr. Moss reflected that one of the questions, stemming from the CyberSkills Task Force, centered on the balance between full-time employees versus contractors. The concern expressed was if DHS was to rely upon contractors for expertise, then our workforce needs to be better at private management and the management of external contractors. It is important for the

government to ensure that only products and services that are needed are purchased and delivered. Mr. Moss requested the panel address the mixture between full-time employees versus outside expertise.

U/S Spaulding stated that both full-time employees and contractors are needed. She remarked that the Department needs to be stronger at project management. NPPD leadership is aware of the importance of strong program and project management and is currently focusing more resources in that area to enable growth and improvement. The Department relies upon the private sector and contractors, particularly in evolving technology arenas. U/S Spaulding mentioned the Department's intrusion detection and prevention 'Einstein Program'. Historically, government has viewed its role as giving the private sector requirements and specifications for technological solutions. When delivered, the IT solutions often are out of date. To advance the government's approach, NPPD is now stating desired outcomes. Contractors are asked to provide information on how they are going to reach and sustain the outcome. With this change in approach, the burden to innovate rests on the technology world. Although this is a much more difficult approach, U/S Spaulding stated that she believed it will serve the Department well. To successfully employ such an approach, DHS must have strong project and program managers. Although DHS has some, more are needed to be successful.

Mr. Augustine asked to what extent red teams were being used effectively within government and how the government is encouraging private industry to use them.

Deputy Under Secretary Schneck said that red teams are utilized within DHS and there are DHS red teams that collaborate with other Federal agencies due to the significant cyber-threat challenge. Dr. Schneck reminded the Council that adversaries do not operate within the law, are not required to have a lawyer, often have plenty of money for execution, and have developed a strong network of partnerships. Given these factors and advantages, the government must take and train people who aren't thinking the way the network builders initially thought and go in the backdoor and see if they can think like the adversary. The Department is trying to build a team of analytics experts that understand high-performance computing. Red teams are formed to serve as human analysts for the networks of federal agencies.

Dr. Schneck remarked that she does not look at teams as contractors or federal employees. As cyber-threats can impact all aspects of life, it is important to identify unified teams, which understand the current threat, and take action immediately. The Department must build stronger and sharper teams. Unlike many other entities, DHS has a remarkably strong partnership with its Privacy Office; it is a civilian agency, which honors privacy and civil liberties in full transparency. Given the need for strong public and private partnership, everything in cyber should bring a 'See Something, Say Something' approach. This means that when DHS senses something crossing into its network, DHS should be able to tell everybody in the world whether it was good or bad. Information must be disseminated rapidly, 24/7. DHS must gather the intelligence, using different skill sets and automated protocols, adding what DHS systems sense

and disseminate analyzed information, in a rapid sequence, from our machines to other machines. Combining sophisticated technology with human analytics is the only way for the red teams to be elite. In addition to the Department's red teams, the Department has flyaway teams that stem from the National Cybersecurity and Communications Integration Center (NCCIC). These teams are formed with partnerships between Secret Service and the FBI.

Deputy Secretary Mayorkas said the private sector engages with the government to appropriately share information that will benefit other private sector entities. The more information that is appropriately shared from different sources provides the government a greater understanding of the cybersecurity landscape. This greater understanding allows the government to provide better advice and implement measures to maintain and increase the national cyber hygiene level. Deputy Secretary Mayorkas identified two challenges that face NPPD. The first challenge is trust. Currently, there remains significant public controversy regarding data disclosure and public sensitivity regarding private sector corporations providing information to the government for the purposes of data collection and use. Private sector partners remain concerned as well. The second challenge is liability. There is a significant amount of legislative activity around to what extent private companies are exposed to liability by providing information to the government. He said that there is a lack of consensus, which is currently bogging up legislation.

Mr. Adegbite requested an update on the progress and operational changes that have occurred to support employee retention and in-house employee skill-growth. He also requested that the panel address whether progress has been made to retain key talent from moving to the private sector and away from the Department's mission. Mr. Adegbite recognized that this is an issue that the private sector also struggles with. He acknowledged that it has been a relatively short amount of time since the HSAC Task Force on CyberSkills report was completed.

Dr. Schneck responded that there are two primary reasons that talented individuals typically leave for the private sector. They include financial reasons (higher pay) and frustration with the government. Although DHS cannot compete with the private sector on salaries, the Department is doing a lot to create an environment that people do not want to leave. She believes the importance of the mission where people feel they are making a real difference through innovation, have room for promotion, and are working with leadership to help shape the future. DHS is creating an environment where the Department is responsible for innovation, not just funding it. Dr. Schneck remarked that two new exceptional leaders have joined their team. They are: Assistant Secretary of the Office of Cybersecurity & Communications, Dr. Andy Ozment; and Deputy Assistant Secretary for Cybersecurity Operations and Programs, General Gregory Touhill. Leadership is ensuring that all employees are charged with helping to build the mission. With this approach, NPPD is creating an environment that people want to work in. U/S Spaulding added that she thinks the statistics show that retention rates have improved and there is less turn over than one would expect given the challenges. She reaffirmed that retention rates are better than expected and concurred with the reasons Dr. Schneck outlined.

Ms. Thomas emphasized that cybersecurity is a national challenge and requires close interactions between the private sector and the government. She commended the Department for their conversations with venture capitalists and CEOs; however, she wanted to know if there was interaction with the investment banking community.

Dr. Schneck indicated that DHS was also interacting with the investment banking community in many areas. The banks have information sharing analysis centers, and have been early adopters to the Department's automated security indicator protocol. This protocol means the Department has developed ways to use the speed of machines to send information about what safe web traffic is and protocols to accept such traffic. Additionally, Secretary Johnson met with the top executives from the banking industry. The Secretary had a candid meeting with these executives to discuss their challenges, hear input from the banking industry executives, gauge their understanding of DHS, and to seek input.

Ms. Thomas asked if there could be a more specific answer to the interaction with investment bankers.

U/S Spaulding stated that they were being included. Part of the ongoing conversation includes discussion regarding what the Department can do to work collaboratively with them, to ensure their own cybersecurity. The conversation includes what they can do to be force multipliers and market drivers, just as the venture capitalists and private equity firms are. There is a cross cutting approach between sectors, which must also exist in cybersecurity, since all of the previously mentioned entities consume cybersecurity. There must be an inclusion of cybersecurity in supply chain resilience considerations; consumers must be educated. It is important to ensure one's own cybersecurity and also that of third parties and vendors, where interactions occur. Cybersecurity needs to be a part of an organization's supply chain resilience considerations. Target Corporation was raised as an example; they failed to ensure that vendors had adequate cybersecurity which opened up significant vulnerabilities for them. Ensuring that systems are adequately secure is important before intellectual property is placed in a non-secure environment. There is a need for more educated consumers.

General Allen commented that only so much could be done with Executive Orders (EOs) and Presidential Policy Directives (PPDs). He wanted to know the status of legislative initiatives and what would change with the passage of proposed legislation. He also inquired the effect that the passage of cyber legislation would have on the Department, specifically related to cybersecurity, if all requested items are passed.

U/S Spaulding spoke regarding her earlier reference to legislation that would give the Department more hiring flexibility and authorities; she feels progress is being made in this area. Another piece of legislation she discussed was requested reforms to the Federal Information Security Management Act (FISMA). It is the hope that the current cumbersome process, involving compliance based checklists, can be revolutionized using the continuous diagnostics

and mitigation program. These changes are beginning to be instituted at departments and agencies now. This change would provide a near real time surveillance of the network health and help identify places that need to be addressed and prioritized on a continuous basis. Although there are great efficiencies and savings, without legislative relief, it is difficult for agencies to free up the resources to move in a more effective and revolutionary way of doing diagnosis and mitigation. It is NPPD's responsibility to ensure the cybersecurity of the .gov domain and work with CIOs and CSOs of other departments and agencies, piggybacking on OMB's authorities which have been delegated to NPPD. Having more clear authorities would be beneficial to ensure the Department could move much more quickly on crisis. For example, during Heartbleed, lawyers raised a question regarding what authorities the Department had to come in. The current legislative framework pre-dates many of the current responsibilities of the Department. Clarification of authorities is necessary through new legislation.

U/S Spaulding then went on to discuss how privacy considerations could be strengthened. Another area that the Department could support legislation is in the liabilities associated with information sharing. The Department would benefit from increased clarity in the law regarding as to what can and cannot be shared, and how to do so. In U/S Spaulding's opinion, the Department and Administration could also support narrowly focused, targeted liability protection. It would be beneficial to ensure clear lines and clear authorities were established. Another important area for improvement includes actions taken, with government furnished information; this includes occasions when the private sector acts based on information which the government provides. Due to the strong public policy behind liability, this is a lot harder to work through. Narrowly scoped and targeted liability protection is something that NPPD could support.

Deputy Secretary Mayorkas added two thoughts. First, he commented that General Allen was correct in his assessment that PPDs and EOs are limited in their scope, especially within the private sector and can only have a certain effect. Cybersecurity is a relatively new phenomenon, at least to the degree that the Department is experiencing and on a comparative basis. In his opinion, legislation would provide codification and better assist an all government approach to cybersecurity. Secondly, the Deputy Secretary stated that liability concerns make entities hesitate in providing information. If there were liability sections, limiting liability, there would likely be more support for information sharing. He personally is interested in seeing whether disclosure law would function in the cyber realm. For example, would cyber intrusion be viewed as material and therefore compelling disclosure either qualitatively or quantitatively, and whether the regulatory framework actually begins to address that? Deputy Secretary Mayorkas believes that we may see some activity in that area in the near future. U/S Spaulding stated that a final legislative priority is federal breach notification. Currently, the Department is reliant upon an intermittent patchwork of state breach notification laws.

Mayor Parker expressed concern that cities may not be doing enough to protect their cybersecurity infrastructure. She wanted to know what was being done at the city-level to

protect critical infrastructure. Dr. Schneck fielded the question by talking about how the C^3 Voluntary Program is used to reach out to the state and local levels. One of the first things that was done upon Dr. Schneck's arrival at the Department was to allocated funds to all 50 states for their managed security services. Using this funding, the states used the high level guidelines of the Framework for Improving Critical Infrastructure Cybersecurity, Version 1, National Institutes of Technology, February 2014 as they individually reviewed how their state would improve their own cybersecurity programs. The funding for this program is short-term, but the state will be able to bring cybersecurity to their governor to determine how to invest over the next years, even with slim resources. Part of the reason that the state, local, and city levels have unsecure environments is due to funding. Many state and local jurisdictions realize that their networks are not secure, but simply do not have the funding to handle the process of securing their infrastructures. Dr. Schneck believes that a portion of the needed funding will come due to an increased awareness and activity from both the government and private sector in relation to cybersecurity. In relation to the budget, cybersecurity needs to be seen to have the importance of other risk and consequence equations. Utilizing the multi-state Information Sharing and Analysis Center (ISAC), state governments have the opportunity to get secured while at the same time looking at how to better allocate money in the future to improve cybersecurity efforts. Additionally, it is important for cybersecurity to be seen as something that is worth investing in from a risk management perspective. Such basic cybersecurity measures do not require an enormous amount of money. States can make some good improvements without spending everything the vendors would want them to spend.

Mayor Parker followed up by stating that she feels that clear standards should be the first step achieved; cities know that they have problems, but they do not know necessarily know how to solve them. U/S Spaulding replied that pursuant to the President's February 2013, Executive Order, Improving Critical Infrastructure Cybersecurity, they are looking at various ways to incentivize the adoption of the cybersecurity framework.

Specifically, they are looking at how to make grant programs appropriate for cybersecurity improvements. Recently U/S Spaulding was in Philadelphia talking with stakeholders about the transition away from Windows XP. This represented a huge financial burden for the city. The Department must be advocates for stakeholders, both within the government and the private sector. The Department does this by getting out and talking about the threats and consequences that can occur, in order to help prioritize the allocation of resources. U/S Spaulding said that they welcome any recommendations regarding how the Department can provide better assistance.

Ms. Lute brought up that under the Multi-State Information Sharing & Analysis Center (MS-ISAC), which many signed onto with the National Governor's Association and the Council on Cyber Security. The MS-ISAC focuses on four key measures that address four important questions. These measures are featured in ongoing diagnostics and mitigation which eliminates between 80 and 90% of all known attacks. These four questions are:

1. Do we know what is connected to our networks?
2. Do we know what is running (or trying to run) on our networks?
3. Are we limiting and managing those who have administrative permission to change, bypass, or override the security controls?
4. Is there a continuous diagnostics and mitigation CDM like in DHS in place to get the functioning machines to detect any behaviors of vulnerabilities that would be considered anomalies and allow us to patch in at real time?

If there were to be a fifth question, Ms. Lute said it should be to ask your CIO how he/she would demonstrate all of the answers. Ms. Lute concluded by saying that there is a national campaign that the MS-ISAC, National Governor's Association, and the Council on Cyber Security has developed in order to underpin the NIST framework, DHS's agenda, and to enhance the message that cyber is an integral part of infrastructure security, and without it you are not secure.

Mr. Magaw asked whether there is currently a sabbatical program that allows personnel to be sent to the private sector or vice versa to ensure that there is a trade back and forth. In his opinion, it is a very positive interaction if it can be kept at a high-level and be a priority. U/S Spaulding responded by talking about the Loaned Executive Program. This program allows private sector expertise to be brought into the Department; both the Secretary and Deputy Secretary support this program. The bigger challenge is to find a way to get DHS personnel to spend time in the private sector; there have been conversations with some stakeholders to try to develop a plan. U/S Spaulding believes there is huge value to such an arrangement and appreciated the suggestion.

Judge Webster thanked the members for the interesting discussion and attention given to cybersecurity and reminded the DHS Leadership that he hoped that they would use the Council to help in any ways needed. He then introduced Bonnie Michelman, HSAC member and the Chair of the Faith-based Security and Communication Advisory Subcommittee (FBAC), to give a report out on the recommendations of the subcommittee.

Faith Based Security and Communications Subcommittee Report

Bonnie Michelman introduced herself as the Chair of the Homeland Security Advisory Council's Faith-based Security and Communication Advisory Subcommittee (FBAC). She thanked her co vice chairs, John Hodson and Paul Goldenberg. Bonnie In addition, she thanked the members of FBAC as well as Mohamed Elibiary and Ali Soufan, the only other HSAC member on the Subcommittee.

Ms. Michelman spoke about how FBAC's membership is some of the best people and leaders, representing different cultures, religions and philosophies. Over the past three years, the group has developed significant trust and friendship between each community. Members of this Subcommittee deeply care about security of everyone's faith community, not just their own. The members have come together several times as individuals in order to support each other during

tough times. Over the course of the FBAC's work, the Subcommittee witnessed attacks on the Sikh community, the Catholic community, the Jewish community, and the Muslim community, among others. Members of the FBAC, in their individual capacity have gone to each of these respective places to proactively offer support, help, and guidance. FBAC unified when the group came together to help DHS understand what faith-based communities need from DHS and vice versa. That conversation has evolved. Now FBAC is structuring discussions about not only what each community needs from DHS, but also how DHS can assist in the conversation between the faith-based communities. Ms. Michelman thanked the FBAC's DHS partners, John Cohen, Acting Under Secretary of Intelligence and Analysis, Bill Flynn, Principle Deputy Assistant Secretary for the Office of Infrastructure Protection, Erin O'Connor, Homeland Security Advisory Council Executive Director, and Mike Miron, Homeland Security Advisory Council Director. Ms. Michelman also thanked Mr. Miron for his innovative support, listening and helping the Subcommittee move forward.

In May of 2012, FBAC issued their first set of findings and recommendations. They focused on faith-based organizations and how DHS could continue to improve upon bi-directional homeland security information sharing and the resilience, as well as the protection of faith-based organizations who are often unsung heroes of national and local response. Ms. Michelman expressed that she was pleased to hear U/S Spaulding and Deputy Secretary Mayorkas speak about the importance of involving the private sector in bi-directional communication and sharing intelligence with them. In October 2012, former Secretary Napolitano reaffirmed the importance of the FBAC as a subcommittee of the HSAC.

FBAC's value statement says, "The members of the faith-based organization who serve in the Department of Homeland Security Advisory Council's FBAC strongly and uniformly denounce violence against any other faith-based organization to include their houses of worship and those who worship. When any threat targets one member of the faith-based community, they target all of us and they'll be met with stiff resistance in their attempt to divide us against hate."

Ms. Michelman continued with the guiding principles of the FBAC, which are to ensure a more augmented outreach and training program in order to achieve social cohesion between the faith-based organizations and also with DHS. The FBAC issued a report in May of 2012 to be used as a foundational document by the White House as they created model emergency management plans for schools, institutions of higher education, and houses of worship. This effort was part of the implementation of the President's 23 Executive Actions to Reduce Gun Violence in January of 2013. Additionally, Former Secretary Napolitano also moderated a session on houses of worship which was conducted at the White House. Panelists included FBAC members Paul Goldenberg and Mary Marr. FBAC members in their individual capacities continued to support other communities in times of need.

After the 2013 Boston Marathon bombing, many members of the FBAC signed onto or issued statements calling for the unity of all faiths and partnerships with law enforcement in the

aftermath of the Boston Marathon tragedy. More recently, the FBAC has worked cooperatively and collaboratively in the response to the Overland Campus incident.

Ms. Michelman stated there are many benefits for the Department and its relationship with the FBAC. This includes information sharing and providing timely, actionable bidirectional information from trusted reliable partners. These approaches have been used in many different ways. This is a new formalized methodology that did not exist before.

The FBAC members have also supported four table-top training exercises (TTX) in the past year, as well as one large one. These exercises focused on information sharing and present partnership development with mitigation, sector wide enhancement, and lessons learned. Exercises were held in Dearborn, Michigan, Bridgewater, New Jersey, Salt Lake City, Utah, and Dallas, Texas. Each focused on information sharing and present partnership development with mitigation, sector wide enhancement and lessons learned. The table-top activities were phenomenally successful.

In May of 2012, recommendations also provided a forum for other localized training. This included a training held in Cook County, Chicago on Countering Violent Extremism (CVE), led by Michael Masters.

In addition to the formal recommendations of the Subcommittee, many members have been called upon to provide individual feedback on DHS domestic policies, which may have local and tactical relationships. Human and material resources are strategic assets to ongoing security mitigation. Working with faith-based organizations, this partnership is a valuable link for successful and sound leadership nationally and locally.

The recommendations from the FBAC are:

1.) DHS should designate a single point of contact between DHS and faith-based organizations for security related issues. This contact would help to continue building relationships at the national, state, and local levels; continue to develop faith-based organizations two-way informational sharing in a formalized way, and would continue to develop FBO's training; continue to develop and implement an FBO incident-based crisis communication plan; continue receiving calls and emails from faith-based organizations on security-related issues; and would identify and provide such opportunities for faith-based organization funding.
2.) DHS should fund additional faith-based organization centric tabletop as well as functional exercises in fiscal year 2014 and 2015, with specific focus on issues of critical importance such as active shooter scenarios and violent extremism.
3.) DHS should continue to develop and enhance relationships and bidirectional communication with faith-based organizations, protective security advisors, center personnel, and local law enforcement to further Homeland Security information sharing and intelligence sharing.

4.) Finally, the FBAC will meet in person in the fall of 2014 in order to prepare the Subcommittee'snext Report to the HSAC.

Bonnie Michelman then turned the meeting over to Vice Chair of the FBAC, Paul Goldenberg.

Mr. Goldenberg spoke of visiting a Jewish kindergarten in Berlin for a meeting in regards to the OSCE, through his role as Senior Law Enforcement Advisor; they were there to address a rise of extremism, neo-Nazism. The kindergarten was well protected with guards holding machine guns and barbed wire fences surrounding the building; Mr. Goldenberg stated how he believed nothing like this would ever happen in the U.S.

Many things bring the members in the room together as Americans, but two things that specifically do so are children and safety in each person's respective house of worship. It is extremely important that there is a connection to the local police from houses of worship. Just as important is that there is a connection to the state police agencies and beyond.

In the Kansas shooting, DHS was on the ground within an hour. The Protective Security Advisors (PSAs) were on the ground then, and are still there working and empowering the committee to be force multipliers. Two PSAs are training individuals in Kansas on how to identify suspicious incidents. The PSAs have been working very closely with the faith-based groups and educating these groups; unfortunately, the more PSAs educate the more they are finding out faith- based groups are subject to attack. It does however provide information that is needed to better protect the country. Prior to the FBAC, there was no "911" for houses of worship to pick up the phone and be able to connect with Homeland Security. Connections to DHS, state police and local police agencies are critical for faith-based organizations. Empowerment and sharing knowledge are very important.

Many faith-based institutions are also subject to cyber-attacks as well. These attacks are continuous and happen every day.

Paul Goldenberg finished by thanking DHS for the good work they have done in this area.

Ms. Michelman finished by acknowledging that there is still a lot of work and education left to do, yet the work is being done at a table of 35 or 40 people who make a great team. She expressed hope that the HSAC would adopt the recommendations.

HSAC Deliberation and Approval of Faith-Based Interim Report

Judge Webster asked the HSAC to vote on approval of the interim report and if there was any discussion. There was no discussion and a vote was taken and the motion passed by acclamation that the report be sent to Secretary Johnson for his review and possible implementation..

Trade and Travel Facilitation Discussion

Deputy Secretary Mayorkas informed the HSAC that the largest effort currently underway regarding trade is the International Trade Data System (ITDS) by executive order of the President. Trade and travel facilitation is a significant focus of the Department. Deputy Secretary Mayorkas remarked that there is often a preconception that the facilitation of trade and travel is at odds with our national security, but he believes that is a false paradigm. There might be some tensions with the facilitation of trade and travel, but progress can be made without encroaching upon our responsibilities for security. The ITDS is a trade single window through which the trade industry is supposed to interact with the government on the movement of cargo and goods.

Pursuant to the President's directive, DHS is to complete the development of ITDS by the end of the calendar year of 2016, which is a very significant technological undertaking. This effort involves many Federal agencies; however, DHS is designated as the lead.

While discussing the facilitation of travel, the Deputy Secretary raised tourism as an area where DHS needs to partner more closely with the private sector. As of now, there is limited legislative authority for that partnership. An expansion of this legislative authority would greatly benefit DHS and the private sector community.

Preclearance provides an example of where the national security imperative coincides perfectly with the economic imperative. The Secretary has expressed publicly that his intention is to push forward on the expansion of preclearance around the world and has just returned from a trip to the Middle East, where a portion of the agenda was about preclearance.

DHS is speaking with other countries in Europe and Asia about preclearance. Preclearance, from a national security prospective, provides greater security, as the nation can ensure that the individuals boarding planes do not pose a threat to the United States. It is better to know if someone poses a threat before the individual boards the plane, rather than after that individual has landed within United States. Domestic airports have many challenges with respect to the movement of passengers. If DHS is able to shift some of the security responsibilities to the front-end of the travel process it will help yield better service within domestic airports.

To deal with line management, DHS is attempting to partner with the private sector in novel ways. This is an area where the Council may be able to assist. Recently DHS issued requests of proposals for private industry to loan executives to DHS -- experienced individuals to come into the government, paid by their private sector employers, but to work with DHS on a temporary but full-time basis to provide advice for six months to a year. Executives may come with expertise in management, marketing, or the development of metrics to ensure top performance. These individuals could share with the Department the private sector perspective, the private sector best practices and their expertise. Disney, Universal Studios, and Knotts Berry Farm all serve as tourist destinations. They are well advanced in the science of line management, and DHS would greatly benefit by importing such talent.

Dealing with customer service, the Transportation Security Administration (TSA) and Customs and Border Protection (CBP) have made great strides in their entry process with TSA Pre-Check and similar programs. However, companies that have spent millions and millions of dollars in customer service can assist DHS greatly in those efforts. Deputy Secretary Mayorkas ended his comments by saying DHS will see tremendous benefits by expanding the public-private partnership. He indicated that he will be visiting the Miami Airport, an airport that suffers significant challenges, to see how DHS can partner with the private sector to improve the experience at the airport. Quality of experience is a driver of travel within the United States. The greater the amount of travel the economic benefits are monumental.

Deputy Secretary Mayorkas spoke about the need for legislative changes, allowing DHS to have the authority to accept private funds in a public-private partnership in airports in five different locations. This was previously done last year and DHS is entitled to do that again this year. An expansion of the public-private partnership would be very beneficial in those efforts.

The Deputy Secretary also stated that CEO's had expressed interest in the Department's Loan Executive Program but to date he has been disappointed in the level of participation and number of submissions.

Ambassador Jones asked what the status was on border crossing, particularly pertaining to Mexico. He wanted to know what the relationship is between Mexico and DHS in dealing with border crossings as previously the Mexican government wanted to improve the border crossings, but we were not in sync with them and the other way around.

Deputy Secretary Mayorkas replied that DHS has a tremendous pool of resources in the movement of people and goods across the southwest border. DHS has committed, as a government and as an administration, a considerable amount of funds to improve the Laredo Port, a critical port of entry, and others. DHS has a wonderful relationship with Mexico and is following that relationship with the resources that it needs. DHS has allocated 2,000 new Customs and Border Protection Officers that DHS has received funding for, and also worked to increase physical capacity of those ports of entry as well. Laredo is going to expand exponentially because DHS can only do so much with the current number of lanes.

Ms. Lemack expressed that it was encouraging to hear the Deputy Secretary mention reaching out to the private sector to discuss service; however, mentioned a lot of times the discussion is about security instead. She wanted to know if DHS was reaching out to the private sector technology companies to have their executives come in to assist with travel security. She also wanted to know if the Deputy Secretary could comment on the concerns of preclearance in the United Arab Emirates (UAE) and other locations.

Deputy Secretary Mayorkas replied that DHS has brought in increasing technology to the travel effort. DHS has the automated passport controls that have brought great advances in many airports. Dallas-Fort Worth and Chicago O'Hare airports have seen over a 40 percent drop in

wait times using preclearance and the automated passport controls. DHS is working on mobile technology, and is bringing in technology experts to see what the possibilities are on that type of facilitation of travel. Deputy Secretary Mayorkas asked Deputy Administrator of TSA, John Halinski, to speak about airport security and the private sector.

Deputy Administrator Halinski mentioned the threat that TSA faces is from commercial entities. To fight this threat, TSA has worked with DHS Intelligence and Analysis (I&A), Customs and Border Protection (CBP), as well as the Office of the Director of National Intelligence, to create a domain awareness intelligence group. Right now this group is in the starting stage, but will incorporate the private sector with DHS entities. The Air Domain Intelligence-Integration and Analysis Center pilot program is at our Annapolis Junction facility. This facility will bring in private sector and DHS entities together to tackle challenges, operating in both an open source and classified levels. All members of the team will be cleared and have access to classified information to get a better understanding of the threats.

Deputy Secretary Mayorkas addressed Ms. Lemack's second question regarding preclearance. He said that preclearance was perceived as advantaging one airline over the others commercially. DHS selected a site for preclearance based on the security imperative, as well as the willingness and readiness of the site to be able to deliver preclearance. DHS will push for preclearance to be where it is most important from a security prospective, not motivated by advantaging one commercial entity over another.

Congresswoman Holtzman had a question about the issue of trade, and wanted to know what the process is of screening cargo at ports.

Deputy Secretary Mayorkas replied that DHS has applied risk-based screening protocols to not only people, but also cargo. DHS has developed advanced technology such as the ability to screen cargo with a more advanced x-ray technology on the southwest border and at the Peace Bridge on the northeast border. Deputy Secretary Mayorkas asked the Deputy Commissioner of CBP, Kevin McAleenan, to address the question as well.

Deputy Commissioner McAleenan mentioned five areas why CBP thinks their risk-based approach, and layered security approach in partnership with the Coast Guard and foreign authorities, works.

1.) Dealing with data, CBP now collects advanced data on all cargo that will arrive in the U.S. before it is ever placed on a vehicle at a foreign seaport. Additionally, other information is collected about the import, including how it will be stowed on a vehicle.
2.) CBP is collecting data through sophisticated, automated, targeting tools. These tools are driven by intelligence and are available to analysts from multiple agencies for identifying shipments that might present a risk before being shipped.

3.) CBP inspects cargo at the earliest point possible in the supply chain. Through CBP's Container Security Initiative, they have personnel in 58 seaports abroad and partnerships with foreign customs authorities to examine cargo that is believed to have high risk prior to it being put on a vessel. Of those shipments, CBP uses advanced data to focus on the 85% of the shipments that CBP thinks may present a potential risk. The remaining 15% are checked as soon as they hit docks.
4.) For the highest consequence threats of rad nuke, CBP screens 99.8 percent of all containerized cargo through radiation portal monitors. This is a sophisticated and sensitive technology that assists to identify radiological and nuclear materials.
5.) Through the Customs-Trade Partnership Against Terrorism, which has 10,750 members, CBP has great insight into the global supply chain. Efforts are being made to expand this program's network by including other countries that possess trusted trader programs that have confirmed security standards. Fifty percent of all maritime cargo is shipped or is going through a supply chain which CBP has verified and vetted in concert with the companies that are moving the goods. CBP is working on expanding the network by recognizing other countries' trusted trader programs upon verification. This enables CBP to have a broader network. It is called mutual recognition in terms of the security of the supply chain.

Deputy Secretary Mayorkas added that on a visit to both the northern border and southern border, he noticed extraordinary strides that have been made in technological advancement. Yet, some of the processes are still very primitive and time consuming. For example, at the port of entry at Laredo where there is a lot of traffic, produce is coming in on wooden pallets that have to be inspected to make sure they are not infected by wood burrowing insects; this is a manual process that is time consuming. This is an area that will need a great deal of attention.

Mr. Augustine wanted to know if everyone who has a top secret clearance or a secret clearance could be put into pre-check. Given the amount of illegal marijuana crossing onto the border daily, he also inquired as to what is being done to monitor how much nuclear material is coming in at various checkpoints.

Deputy Administrator Halinski replied that TSA is striving to get all populations into pre-check. TSA has the vast majority of people with top secret clearance enrolled in pre-check and have been able to enroll Department of Defense personnel in pre-check. The issue CBP has found dealing with top secret SCI clearance is that some agencies do not want to identify people who have clearances. TSA is currently working with other areas of civilians in the government.

Deputy Secretary Mayorkas asked Deputy Commissioner McAleenan to answer the second part of Mr. Augustine's question on nuclear capabilities between ports of entry.

Deputy Commissioner McAleenan stated that CBP cannot be overly focused on one vector and CBP must deter people trying to use the legal flows to bring in radiological nuclear material.

Between the ports of entry and the Department, there has been increased effectiveness each year over the past five years between ports. Due to the increase in resources for the Border Patrol, a strong deterrent for attempting to bring nuclear weapons has been the new technological approaches to identify people crossing, both fixed and mobile. This is a continuing effort, and CBP needs to keep getting better.

Judge Webster provided members of the public with the contact information for the HSAC so they could provide comments if they wanted.

Written public comments after the meeting must be identified by Docket No. DHS-2014-0002 and may be submitted by one of the following methods:

Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.

- Email: *HSAC@hq.dhs.gov*. Include docket number in the subject line of the message.
- Fax: (202) 282-9207.
- Mail: Homeland Security Advisory Council, Department of Homeland Security, Mailstop 0445, 245 Murray Lane SW., Washington, DC 20528.

He then invited the members of the public to leave the room and thanked them for their interest and attendance. The open session adjourned and the meeting moved to a closed session.

Homeland Security Advisory Council (HSAC) Meeting - Closed Session
U.S Coast Guard Headquarters
Washington, D.C. 20528

EXECUTIVE SUMMARY

4:15 to 5:30 p.m.
Thursday, June 5, 2014

HSAC Chair, Judge William Webster brought the closed session to order.

General Frank Taylor, Under Secretary for the Office of Intelligence and Analysis provided the members with a domestic intelligence briefing focused on threats against the homeland.

Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity for the National Protection and Programs Directorate and YuLin Bingle, Director of Cyber Intelligence for the Office of Intelligence and Analysis provided the members with a domestic intelligence briefing focused on cyber threats against the homeland.

John Halinski, Deputy Administrator for the Transportation Security Administration provided members with a sensitive briefing on their risk-based security program.

Megan Mack, Officer for Civil Rights and Civil Liberties provided a strategic overview on the Department's implementation plan to counter domestic violent extremism. These efforts focus on roundtable discussions and educating community and local law enforcement leaders on topics including various cultural and religious practices.

Due to the lack of time members were not provide an operational update on immigration enforcement.

Judge Webster adjourned the meeting.