

U.S. Department of Homeland Security

Homeland Security Advisory Council

June 2, 2016 Public Meeting

Executive Summary

The meeting of the Homeland Security Advisory Council (HSAC) was convened from 1:50 p.m. to 3:37 p.m. in the Woodrow Wilson International Center for Scholars, Washington, D.C. The meeting was open to members of the public under the provisions of the Federal Advisory Committee Act (FACA), P.L. 92-463 and 5 U.S.C. § 552b.

The following individuals were in attendance:

HSAC Members

William Webster, <i>Chair</i>	Carie Lemack
Stephen Adegbite	Wilson "Bill" Livingood
John R. Allen	John Magaw
Norman Augustine	Christian Marrone
Ron Barber	David A. Martin
John Chaussee (proxy for Gary Kelly)	Michael Masters (proxy for Ali Soufan)
Marshall Fitz	Ned Norris, Jr.
Paul Goldenberg	Farah Pandith
Elizabeth "Liz" Holtzman	John Pistole
Jim Jones	Robert Rose
Juliette Kayyem	Paul Stockton
John Kelly	Karen Tandy
	James Waters (proxy for William Bratton)

Also Present

Jeh C. Johnson, Secretary, DHS
Sarah Morgenthau, Executive Director, Homeland Security Advisory Council, DHS
Chris Boyer, Assistant Vice President of Global Public Policy, AT&T
Scott DePasquale, Chairman & CEO, Utilidata; Chairman, Rhode Island Cybersecurity Commission
Russ Fitzgibbons, Executive Vice President & Chief Risk Officer, The Clearing House
Adnan Kifayat, German Marshall Fund
Agnes Kirk, Chief Security Officer, Washington State Department of Information Services
Joanna Nunan, Military Advisory to the Secretary, DHS
George Selim, Director, Office for Community Partnerships, DHS
Suzanne Spaulding, Under Secretary, National Protection and Programs Directorate, DHS

Welcome by HSAC Leadership and Swearing In of New Members

William Webster, Chair of the Homeland Security Advisory Council, called the open session of the meeting to order at 1:50 p.m. Chair Webster welcomed Homeland Security Advisory Council (HSAC) members, attendees from the public and press, and Secretary Jeh Johnson.

Secretary of Homeland Security Jeh Johnson administered the oath of office to the new HSAC members, Karen Tandy and General John Kelly. Additionally, Secretary Johnson thanked General Kelly for his service by presenting him with the Homeland Security Distinguished Service Medal.

Remarks by Secretary Jeh Johnson

Secretary Johnson reviewed his top priorities for his remaining time in office. His overall priority is to reform management at the Department of Homeland Security (DHS) through continued implementation of the Unity of Effort initiative. The House of Representatives has codified many of the initiative's elements through legislation and the Senate is currently marking up a bill that looks to do the same. Secretary Johnson also wants to close any FY17 budgetary challenges and to increase levels of DHS employee satisfaction. The Secretary and Deputy Secretary have obtained employee feedback through the Federal Employee Viewpoint Survey and by conducting workforce engagement meetings with DHS staff throughout the country. Feedback from over 3,000 employees was used to develop DHS's new mission statement.

Other priorities include effectively managing aviation security and increased wait times at airports, preventing illegal migration at the U.S.'s southwest border, improving and implementing cybersecurity measures, building up Secret Service staff levels, vetting and accepting 10,000 Syrian refugees by the end of FY16, and continuing efforts to counter violent extremism.

The Secretary has submitted two budget reprogramming requests to Congress in order to help implement measures that will work to reduce airport wait times without compromising aviation security, such as converting more TSOs from part-time to full-time. The Secretary has also participated in several press events throughout Central and South America to promote safe and legal ways to migrate to the U.S. Although the amount of illegal migrants apprehended at the southwest border has been higher in 2016 than it was in 2015, it is still much lower than the number apprehended at this point in 2014. DHS has added security checks to the vetting process for resettling Syrian refugees in the U.S. Although DHS appears to be falling behind its pace of resettling Syrian refugees in the U.S., this is only in terms of physical resettlement; many more refugees have already been approved and pre-approved for resettlement, pending security checks. Additional screening resources have been added in Turkey and Jordan to aid in meeting the U.S.'s resettlement goal. Secretary Johnson asked that, at their next meeting, the HSAC discuss what agenda items should be considered during DHS's transition to a new presidential administration.

Cybersecurity Subcommittee Report

The Subcommittee had been asked to improve the National Cyber Incident Response Plan (NCIRP) by identifying the readiness of lifeline infrastructure sectors to meet emerging threats

and by recommending ways in which to build cross-sector capabilities to accelerate the restoration of critical services in the event of a cyber-attack. In their report, the Subcommittee found that individual lifeline infrastructure sectors are strong and continually improving in meeting direct threats against their own sector. However, effort needs to be made both in the NCIRP and by industries to build stronger cross-sector resilience. Cybersecurity incidents will need different approaches within the all-hazards preparedness common framework because of factors such as their potentially unlimited geographic scope, the possibility of repeated attacks due to the existence of malware, and because they can create a contested environment in which it could be difficult for the government to communicate with the public. The NCIRP also needs to better define the role of local and state governments during cybersecurity incidents.

Chris Boyer, Assistant Vice President of Global Public Policy at AT&T Services, presented three major points from the communication sector's recommendations to DHS. Firstly, the communications industry needs a finalized NCIRP that specifies how private industry should interact with the government in the event of a cybersecurity incident. Secondly, the communications sector recommends that DHS adopt the scale from the National Security Telecommunications Advisory Committee's (NSTAC) ICT mobilization report that ranks different cybersecurity threats and then develop triggers for different levels of threat. Finally, there is general agreement within the sector on the need for a better cross-sector emergency response capability.

Russ Fitzgibbons, Executive Vice President and Chief Risk Officer for The Clearing House, presented recommendations made by the financial sector. The financial sector believes that the final plan should clarify involved entities' roles and be flexible enough to respond to the diversity of ways a cybersecurity threat can manifest itself. The sector recommends that the crisis management and escalation process be formalized and include the ability for communication across sectors. Finally, the financial sector also recommends the creation of, and DHS participation in, a stakeholder group to better understand and plan for the cross-sector systemic impact of cybersecurity incidents.

Although Tom Fanning, Chair of the Electricity Subsector Coordinating Council (ESCC), was unable to present at this meeting, the electric sector's report is included in the Subcommittee's report. In its report, the ESCC found that they are well-positioned to organize for cyber response and serve as a partner for other subsectors within the electric sector. The Council recommends improving cross-sector response capability through the creation of a strategic infrastructure executive council.

The Subcommittee had also been asked to explore how DHS can provide a more unified approach to support state, local, tribal, and territorial (SLTT) cybersecurity. They found that the gap between the cybersecurity threat and SLTT progress in addressing it is too big, and hypothesized several possible explanations for this gap. One explanation is the existence of the so-called cyber conundrum, in which there is no consensus mechanism on protecting information received from DHS about a cybersecurity incident affecting private networks and what they can share with the SLTT community. The Subcommittee believes that rather than solving this conundrum at this point in time, the SLTT community can assume that there is a constant cybersecurity threat on networks. Another explanation for the gap is that there is still a divide between traditional and cyber public safety in which programs and procedures addressing

traditional threats are much more established and accepted than those addressing cybersecurity threats. In order to fix the gap, the Subcommittee has three recommendations for DHS and three for the SLTT community. The Subcommittee recommends that DHS simplify and eliminate redundancies in the programs surrounding cybersecurity, be more aggressive in assessments and guidance to the SLTT community, and help states implement a unified state model. For the SLTT community, the Subcommittee recommends that members put a governance system in place, ensure that their own networks are strong and in order before focusing on other cybersecurity concerns, and focus on the critical needs of their particular jurisdictions.

Member Rose added that there is still confusion in the SLTT community about who to call in the event of a cybersecurity incident. He also commented that HSAC members have discussed setting up a classified information exchange based on critical infrastructure areas and suggested that such a system could be used to help address the cyber conundrum. Agnes Kirk, Chief Security Officer at the Washington State Department of Information, stressed that both DHS and the SLTT community have been working on improving cybersecurity capabilities but they need to continue to work together in order to make progress. Scott DePasquale, Chairman of Utilidata and the Rhode Island Cybersecurity Commission, hypothesized that efforts made by DHS to improve methods of responding to cybersecurity incidents will be ineffective until SLTT governments invest in the structures that can integrate this information into the rest of their homeland security systems. He added that DHS has the ability to use grants to incentivize states to build these needed structures.

Secretary Johnson said SLTT community members should call DHS's National Cybersecurity and Communications Integration Center (NCCIC) in the event of a cybersecurity incident. Suzanne Spaulding, Under Secretary for the National Protection and Programs Directorate, thanked the private and public sectors for working together to help improve the U.S.'s overall capability to respond to cybersecurity incidents and thanked the Subcommittee for emphasizing how to mitigate consequences in their report. She noted that DHS is working to simplify and streamline their message, activities, structure, and web presence, and is also working to solve the cyber conundrum's information sharing issue.

Countering Violent Extremism (CVE) Subcommittee Report

This report is situated in the context of the current global climate and has leveraged a diverse range of outside expertise. The premise of this report stems from the belief that the threat posed by violent extremists is serious and is growing and evolving quickly. The Subcommittee holds the opinion that the U.S. can build a better system to address and defeat the extremists' ideological appeal and hopes that this report will help provide the architecture for such a system.

The recommendations in this report center around five basic themes. The themes are as follows: a critical need for someone credible to take charge and build on the leadership already demonstrated by DHS, a focus on the millennial generation, a national focus that includes state and local governance, learning from small and nascent CVE activities and developing those that are effective, and partnering with all sectors of U.S. society.

This report contains nine recommendations and 61 specific actions, which can be classified as either internal or external in nature. Internal recommendations include those that work to

strengthen and obtain more resources for the Office for Community Partnerships, improve and professionalize the way data is analyzed and utilized, clarify language and lexicon around CVE, and build stronger partnerships between DHS and other agencies. External recommendations include those that work to connect funding to effective programs, connect technology to content and distribution, connect expertise to civil society, and connect credible messengers to target audiences. The Subcommittee has been careful not to recommend actions that will require individuals to overstep their authorities. George Selim, Director of the Office for Community Partnerships (OCP), commented that this report has been and will continue to be useful in helping the OCP navigate the complex issues it has encountered during its period of establishment. He views these recommendations as validation for what has already been done and a mandate for what still needs to be done.

Secretary Johnson asked two questions in response to this report. His first was how success in CVE can best be measured. Member Pandith responded that two metrics should be used, the first of which is the amount and effectiveness of experimentation in CVE. DHS should encourage communities throughout the U.S. to develop programs and initiatives to combat violent extremism at the local level because having a diversity of options will help DHS better understand what does and doesn't work. The second metric should be the measurement of how children are accessing information about terrorist organizations and their community's subsequent response. Secretary Johnson's second question was to ask if the U.S. government should be involved in the trusted flagger business and whether this should be part of the CVE mission. Member Pandith answered that the government, rather than become a trusted flagger, should allow trusted networks from localized entities to be the networks that interact with at-risk communities.

Public Comment

There were no public comments.

Council Deliberation and Voting on Reports

The HSAC first deliberated the Cybersecurity Subcommittee's report and recommendations. Member Holtzman asked if federal agencies and the President have sufficient powers under existing statutes to properly respond to the consequences of a cyber-attack. The Subcommittee members responded that they did not address this issue directly in their report but have cited it for future analysis. Member Norris thanked the Subcommittee members for including tribal and territorial governments in their discussion about cybersecurity at the SLTT level. A motion to accept the Cybersecurity Subcommittee's recommendations was made, seconded, and passed unanimously.

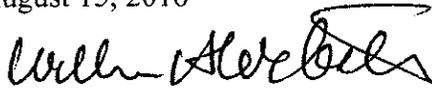
There were no questions regarding the Countering Violent Extremism Subcommittee's report and recommendations. A motion to accept the Countering Violent Extremism Subcommittee's recommendations was made, seconded, and passed.

Public Session Concludes

Members of the public can submit additional questions to the HSAC in writing or by email. Chair Webster thanked everyone for their participation and adjourned the meeting at 3:37 p.m.

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

August 15, 2016

A handwritten signature in black ink, appearing to read "William H. Webster". The signature is written in a cursive style with a prominent loop at the end.

Signed and Dated *aug. 15 2016*

Judge William H. Webster, Chairman, Homeland Security Advisory Council