

DEPARTMENT OF HOMELAND SECURITY
APPROPRIATIONS FOR 2020

HEARINGS
BEFORE A
SUBCOMMITTEE OF THE
COMMITTEE ON APPROPRIATIONS
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTEENTH CONGRESS
FIRST SESSION

SUBCOMMITTEE ON HOMELAND SECURITY

LUCILLE ROYBAL-ALLARD, California, Chairwoman

HENRY CUELLAR, Texas
C. A. DUTCH RUPPERSBERGER, Maryland
DAVID E. PRICE, North Carolina
DEBBIE WASSERMAN SCHULTZ, Florida
GRACE MENG, New York
PETE AGUILAR, California

CHUCK FLEISCHMANN, Tennessee
STEVEN M. PALAZZO, Mississippi
DAN NEWHOUSE, Washington
JOHN H. RUTHERFORD, Florida

NOTE: Under committee rules, Mrs. Lowey, as chairwoman of the full committee, and Ms. Granger, as ranking minority member of the full committee, are authorized to sit as members of all subcommittees.

DAREK NEWBY, MICHAEL S. HERMAN, ROBERT JOACHIM,
KRIS MALLARD, KARYN RICHMAN, and ELIZABETH LAPHAM
Subcommittee Staff

PART 2

DEPARTMENT OF HOMELAND SECURITY

	Page
Department of Homeland Security—Office of Inspector General	1
Federal Emergency Management Agency	67
Securing Federal Networks and State Election Systems	123
United States Coast Guard	167
Transportation Security Administration	199



Printed for the use of the Committee on Appropriations

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON APPROPRIATIONS

NITA M. LOWEY, New York, *Chairwoman*

MARCY KAPTUR, Ohio	KAY GRANGER, Texas
PETER J. VISCLOSKEY, Indiana	HAROLD ROGERS, Kentucky
JOSE E. SERRANO, New York	ROBERT B. ADERHOLT, Alabama
ROSA L. DELAURO, Connecticut	MICHAEL K. SIMPSON, Idaho
DAVID E. PRICE, North Carolina	JOHN R. CARTER, Texas
LUCILLE ROYBAL-ALLARD, California	KEN CALVERT, California
SANFORD D. BISHOP, Jr., Georgia	TOM COLE, Oklahoma
BARBARA LEE, California	MARIO DIAZ-BALART, Florida
BETTY McCOLLUM, Minnesota	TOM GRAVES, Georgia
TIM RYAN, Ohio	STEVE WOMACK, Arkansas
C. A. DUTCH RUPPERSBERGER, Maryland	JEFF FORTENBERRY, Nebraska
DEBBIE WASSERMAN SCHULTZ, Florida	CHUCK FLEISCHMANN, Tennessee
HENRY CUELLAR, Texas	JAIME HERRERA BEUTLER, Washington
CHELLIE PINGREE, Maine	DAVID P. JOYCE, Ohio
MIKE QUIGLEY, Illinois	ANDY HARRIS, Maryland
DEREK KILMER, Washington	MARTHA ROBY, Alabama
MATT CARTWRIGHT, Pennsylvania	MARK E. AMODEI, Nevada
GRACE MENG, New York	CHRIS STEWART, Utah
MARK POCAN, Wisconsin	STEVEN M. PALAZZO, Mississippi
KATHERINE M. CLARK, Massachusetts	DAN NEWHOUSE, Washington
PETE AGUILAR, California	JOHN R. MOOLENAAR, Michigan
LOIS FRANKEL, Florida	JOHN H. RUTHERFORD, Florida
CHERI BUSTOS, Illinois	WILL HURD, Texas
BONNIE WATSON COLEMAN, New Jersey	
BRENDA L. LAWRENCE, Michigan	
NORMA J. TORRES, California	
CHARLIE CRIST, Florida	
ANN KIRKPATRICK, Arizona	
ED CASE, Hawaii	

SHALANDA YOUNG, *Clerk and Staff Director*

**DEPARTMENT OF HOMELAND SECURITY
APPROPRIATIONS FOR 2020**

WEDNESDAY, MARCH 6, 2019.

**OVERSIGHT HEARING—DHS OFFICE OF INSPECTOR
GENERAL**

WITNESS

**JOHN V. KELLY, SENIOR OFFICIAL PERFORMING THE DUTIES OF
INSPECTOR GENERAL, OFFICE OF INSPECTOR GENERAL**

Ms. ROYBAL-ALLARD. The subcommittee will come to order. I welcome everyone to the first Department of Homeland Security Subcommittee hearing of the 116th Congress and my first hearing as chair.

I would also like to welcome and acknowledge two new members of the hearing, Debbie Wasserman Schultz and Grace Meng on the Democratic side, and I have been—and Mr. Rutherford also is a new to the committee and Mr. Aguilar.

I have been a member of this subcommittee since it was established in 108th Congress, following the horror and the tragedies of 9/11. I served as ranking member in the 114th and the 115th Congress. My first experience as chair of the subcommittee was finishing the fiscal year 2019 DHS spending bill. Based on that experience, I can attest to the fact that the role of chair is never easy and much more than merely funding the various DHS agencies.

Members of the subcommittee do not always agree. In fact, at times, we strongly disagree on funding and policy matters. My experience, however, is that those disagreements are founded on the belief of what is in the best interest of our country. Our subcommittee has always had a strong tradition of collegiality, professionalism and bipartisan support for the Department's many important missions.

As our members work together to protect our homeland, it is my intent that my tenure as chair will continue that tradition of commitment to bipartisanship, fairness and public service. I can think of no better partner to join me in that effort and the distinguished gentleman from Tennessee, Ranking Member Fleischmann, also a longtime member of this subcommittee. I would now like to turn it over to Ranking Member Fleischmann for his opening remarks.

Mr. FLEISCHMANN. Thank you, Madam Chairman, and I wish to congratulate you on your ascension to this position. It's not only well-deserve but we all look forward to working with you.

And to my colleagues on both sides of the dais, this subcommittee is a subcommittee I have actually been on since I have

been with—been an appropriator. So it's a privilege and we look forward to working together.

I would also like to join in welcoming our Acting Inspector General Kelly to the subcommittee today. Thank you, sir, for being here. We look forward to hearing from your testimony.

And Madam Chairman, I want to thank you for your work in the efforts of all your staff—we have already started work very well with staff on both sides of the aisle, and I appreciate that—to keep on the details and oversight of this massive Department across the billions of dollars, the multitude of programs and the thousands of agents, officers, mariners and all the employees to help protect our Nation and keep our people safe without waste, fraud or abuse.

Thank you, Mr. Kelly; I look forward to hearing your testimony.

And Madam Chairman, I yield back.

Ms. ROYBAL-ALLARD. Thank you.

I would like to go over some housekeeping matters. The order in which members will be called for questioning will be based on the seniority of those who were present when the hearing was called to order, alternating between majority and minority members. Also, to ensure that everyone has ample opportunity to ask questions, I would ask each member to keep their turn to the allotted 5 minutes per round.

Mr. Kelly, thank you for joining us this morning. There are many critical areas for oversight of the Department of Homeland Security. Therefore, it is fitting to formally begin our hearings with the Office of the Inspector General, which is perhaps in the best position to inform us how the Department of Homeland Security is doing. Mr. Kelly, we look forward to your testimony, we will submit the full text of your official statement for the record. Please begin.

Mr. KELLY. Madam Chairwoman, ranking member and members of the subcommittee, thank you for inviting me today.

My testimony will focus on four areas: family separations, unannounced inspections at ICE detention facilities, Departmental efforts to hire and train border patrol agents and immigration officers, and finally oversight of FEMA disaster assistance work.

Concerning family separations, in May 2018, DHS in concert with DOJ established a zero-tolerance policy for adult aliens illegally arriving in the United States minor children. In response to that action, I deployed a team in June to conduct unannounced visits at CBP and ICE facilities.

As a result of those visits, we had six observations. First, DHS was not fully prepared to implement the zero-tolerance policy. Second, the lack of fully integrated immigration information technology systems made it difficult for DHS to track separated parents and children.

Third, DHS urged asylum-seekers to come to ports of entry for processing, but, at the same time, CBP regulated the number of asylum-seekers entering the ports. This likely resulted in additional illegal border crossings. Fourth, CBP detain children for extended periods and in facilities for short-term detention. Fifth, the lack of reliable data poses an obstacle to accurate reporting on family separations. Sixth, DHS dissemination of inconsistent or inaccurate information resulted in confusion among detained parents about the separation and reunification process.

We also had four observations of the CBP facilities we visited; our observations cannot be generalized to other times or locations. First, the facilities we looked at, they generally appear to be in compliance with the detention facility standards. Second, the children had access to hygiene items and clean bedding.

Third, we did not encounter issues with temperature, ventilation, access to emergency medical care, supervision, or access to phones. Fourth, for all the CBP facilities we visited children had access to food and snacks and did not complain of hunger.

As for ICE inspections, we have conducted unannounced inspections at ice detention facilities since 2016. In 2017, we inspected five detention facilities and have significant concerns about the treatment and care at four of those facilities, where we observed potentially unsafe and unhealthy conditions.

In 2018, we issued two reports. Our inspection of ICE's Essex County center we observed extreme mishandling of meats, including spoiled meat. This can spread salmonella, listeria and E. coli.

This resulted in detainees filing grievances. One detainee wrote, for dinner, we were served meat balls that smell like fecal matter. Another detainee wrote, the food we received has been complete garbage, it's becoming impossible to eat. It gets worse every day. It literally looks like it came from the garbage dumpster. ICE agreed with our recommendations and are working on resolving those findings.

For ICE's Adelanto center, we issued a Management Alert because we observed braided bed-sheets, referred to as nooses, hanging from 15 cells we visited. This is a real threat. In March of 2017, a detainee died after being found hanging from his bed sheet in a cell at this facility. Again, ICE agreed with our recommendations and are addressing our findings.

Concerning the hiring and training of law enforcement officials, CBP and ICE continue to face significant challenges. In November 2017, CBP awarded Accenture a contract totaling nearly \$300 million to recruit and hire 7,500 agents and officers. We determined the Accenture contract did not provide the promised hiring results, yet CBP Accenture—paid Accenture over \$13 million for start up costs, recruiting expenses and other expenses. In return, Accenture processed two job-accepted individuals.

If CBP achieved its hiring goals, our recent audit determined that the Federal Law Enforcement Training Centers did not have the capacity to train all the law enforcement officers CBP and ICE intended to hire. This is because FLETC does not have the facilities or the funding to satisfy the increase in training required by the hiring goals.

As for FEMA oversight, Hurricanes Harvey, Irma and Maria made landfall in a four-week period during August and September 2017. These storms rank as three of the five most expensive storms in U.S. history. One of the chief challenges FEMA faces in post-disaster environment is a vulnerability of fraud and abuse. Thus, OIG's criminal investigators play very active role during the post-disaster period. Currently, investigations related to FEMA represent about 30 percent of our open investigative caseload.

For almost a decade we have been issuing annual FEMA capping audit reports. Those reports consolidate FEMA audit related find-

ings and recommendations. We designed them to inform FEMA about significant and systemic issues of non-compliance and program deficiencies. These reports show that FEMA does not manage disaster relief grants and funds adequately, hold states accountable for properly managing disaster relief funds, or provide adequate monitoring and technical assistance to sub-grantees.

Madam Chairwoman, this concludes my testimony. I will be pleased to answer questions from you or the members of the committee.

[The prepared statement of Mr. Kelly follows:]

OFFICE OF INSPECTOR GENERAL

**Testimony of Acting Inspector
General John V. Kelly**

**Before the Committee on
Appropriations, Subcommittee on
Homeland Security**

U.S. House of Representatives

"DHS Office of Inspector General"



**Homeland
Security**

**March 6, 2019
9:30 AM**



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Chairwoman Roybal-Allard, Ranking Member Fleischmann, and members of the Subcommittee, thank you for inviting me today to discuss the work of the Department of Homeland Security (DHS) Office of Inspector General (OIG). I am pleased to have the opportunity to share our office's recent oversight efforts into some of the Department's most high profile areas of work.

It is the OIG's mission to provide independent, objective oversight and promote excellence, integrity, and accountability within DHS. Through our work, we help the Department address challenges and fulfill its vital mission of protecting and securing our Nation. The work of the OIG is done by about 790 dedicated federal employees located both in Washington, D.C. and in 32 field offices across the United States.

One of OIG leadership's most persistent challenges is determining how best to leverage our relatively small staff to provide comprehensive oversight of the third-largest Cabinet department with over 240,000 federal employees and the most diverse mission set in the Federal government. We have recently created a new process internally to address this challenge, whereby leadership across all functions of our agency meet in a weekly discussion to set priorities regarding the DHS programs we will audit, inspect, review, and investigate. Through this approach, we are able to take into account our legislatively mandated reviews, congressional requests, referrals from other oversight agencies, and discretionary job proposals to create a balanced and comprehensive oversight portfolio. Our ultimate goal is to be a nimble organization poised to quickly respond to DHS' highest risk challenges with impactful oversight that provides value to the Department, the Congress, and the American taxpayer.

In fiscal year (FY) 2018 alone we released 89 audits, inspections, and other reviews containing 318 recommendations. During the same time period, the work of our office's criminal investigators resulted in 103 arrests, 132 indictments, 76 convictions and 31 personnel actions. Complaints from DHS employees and the public to our hotline continue to grow, with 40,657 complaints received in FY 2018 and 7,331 received to date in FY 2019. DHS OIG's return on investment averages \$9.47 over the last 5 years, meaning that for every \$1 invested in the OIG, we have identified \$9.47 in potential savings.

My testimony today will focus on our recent work in the areas of: (1) family separation, (2) unannounced inspections of U.S. Immigration and Customs Enforcement (ICE) facilities, (3) the Department's efforts to hire and train border patrol agents and immigration officers, and (4) oversight of the Federal Emergency Management Agency (FEMA) disaster relief work.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Initial Observations Regarding Family Separation Issues Under the Zero Tolerance Policy

Last year, the Administration's Zero Tolerance Policy and the resulting family separations sparked intense public debate. In early May 2018, DHS determined that the Zero Tolerance Policy would cover alien adult arriving illegally in the United States with minor children, a change to its approach to immigration enforcement. Because the minor children cannot be held in criminal custody with an adult, alien adults who entered the United States illegally would have to be separated from any accompanying minor children when the adults were referred for criminal prosecution. The children, who DHS then deemed to be unaccompanied alien children (UAC) were held in DHS custody until they could be transferred to the U.S. Department of Health and Human Services (HHS) Office of Refugee Resettlement (ORR).

In response to significant congressional and public interest, DHS OIG deployed a multi-disciplinary team comprised of attorneys, inspectors, and criminal investigators to areas in and around El Paso and McAllen, Texas to conduct unannounced visits at Customs and Border Protection (CBP) and ICE facilities between June 26 and June 28, 2018. While our work did not evaluate the merits of the Zero Tolerance Policy, family separations or the Department's efforts to reunify separated families, we did report on our observations made in the field¹, including:

- DHS was not fully prepared to implement the Zero Tolerance Policy or to deal with certain effects of the policy following implementation.
- A lack of fully integrated Federal immigration information technology system made it difficult for DHS to reliably track separated parents and children.
- CBP regulated the number of asylum-seekers entering at the ports of entry, which may have resulted in additional illegal border crossings.
- CBP detained UACs for extended periods in facilities intended for short-term detention.
- Lack of access to reliable data poses an obstacle to accurate reporting on family separations.

¹ *Special Review – Initial Observations Regarding Family Separation Issues Under the Zero Tolerance Policy (OIG-18-84)*.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- Dissemination of inconsistent or inaccurate information resulted in confusion among alien parents about separation and reunification process.

Our observations indicate that DHS was not fully prepared to implement the Zero Tolerance Policy, or to deal with certain effects of the policy following implementation. For instance, while the Government encouraged all asylum-seekers to come to ports of entry to make their asylum claims, CBP managed the flow of people who could enter at those ports of entry through metering, which may have led to additional illegal border crossings. Additionally, CBP held alien children separated under the policy for long periods in facilities intended solely for short-term detention.² The OIG team also observed that a lack of a fully integrated Federal immigration information technology system made it difficult for DHS to reliably track separated parents and children, raising questions about the Government's ability to accurately report on separations and subsequent reunifications. Finally, inconsistencies in the information provided to alien parents resulted in some parents not understanding that their children would be separated from them, and made communicating with their children after separation difficult.

Next Steps

As we noted in our *Initial Observations* report, while Executive Order 13841 halted the practice of family separation, OIG multi-disciplinary family separation teams continue to work on the issues we identified during our initial observations.

We initiated a full-scale audit in October looking at the effectiveness of DHS' IT systems for tracking and supporting efforts to reunify unaccompanied alien children with separated families. Our audit will determine whether the IT systems and processes DHS relied upon were adequate to carry out specific border security operations, including tracking separated families, prior to and following the implementation of the Zero Tolerance Policy. We are also looking at whether DHS effectively tracked family reunification efforts following the federal judge's court order in late June 2018. Using our data analytics capabilities, we will assess data reliability and the accuracy of DHS's reported numbers for separated parents and children. We are currently in the fieldwork phase.

² Notwithstanding this observation, OIG observed that the DHS facilities it visited appeared to be operating in substantial compliance with applicable standards for holding children. The detailed results of OIG's unannounced inspections of these facilities are described in a separate OIG report titled *Results of Unannounced Inspections of Conditions for Unaccompanied Alien Children in CBP Custody (OIG-18-87)*, discussed later in this testimony.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

We have also opened a review into CBP's Processing of Asylum Seekers at Ports of Entry. The objective of this work is to determine whether CBP Office of Field Operations is turning away those who present themselves for asylum at ports of entry and separating family units that seek asylum and documenting separations appropriately. As part of its ongoing fieldwork, the team travelled to ports of entry in Texas, Arizona, and California, where it observed operations, gathered documents, and interviewed CBP officers, representatives of non-governmental organizations, and asylum seekers.

Finally, we will take a closer look at the removal of separated alien families. Our work will determine whether ICE removed any parents without first offering them the opportunity to bring their separated children with them. The review will identify why this may have happened and how many separated parents may have been removed without having that option.

Results of Unannounced Inspections of Conditions for Unaccompanied Alien Children in CBP Custody

As part of our initial observation work regarding the Zero Tolerance Policy and family separations, we reported on the conditions we observed in the Texas CBP facilities we visited on June 26-28, 2018.³ We visited nine CBP facilities in McAllen and El Paso, Texas, including five Border Patrol stations and four CBP Office of Field Operations (OFO) ports of entry.

As you are aware, CBP facilities must provide safe and sanitary holding facilities as detailed in CBP's 2015 *National Standards on Transport, Escort, Detention and Search* (TEDS Standards). Generally, CBP must transfer UACs into the custody of ORR within 72 hours of identifying them as such. The TEDS Standards also outline protocols for CBP on how to treat vulnerable populations and specify requirements for general care and conditions for children in temporary custody.

The CBP facilities we visited appeared to be operating in compliance with the TEDS Standards. While there was one exception of inconsistent cleanliness of the hold rooms, we observed that UACs had access to hygiene items and clean bedding at all facilities we visited. We did not encounter issues with temperatures or ventilation, access to emergency medical care, inadequate supervision, or access to telephones. In all nine CBP facilities we visited, UACs had access to food and snacks; the children we spoke with did not complain of hunger and said they had enough food.

³ *Results of Unannounced Inspections of Conditions for Unaccompanied Alien Children in CBP Custody* (OIG-18-87).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

We also observed that OFO ports of entry had offices and storage spaces redesigned into holding rooms to be able to hold more UACs, family units, and other border crossers referred for processing. For example, at the Gateway International Bridge in Brownsville, one hold room with a bathroom and sink was only used as a bathroom so that temporary hold rooms that did not have bathroom facilities could have access to them. The OFO ports of entry we visited have very limited number of holding cells for short-term custody. We observed in these situations when a UAC was required to be held separately from unrelated adults, there was limited ability to hold other people.

Our observations are limited to the times and locations of the team's visits and cannot be generalized to other times or locations. We are certainly aware of the deaths late last year of two minor children who died while in DHS custody and we have open investigations into the facts and circumstances of both children's deaths. We are also investigating the death of a third child who died shortly after being released from DHS custody. We will report out publicly on these investigations once complete. Additionally, several of our reports have identified significant issues with ICE facilities.

Unannounced Inspections of ICE Facilities

In response to requirements set forth by this Committee and concerns raised by immigrant rights groups and complaints to the OIG Hotline, the OIG conducts unannounced inspections of detention facilities to evaluate compliance with ICE detention standards. We generally limit the scope of our inspections to the ICE *Performance-Based National Detention Standards* (ICE Standards) for health, safety, medical and mental health care records, grievances, classification and searches, use of segregation, use of force, language access, and staff detainee communication. Our inspections focus on elements of the ICE Standards that can be observed and evaluated by OIG employees who do not have specialized training in medicine, mental health, or corrections.

In 2017, our inspection of five detention facilities raised significant concerns about the treatment and care at four of the facilities visited.⁴ At these four facilities we observed potentially unsafe and unhealthy detention conditions. Further, in violation of ICE Standards, all detainees entering one facility were strip-searched. In our two most recent unannounced inspections of Essex County Correctional Facility in Newark, New Jersey⁵ and Adelanto ICE

⁴ [Concerns about ICE Detainee Treatment and Care at Detention Facilities \(OIG-18-32\)](#).

⁵ [Issues Requiring Action at the Essex County Correctional Facility in Newark, New Jersey \(OIG-19-20\)](#).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Processing Center in Adelanto, California⁶, we found significant health and safety risks in violation of ICE Standards. Specifically, we found the following issues of concern:

- Unreported Security Incidents
- Food Safety Issues
- Facility Conditions
- Nooses in Detainee Cells
- Improper and Overly Restrictive Segregation
- Untimely and Inadequate Detainee Medical Care

Unreported Security Incidents

According to the ICE Standards, Essex County Correctional Facility must report to ICE any incidents involving detainees. However, the facility failed to do so following a detainee's discovery and reporting of a guard's loaded handgun left in a facility staff bathroom that the detainee was cleaning. This marks the fourth time in less than a year that the facility failed to notify ICE of incidents involving detainees and raises serious concerns about the facility's ability to handle security issues.

Interviews with detainees and facility management revealed facility leadership completed a review of the incident, but did not interview the detainee who found the weapon. Rather, facility leadership reported to us that they told the detainee not to discuss the matter with anyone else. The review documented by the facility does not mention that the detainee found and reported the loaded weapon.

Facility records also do not indicate that ICE was notified of the incident, as required by ICE Standards. ICE confirmed it was never notified, despite previously citing the facility for failure to report issues involving detainees, including detainee fights and hospitalization for mental illness.

During our site visit, we notified ICE of the incident and, in August 2018, ICE issued a Contract Discrepancy Report. The report outlined this incident as the fourth time in less than a year that the Essex Facility had failed to notify ICE of detainee-related incidents. The penalty for this discrepancy report can be a fine up to a 5 percent reduction of invoiced amounts. The penalty is pending final review and issuance by ICE.

⁶ *Management Alert – Issues Requiring Action at the Adelanto ICE Processing Center in Adelanto, California* (OIG-18-86).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Health and safety concerns at Essex County and Adelanto ICE Processing Center

At Essex County Correctional, we also observed extreme mishandling of meats, which of course can spread salmonella, listeria, and E. coli, leading to serious foodborne illnesses. We observed facility staff serving potentially spoiled meat to detainees. Over a seven month period in 2018, detainees filed approximately 200 kitchen-related grievances (about 12 percent of all grievances filed) with comments such as:

- “For dinner, we were served meatballs that smell like fecal matter. The food was rotten.”
- “The food that we received has been complete garbage, it’s becoming impossible to eat it. It gets worse every day. It literally looks like it came from the garbage dumpster; I have a stomach infection because of it and the nurse herself told me it was caused by the food.”⁷

The facility at Essex also presents a risk to detainee health and safety. ICE Standards require the facility to conduct preventive maintenance and regular inspections to ensure timely repairs. Despite these standards, we observed conditions that pose serious health and safety risks for detainees, including leaking ceilings in detainee living areas, showers laced with mold and peeling paint, and dilapidated beds. These facility conditions revealed serious concerns about basic maintenance and upkeep.

We observed violations of the ICE Standards at the Adelanto ICE Processing Center in Adelanto, California that were equally concerning. As detailed in our *Management Alert – Issues Requiring Action at the Adelanto ICE Processing Center in Adelanto, California*⁸, we observed braided bedsheets, referred to as nooses by center staff and detainees, hanging from vents in 15 of the 20 cells we visited within 4 housing units. Interviews with detainees provided a variety of reasons for braiding and hanging bedsheets, with one detainee noting “I’ve seen a few attempted suicides using the braided sheets by the vents and then the guards laugh at them and call them ‘suicide failures’ once they are back from medical.”

In March 2017, a 32-year old male died at an area hospital after being found hanging from his bedsheets in an Adelanto cell. In the months after this suicide, ICE compliance reports documented at least three suicide attempts by hanging at Adelanto, two of which specifically used bedsheets. Media reports based on 911 call logs indicate at least four other suicide attempts at the

⁷ *Issues Requiring Action at the Essex County Correctional Facility in Newark, New Jersey* (OIG-19-20).

⁸ *Management Alert – Issues Requiring Action at the Adelanto ICE Processing Center in Adelanto, California* (OIG-18-86).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

center from December 2016 to July 2017.⁹ In total, these reports represent at least seven suicide attempts at the Adelanto Center from December 2016 to October 2017. Nationwide, self-inflicted strangulation accounts for 4 of the 20 detainee deaths reported between October 2016 to July 2018, according to ICE news releases.

ICE has not taken seriously the recurring problem of detainees hanging bedsheet nooses at the Adelanto Center and according to a senior ICE official, ICE management at Adelanto does not believe it is necessary or a priority to address the braided sheets issue. It must be noted that all ICE detainees are held in civil, not criminal, custody. ICE detention is administrative in nature, aimed to process and prepare detainees for removal. ICE must ensure the Adelanto Center and all ICE facilities comply with detention standards to establish an environment that protects the safety, rights, and health of detainees. Although this form of civil custody should be non-punitive, some of the center conditions and detainee treatment we identified during our visits and outlined in the Management Alert are similar to those one may see in criminal custody.

ICE's Inspections and Monitoring of Detention Facilities Do Not Lead to Sustained Compliance or Systemic Improvements

In addition to our own inspections of conditions, we also are concerned by the findings of our review of the adequacy of ICE's own oversight of immigration facilities. Our report found deficiencies in both ICE's immigration detention inspection and post-inspection follow-up processes.¹⁰

ICE uses two inspection types to examine detention conditions in more than 200 detention facilities. ICE contracts with a private company, Nakamoto Group, Inc., and relies on its Office of Detention Oversight (ODO) for inspections. ICE also uses an onsite monitoring program. Yet, neither the inspections nor the onsite monitoring ensure consistent compliance with detention standards, nor do they promote comprehensive deficiency corrections.

Neither type of inspection ICE uses to examine detention facilities ensures consistent compliance with detention standards or comprehensive correction of identified deficiencies. Specifically, because the Nakamoto inspection scope is too broad, ICE's guidance on procedures is unclear, and Nakamoto's inspection

⁹ Paloma Esquivel, 'We don't feel OK here': Detainee deaths, suicide attempts and hunger strikes plague California immigration facility, LOS ANGELES TIMES (Aug. 8, 2017), <http://www.latimes.com/local/lanow/la-me-ln-adelanto-detention-20170808-story.html>.

¹⁰ *ICE's Inspections and Monitoring of Detention Facilities Do Not Lead to Sustained Compliance or Systemic Improvements (OIG-18-67)*.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

practices are not consistently thorough, its inspections do not fully examine actual conditions or identify all compliance deficiencies. In contrast, ODO uses effective methods and processes to thoroughly inspect facilities and identify deficiencies, but the inspections are too infrequent to ensure the facilities implement all corrections.

Moreover, ICE does not adequately follow up on identified deficiencies or systematically hold facilities accountable for correcting deficiencies, which further diminishes the usefulness of both Nakamoto and ODO inspections. In addition, ICE Enforcement and Removal Operations (ERO) field offices' engagement with onsite monitoring program Detention Service Managers (DSM) is inconsistent, which hinders implementation of needed changes. Although ICE's inspections, follow-up processes, and DSMs' monitoring of facilities help correct some deficiencies, they do not ensure adequate oversight or systemic improvements in detention conditions. As a result, certain deficiencies remain unaddressed for years.

ICE needs to comprehensively examine and assess its inspections process, improve its follow-up procedures for corrective actions, and ensure ERO field offices more consistently engage in overseeing detention operations. Taking such actions will help limit and correct persistent deficiencies, as well as effect long-lasting changes and systemic improvements in ICE detention facilities.

ICE concurred with all seven of our recommendations from our Adelanto Center, Essex County Correctional, and ICE's Inspections and Monitoring of Detention Facilities reports, committing to corrective action to ensure the Adelanto Center meets ICE Standards, and undertaking steps to update processes and guidance to improve oversight over detention facilities.

ICE Contracting Issues

Another way in which ICE could hold detention facilities to applicable detention standards is through contracting tools. We reviewed¹¹ how ICE manages and oversees detention contracts, as ICE contracts with 106 detention facilities to detain removable aliens. In FY 2017, these 106 facilities held an average daily population of more than 25,000 detainees. Since the beginning of FY 2016, ICE has paid more than \$3 billion to the contractors operating these 106 facilities. We found that ICE is failing to use quality assurance tools and impose consequences for contract noncompliance such as failure to meet performance standards. Additionally, the use of waivers may circumvent detention standards specified in contracts. Instead of holding facilities accountable through financial penalties, ICE frequently issued waivers to facilities with

¹¹ *ICE Does Not Fully Use Contracting Tools to Hold Detention Facility Contractors Accountable for Failing to Meet Performance Standards* (OIG-19-18).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

deficient conditions, seeking to exempt them from having to comply with certain detention standards.

In fact, ICE is not imposing financial penalties, even for serious deficiencies such as those we found in the Discrepancy Reports. In addition to the issues flagged by these Discrepancy Reports, from October 2015 to June 2018 various inspections and DSMs found 14,003 deficiencies at the 106 contract facilities we focused on for our review. Deficiencies including those that jeopardize the safety and rights of detainees, such as failing to notify ICE about sexual assaults and failing to forward allegations regarding misconduct of facility staff to ICE ERO. Despite these identified deficiencies, ICE only imposed financial penalties twice.¹²

ICE also has no formal policies and procedures to govern the waiver process, thereby allowing officials without clear authority to grant waivers, and failing to ensure key stakeholders have access to approved waivers. In some cases, officials may violate Federal Acquisition Regulation (FAR) requirements because they seek to effectuate unauthorized changes to contract terms. Key officials admitted there are no policies, procedures, guidance documents, or instructions to explain how to review waiver requests. Further, contract facilities may be exempt from compliance with otherwise applicable detention standards indefinitely, as waivers generally do not have an end date and the Custody Management Division within ERO does not reassess or review waivers after it approves them. In our sample of 65 approved waiver requests, only three had identified expiration dates; the 62 others had no end date.

ICE officials concurred with all our report recommendations, including the recommendation that ICE develop protocols to ensure that all existing and future waivers are (1) approved by ICE officials with appropriate authority; distributed to key stakeholders; consistent with contracting terms; and compliant with FAR requirements, as applicable. ICE also agreed to review all current waivers to determine continuing applicability, and, if appropriate, cancel any waivers that are no longer needed. ICE anticipates completing these actions by April 30, 2019.

Border Security: Hiring and Training DHS Law Enforcement Officials

The Department, CBP, and ICE continue to face significant challenges in identifying, recruiting, hiring, and fielding the number of law enforcement

¹² ICE deducted funds from one facility as a result of a pattern of repeat deficiencies over a 3-year period, primarily related to health care and mental health standards. The other deduction was made due to a U.S. Department of Labor order against the contractor for underpayment of wages and was not related to any identified deficiency.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

officers as mandated by two January 2017 Executive Orders.¹³ In response to multiple OIG Hotline complaints related to the performance and management of a CBP Accenture Contract, we audited the hiring contract and found serious performance issues.

CBP Needs to Address Serious Performance Issues on the Accenture Hiring Contract

In November 2017, CBP awarded Accenture a \$297 million contract to help meet the demands of recruiting and hiring agents and officers under the President's January 25, 2017 Executive Order, *Border Security and Immigration Enforcement Improvements*.¹⁴ The contract includes 1 base year, with 4 option years, to hire 7,500 fully qualified applicants, including Customs and Border Protection Officers, Border Patrol Agents, and Air and Marine Interdiction Agents.

In July 2018, we initiated an audit to determine whether CBP awarded and is managing its \$297 million hiring contract with Accenture in a fiscally responsible manner according to Federal, departmental, and component requirements. Our review determined that Accenture has not provided the promised hiring process or results, yet CBP has paid Accenture approximately \$13.6 million for startup costs, security requirements, recruiting, and applicant support. In return, Accenture has processed two accepted job offers.

Recognizing Accenture could not fulfill the contract's requirements without significant delays, CBP agreed to modify the contract to accommodate Accenture.¹⁵ Under the modification, CBP staff carried out a significant portion of the hiring operations. During this period, since Accenture could not determine which applicants it recruited, CBP agreed to give credit and temporarily pay Accenture for a percentage of all applicants regardless of whether CBP or Accenture processed the applicants. As of October 1, 2018, CBP had processed 14 applicants on behalf of Accenture. All 14 applicants accepted job offers and 7 of the 14 entered on duty, which translated to payment of approximately \$500,000 to Accenture for work CBP had completed.

In its first year, CBP's contract with Accenture has already taken longer to deploy and delivered less capability than promised. Accenture is nowhere near satisfying its 7,500-person hiring goal over the next 5 years. Further, CBP has

¹³ Executive Order 13767- *Border Security and Immigration Enforcement Improvements*, January 25, 2017; and Executive Order 13768- *Enhancing Public Safety in the Interior of the United States*, January 25, 2017.

¹⁴ *Management Alert — CBP Needs to Address Serious Performance Issues on the Accenture Hiring Contract (OIG-19-13)*.

¹⁵ As of October 1, 2018, CBP has modified the contract four times, changing the scope of work and raising the cost ceiling by about \$8 million.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

used significant staffing and resources to help Accenture do the job for which it was contracted. As such, we are concerned that CBP may have paid Accenture for services and tools not provided. CBP risks wasting millions of taxpayer dollars on a hastily approved contract that is not meeting its proposed performance expectations. CBP must hold the contractor accountable, mitigate risk, and devise a strategy to ensure results without additional costs to the Government.

Funding Limitations Impact Training

Between July 2017 and March 2018, we also reviewed and analyzed the January 2017 Executive Orders, DHS's implementation memorandums concerning the January 2017 Executive Orders, and respective agency hiring plans and training strategies.¹⁶ While the Federal Law Enforcement Training Centers (FLETC), U.S. Border Patrol (USBP) and ICE have each developed hiring surge training plans and strategies, funding limitations has delayed implementation. As a result, the Department pushed FY 2017 and 2018 hiring and training projections to FY 2019 and beyond. Funding limitations will also delay efforts to improve and construct necessary training venues and facilities.

The existing training venues are in need of improvement. Consider how USBP revised its training curriculum based on current research and identified areas to enhance training, emphasizing performance based scenarios. However, because of lack of funding, CBP has not been able to construct most of the required venues to incorporate curriculum revisions. USBP Academy instructors are conducting trainings using "workarounds" that lack performance-based realistic settings. According to a senior USBP Academy Official "the workarounds were intended as a short term fix, and are not meant to be a permanent part of the training program."¹⁷ Without necessary improvements, the quality of instruction will remain below intended levels and not include exposure to authentic environments. This presents a significant safety risk to the officers and anyone within their enforcement authority.

FEMA Oversight

DHS OIG has traditionally dedicated significant attention and resources to providing oversight to FEMA specifically. For many years, Congress funded OIG's oversight of FEMA's Disaster Relief Fund (DRF) spending through a transfer of funds from the DRF to OIG. Initially a \$16 million transfer, that number increased to \$24 million in recent years. While the FEMA Disaster

¹⁶ *DHS Training Needs for Hiring 15,000 Border Patrol Agents and Immigration Officers (OIG-19-07)*.

¹⁷ *Id.*



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Relief Fund transfer itself was discontinued in the FY 2017 appropriation, the appropriations committees directed OIG to continue to dedicate a minimum of almost \$21 million in FY 2017 and \$17 million in FY 2018 to disaster-related investigations and audits and we have done so. After the historic and devastating hurricane season of 2017, Congress also appropriated \$35 million total in a combination of no-year and three-year supplemental funding to OIG for disaster-related oversight.

Hurricanes Harvey, Irma, and Maria made landfall in a four-week time period during August and September 2017. These storms now rank as three of the five most expensive in U.S. history, according to the National Oceanic and Atmospheric Administration (NOAA).¹⁸ This makes the 2017 hurricane season the costliest in U.S. history, topping even the 2005 season, which included Katrina, Rita, and Wilma. For our office, the first order of business in response to the unprecedented disasters was to deploy auditors and investigators to FEMA's Joint Field Offices (JFOs) in Texas, Florida, and Puerto Rico. We quickly deployed staff from our local field offices as well as other auditors, analysts, and criminal investigators from around the country. Having OIG staff on the ground serves multiple purposes: we serve as an independent unit for oversight of disaster response and recovery activities, to detect and alert FEMA of systemic problems, and to help ensure accountability over Federal funds. Our deployment activities are focused on identifying potential risks and vulnerabilities and providing our stakeholders with timely, useful information to address emerging challenges and ongoing operations. Based on auditors' observations and analysis, we identified several areas where additional, more comprehensive traditional audit work was needed.

One of the chief challenges in a post-disaster environment is the vulnerability for fraud and abuse. Unfortunately, there are those that wish to profit from disasters, turning survivors into victims. Thus, OIG's criminal investigators play a very active and essential role during the post-disaster period. Our office works closely with the National Center for Disaster Fraud Hotline as we receive and process complaints. We also team with state and local law enforcement, federal partners, and U.S. Attorney's Offices in the affected jurisdictions to create local disaster fraud task forces. Currently, investigations related to FEMA fraud—from both 2017 and earlier disasters—represent 29.7 percent of OIG's currently open criminal investigative caseload.

In addition to the situational challenges facing FEMA during the 2017 hurricane season, other challenges to FEMA's programs and operations tend to be more persistent and systemic vulnerabilities:

¹⁸ Damages from Harvey are estimated at \$125 billion; Maria's damages are estimated at \$90 billion; and Irma's at \$50 billion.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- Improper procurement practices;
- Duplication of benefits;
- Mismanagement of disaster costs;
- Privacy vulnerabilities;
- Limitations in the ability to quickly protect survivors' homes and property from further damage;
- Obstacles with accurate and timely home inspections;
- Incomplete controls when providing Federal funds to high-risk entities; and
- Inconsistent contract oversight.

Unmitigated, these challenges could delay survivors' recovery and put billions of dollars of Federal funds at risk.

For almost a decade, OIG has been reporting on some of these persistent and systemic challenges in annual "capping" reports.¹⁹ These reports consolidate all of OIG's FEMA-related findings and recommendations for the year and are designed to inform FEMA headquarters officials about significant and systemic issues of noncompliance and program inefficiencies that warrant FEMA's attention. As reported in our most recent capping report—consolidating our FY 2017 audit work—between FY 2009 and FY 2017, OIG audited FEMA grant funds totaling \$13.75 billion and reported potential monetary benefits of \$6.55 billion.

Collectively, our FY 2017 work shows that FEMA continues to face systemic problems and operational challenges, and fails to manage disaster relief grants and funds adequately. Furthermore, FEMA remains ineffective at holding grant recipients accountable for properly managing disaster relief funds and providing adequate monitoring of or technical assistance to subgrantees. We continue to identify problems such as improper contracting activities, and ineligible and unsupported expenditures.

Of particular concern to the OIG, the challenges identified in our annual capping reports tend to repeat year after year. For example, our FYs 2016, 2015, and 2014 summary reports also found that FEMA did not manage disaster relief grants and funds adequately and did not hold grant recipients accountable for properly managing disaster relief funds.²⁰ Moreover, since FY 2010, we have consistently reported that states, which are required to provide oversight of grant funds and subgrantee activities, are not doing an adequate job of educating subgrantees and enforcing Federal regulations through

¹⁹ *Summary and Key Findings of Fiscal Year 2017 FEMA Disaster Grant and Program Audits (OIG-18-75)* was the ninth annual capping report issued by our office.

²⁰ *Summary and Key Findings of Fiscal Year 2016 FEMA Disaster Grant and Program Audits (OIG-18-06)*



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

effective and vigilant monitoring. We encourage FEMA to continue to take action on its commitment to strengthen grants management, including creating a plan that will identify root causes and identify solutions that are specific, viable, and can be implemented and managed to help prevent recurring problems similar to those that we have identified over the years.

Ongoing and Future Disaster Work

The OIG has a number of ongoing and planned audits related to disasters. Currently, we have audits underway regarding FEMA's Transitional Shelter Assistance Program, Individual Auto Assistance, as well as debris procurement issues. The majority of these reviews will be reported between spring and winter 2019. We are also initiating work to address mandates in the Disaster Recovery Reform Act of 2018, including reviews of state and tribal housing strategies and the lease and repair of rental units for temporary housing. We also have a number of planned and on-going audits in response to congressional requests and discretionary work, including reviews of FEMA's Sheltering and Temporary Emergency Power programs across different states and in Puerto Rico and more narrow reviews of FEMA contract management and debris removal efforts.

Ongoing projects also include reviews of:

- FEMA's Public Assistance (PA) grant awards to Puerto Rico Electric Power Authority (PREPA) and PREPA's contracts with Whitefish Energy Holdings LCC and Cobra;
- Supply chain issues related to FEMA's response to Hurricanes Irma and Maria in Puerto Rico;
- FEMA's advance contract strategy for Puerto Rico;
- Capacity Audits of various municipalities that received Public Assistance Grant Program funds. These audits, which are contracted to Independent Public Accountants, assess whether grant fund recipients and subrecipients have established and implemented policies, procedures, and practices to help ensure that funds are accounted for and expended in accordance with Federal regulations and FEMA guidance.

Finally, we will continue to conduct reviews of FEMA's oversight of state public assistance grant management and have initiated a broad review of FEMA's recovery of questioned state grant costs.

Madame Chairwoman, this concludes my testimony.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

I am pleased to answer your questions, as well as those of the other Members.

Thank you.

Ms. ROYBAL-ALLARD. Thank you, Mr. Kelly.

In January, the OIG issued a report finding that ICE has repeatedly issued waivers to contract detention facilities that are in violation of performance standards. Largely in response to that report, the statement accompanying the fiscal year 2019 funding act for DHS directs that the ICE director shall have sole authority to provide waivers. It also requires the director to notify the House and the Senate subcommittees when waivers are issued.

At what point does the issuance of waivers to performance-based standards at a facility begin to make those standards meaningless?

Mr. KELLY. It is—Madam Chairwoman, it is not good to issue waivers to the standards. Because if you start issuing waivers to the standards, the compliance starts to decrease and it creates an environment where they will be asking for additional waivers.

Ms. ROYBAL-ALLARD. So what you are saying is—

Mr. KELLY. That they are not—

Ms. ROYBAL-ALLARD. That there really aren't any circumstances where a waiver should be given?

Mr. KELLY. We shouldn't be—they should reduce the number of waivers.

Ms. ROYBAL-ALLARD. Last June, the OIG issued a report finding significant weaknesses in ICE's detention facility inspection process. In response to that report, Congress provided significant new funding to the Office of Detention Oversight with the intention of increasing the number of inspections for each facility from once every three years to twice per year.

How do you think more frequent inspections by the Office of Detention Oversight will impact compliance with performance standards? And what other steps could ICE or this committee take to improve compliance?

Mr. KELLY. Madam Chairwoman, if you are encouraging them to conduct more frequent inspections that is good. The report that you refer to pointed out that there were multiple types of inspections that ICE performs. And we pointed out that some of the inspections are not thorough enough and other inspections that are thorough enough are not done as frequent as possible—as need be.

If your recommendation is to make sure that those thorough inspections are done more frequently, that should improve quality.

Ms. ROYBAL-ALLARD. And what plans does your office have to continue its oversight over ICE's detention facility management?

Mr. KELLY. We can—have been doing unannounced inspections at the ICE facilities, as I mentioned, since 2016. And our goal is to continue those unannounced inspections.

Ms. ROYBAL-ALLARD. On another topic, we continue to hear reports about the slow speed of disaster recovery from recent disasters, in particular from the 2017 hurricane season. Next week, we will hold a hearing on FEMA's recovery efforts related to 2017 and 2018 disasters.

Members of this subcommittee and the Subcommittee on Transportation, and Housing and Urban Development will be traveling to Puerto Rico next month to see and hear firsthand how the recovery process is proceeding. And based on funding specifically provided by Congress to provide oversight of these activities, what is your current assessment of how things are going, particularly in re-

gard to recovery efforts in Puerto Rico and the U.S. Virgin Islands, and are the delays we hear about real? And if so, what do you believe to be the crux of the problem?

Mr. KELLY. Madam Chairwoman, I have been doing disaster-related work since Hurricane Katrina, and it is sad to say that the recovery process is not nearly as quick as it needs to be.

Ms. ROYBAL-ALLARD. And when do you expect to publish formal findings on FEMA's activities related to Puerto Rico and the U.S. Virgin Islands?

Mr. KELLY. We have a number of audits going on at this time. We have some audits published on Puerto Rico response. But we have a large body of work addressing the 2017 disasters and we will continue to—to issue reports on—on those disasters.

Ms. ROYBAL-ALLARD. And I would like to highlight the fact that the Inspector General for DHS is serving two customers, both Congress and the secretary—

Mr. KELLY. That is correct.

Ms. ROYBAL-ALLARD. And the relationship between an Office of Inspector General and the leadership of the agency it oversees varies across the government and—during different administrations.

How closely do you work with the secretary, her senior leadership and her senior leaders within the Department's components? And is your strategic planning done in isolation or with input from these agency leaders?

Mr. KELLY. Madam Chairwoman, I would say that the relationship that I and the—my agency has with the Department's senior leadership is very good. Every month, I meet with the deputy secretary to go over issues. Every month, either I or my chief counsel meets with the Department's chief counsel to discuss issues of concerns.

I am—I communicate almost on a weekly basis with the Deputy Secretary concerning issues. I would say that we have an excellent relationship with the—the highest levels within the Department. The relationship with the components is—is a work in progress, depending upon which agency it is, it is better than the others but it is not—it is good, but it can improve.

Mr. FLEISCHMANN. Thank you, Madam Chairman.

General Kelly, good morning again, sir. I went to the border—southwest border about a month ago to see the situation at three land ports of entry. It was a powerful trip to see what we were asking our border agents to do, to manage the influx of people presenting at and between the border situations.

I think everyone on the trip felt that CPB needs more agents. However, your audit report of last week regarding CPB hiring outlines a troubling situation with planning and hiring at the agency. My first question, sir, is how best would you describe the Department's response to not hiring up to the level mandated by this committee nearly eight years ago? Apathy, confusion, good intentions overrun by other demands, how would you characterize it, sir?

Mr. KELLY. I would say probably the latter. They have good intentions. They want to hire the agents; I don't think there is any desire for the Department or CBP not to hire the Border Patrol and ICE officers.

But there is a challenge to hiring them. There's a relatively—the number of people that are applying for the positions are not always adequate to fill all those positions. They have to have a very rigorous process of bringing them onboard. We have been critical of the Department and CBP specifically for not strategically addressing this issue.

The report that you refer to pointed out that back in 2011 this committee demanded that they have a plan. They provided that plan to this committee in 2013, you said that that plan was inadequate and they haven't really come up with a better plan since then. And that—that is pretty much what that report said, I believe.

It—the—but it is a challenging situation to get those men and women to perform those functions, it's a difficult issue and it's not an issue that just—the Border Patrol and ICE has with hiring with law enforcement officers, that is a government-wide problem.

Mr. FLEISCHMANN. Yes, sir. The fiscal 2019 statement of the manager's direct CPB to brief the committee's monthly on its progress toward the development of the staffing model. How confident are you that the agency is up to this task? And then as a follow-up, what questions should we be asking, sir, to keep the Department on track?

Mr. KELLY. I don't want to judge as to how good they are going to be able to do something that they are planning to do that we have not looked at. We have historically found that they have had challenges in this area. The—we have identified problems with polygraphing and making sure that they are interviewing the right individuals in the past.

I would look for their metrics, because often the Department has had poor metrics as to evaluate how well they are doing their job. And I would hold them accountable to their metrics, and try to make sure that their metrics make sense and that they are sufficient to achieve their goals.

Mr. FLEISCHMANN. Combining the issues in the report about hiring with the issues you highlight in the November 26th audit report about training capacity, I see that the Department has had a busy year ahead to—to address the stated recommendations. Say CPB successfully completes a staffing by the end of the year, other than issues of training and specific dollars for new hires are you also looking at CPB's capabilities to successfully onboard many new agents?

Mr. KELLY. The answer to that is yes, we have looked at that. We issued a report, I believe, in 2017 or 2018 addressing issues with onboarding the individuals. The—it is going to be a challenge. The CBP—or, I am sorry, FLETC simply does not have the facilities or the funding to perform all the training that is required.

Mr. FLEISCHMANN. As a follow-up to that comment, sir, would the agency be able to successfully undertake a massive hiring effort?

Mr. KELLY. They would be challenged.

Mr. FLEISCHMANN. Can the agency administratively field successful applicants?

Mr. KELLY. They will be challenged to achieve their goals. They have not achieved their goals in the past. I believe last year was

the first year that they actually had a net increase in the number of Border Patrol agents and it's a relatively small increase that—it doesn't address the 7,500 increase that is the goal.

Mr. FLEISCHMANN. Thank you, General Kelly.

Madam Chair, I yield back.

Ms. ROYBAL-ALLARD. Mr. Ruppertsberger.

Mr. RUPPERSBERGER. Yes, thank you for being here today. I want to get into what our chairwoman talked about a little bit, about your unannounced inspections.

I think in the fiscal year 2019 spending bill the congressional report obligated the Office of Inspector General to continue its program of unannounced inspections at all the CBP and ICE facilities. We know that—that you have found in some of those unannounced inspections some really bad conditions that needed to be dealt with.

And my question, to our knowledge, the OIG has been able to conduct a relatively few amount and is that because of your budgetary restraints? What do you need to be able to do more to have these unannounced inspections? Because from what I have seen so far, that is probably the best accountability we have when you have these unannounced inspections.

Mr. KELLY. We appreciate the funding that this committee provides to the DHS OIG. The—and we will use the funding that you provide—provide us, and the instructions that you provide concerning that funding to achieve the goals that you are looking for. We do have to balance a lot of different issues. We have disaster issues, we have Coast Guard issues, there are other issues with CBP and ICE, we also have the Secret Service and we have a lot of the departmental programs that we also have to address.

The chairman mentioned a strategic process that we have for hiring individuals—or, I am sorry, for performing the work that we do. And that looks at the highest risk programs within the Department. After becoming the Acting Inspector General, I revamped our jobs start process to make sure that we are addressing the highest risk areas within the Department.

Homeland Security is not like some of the other agencies that are—that is relatively static. We have a very dynamic environment that we need to be able to adjust our goals and—and priorities to what is the most important thing to both the Congress and to the Department because we are dual—

Mr. RUPPERSBERGER. And you are right about that. I believe that when we started the Homeland Security we had way too many missions with not a lot—not enough manpower or resources to do the job in many areas. And thank goodness, when the Coast Guard came over, they too do a lot without resources, but they at least are an old organization that was well managed, so it's a real challenge.

I am going to get into one area before my time is up that you weren't prepared to talk about today, but that is in the issue of cybersecurity.

Mr. KELLY. Yes.

Mr. RUPPERSBERGER. You know, the—again Homeland Security has a tremendous amount of responsibility and missions because of the new laws we passed throughout the years. And could you discuss with me where you think our cybersecurity programs are

today? Do you feel that we need more—more manpower and technology to do the job that we have been given?

You know, I think this is so important. One the biggest threats we have in our country, cybersecurity. That I would hope that maybe it would be considered a separate agency with a direct line to the President or whatever, to just make sure we get the funding and—and the priorities.

But at this point, I also know that cybersecurity has been elevated in the Department too maybe that might help. Could you discuss that issue, please?

Mr. KELLY. I would say that it is a work in progress. And I agree with your assessment that this is one of the highest risk areas that the—the Federal Government has. I have directed some of our staff to do that work in the cybersecurity area. That is a very technical area and is very difficult to attract and hire the people with the right capabilities to do that work.

Mr. RUPPERSBERGER. Do you work at all with NSA? I know they have no jurisdiction in our country, but they have a lot of expertise. Do you meet with Inspector General?

Mr. KELLY. Actually, I belong to the Inspector General of the Intelligence Community. And we meet regularly once a quarter. So the answer to your question is yes, I do meet with him and I know Bob Storch personally.

Mr. RUPPERSBERGER. Are you in the process of rendering a report on cybersecurity—you know, with these—

Mr. KELLY. I believe I have an ongoing engagement in that area.

Mr. RUPPERSBERGER. Well, I would like to hear more about that and I will have my staff contact you.

Mr. KELLY. OK.

Mr. RUPPERSBERGER. OK, thank you.

I yield back.

Ms. ROYBAL-ALLARD. Mr. Newhouse.

Mr. NEWHOUSE. Thank you, Chair Roybal-Allard, I appreciate the—having this hearing.

Welcome, General Kelly—

Mr. KELLY. Thank you.

Mr. NEWHOUSE. I appreciate you being here and giving us an update on what you found at the border and some of the areas of responsibility that you have. I, you know, certainly this is an issue that is occupying a lot of our time, as it should, the issue of issue immigration—the bigger issue of immigration but also the securing our border, both on the south and the north, which I happen to have in the state of Washington is a concern as well.

And I don't think any of us on the panel or in Congress would agree—or disagree that something has to change. And to that end I, myself, went to the border to see firsthand. In fact, I think I was there a similar time that your inspectors were at McAllen.

Mr. KELLY. I was down there with that group myself.

Mr. NEWHOUSE. Oh, is that right?

Mr. KELLY. Yes.

Mr. NEWHOUSE. Yes, it was kind of warm that day, if I recall.

Mr. KELLY. It was. [Laughter.]

Mr. NEWHOUSE. I came away fairly certain in the opinion that we have to ensure that DHS has the tools that they need to do

their job that we are asking them to do, and that we should also have proper oversight on how we treat people that are wanting a better life for themselves and their families.

And in my time there, I—like I said, I toured some of those same areas. And while I don't—I am not going to say I disagree with your report, there are just parts of it that I think need some clarification for me. And if you would—

Mr. KELLY. Okay.

Mr. NEWHOUSE. If you could address some of that, it has to do with the separation of the family units, whether they would be at a port of entry or between ports of entry. I would also make the point, I don't—I would agree with you that we don't have enough men and women at the border, as either Customs officials or Border Patrol agents. Like I said, we are asking them to do a near impossible job and we need to give them all the tools that they need in order to be successful.

So could you talk a little bit more about the zero-tolerance policy and what you witnessed there? Can you tell me if—in your opinion, if a family came and presented themselves, was that an immediate—because of the zero tolerance, was that an immediate flag to separate these family units?

I would just like to have further clarification because I think—from what I understand in the DHS's response to your report—that they are, in my words, saying that you misrepresented or at the very least conflated their process that they use. So I would just like some clarification on whether you witnessed families automatically being separated.

Mr. KELLY. The response that the Department had to that report, they said that we presented it not as clearly as—that there was a difference between family separations and the zero tolerance. And that is correct, there—that is two different policies. But one is caused by the other, so you can't really separate them but they are two different policies.

And that is what—how we responded to that question as to what was the—why—when they pointed out that we didn't describe it—they said it made it—we made it sound as if it was the same policy, when in fact it was not. And if you actually look at the report, we don't say it is the same policy but one does cause the other. So that is—does that answer your question?

Mr. NEWHOUSE. But did you see families being separated?

Mr. KELLY. When I was physically there, did I observe the separation of individuals? I didn't. I don't know if some of the other inspectors that—when we were down there did.

Mr. NEWHOUSE. But you, I am sure, talked to people about that—

Mr. KELLY. Yes.

Mr. NEWHOUSE. The fact that some of that happened. Any reasons given for that?

Mr. KELLY. Well, the policy is—DHS's policy is that an unaccompanied child—or a child should not be with someone who has been violating the law or needs to go to—for processing. At that point in time, the child is separated from the adult.

Mr. NEWHOUSE. I see, okay. Got you—

Mr. KELLY. There was—there were situations where they talked about when the parent went to see the judge, sometimes that the child was—when the parent came back, the child might have been moved off to some other place because of some of the time requirements for moving the children—because they are only supposed to be there for a limited amount of time.

Mr. NEWHOUSE. Well, I see my time is expired. But I appreciate your answers. And like I said, this an area of great interest—

Mr. KELLY. Yes.

Mr. NEWHOUSE. And concern. So thank you very much.

Mr. KELLY. The issue that was—the Department had with us was a nuance on which—there are two policies but one causes another—the problem.

Mr. NEWHOUSE. Thank you, Madam Chair.

Ms. ROYBAL-ALLARD. Ms. Meng.

Ms. MENG. Thank you, chairwoman. Thank you, Ranking Member Fleischmann.

And thank you to, General Kelly, for being here and for your service to our country. I wanted to ask about processing delays at USCIS. They have reached crisis levels threatening American families, businesses and many vulnerable populations seeking humanitarian relief.

USCIS's proposed fiscal year 2019 budget requested the transfer of over \$200 million in fee revenue out of USCIS into ICE. The budget specifies that that money would be used for the hiring of over 300 ICE enforcement officers. And this appears to represent part of USCIS's larger shift towards prioritizing immigration enforcement over the service-oriented adjudications at the core of the agency's mandate. What is the OIG doing to ensure that USCIS carries out its duties and services?

Mr. KELLY. We do have some engagements at USCIS, but I do not think that we are looking into that specific issue. I can get back to you at a later date to let you know whether or not we actually do. But off the top of my head, I don't know of any engagements that we have in that area but I can get back to you on that.

Ms. MENG. That would be great. As you probably know, the backlog has more than doubled in just the last year, from about 1 million to the current backlog of 2.3 million. So I would appreciate that.

I also wanted to ask about an article that came out last week, I think it was the Huffington Post, about Adnan Asif Parveen, a Muslim man who was arrested and detained in Texas. According to this article, CPB officers gave him pork sandwiches to eat for the entire duration, 6 days, of his detainment and ignored his religious dietary restrictions.

Has there been or will there be any investigations into CBP and its treatment of detained individuals? And in the interest of time, I will just ask my other question. What protocol is in place to ensure that religious and dietary restrictions of detained individuals are met?

Mr. KELLY. I don't know the answer to that question but we can get back to you on that. And I am not sure if we have opened up an investigation. We could have, but I am not sure. And that would

be probably different than an audit but we can get back to you on both of those issues.

Ms. MENG. Okay, thank you.

And then back to the family separation issue real quick. What is the policy of families which are—who are separated at the border in terms of phone calls? If a mother is separated, whether her children are still at the border or elsewhere in the country, what are the policies for making calls?

Mr. KELLY. There are phones available. But at times it's difficult to make some of those calls because it is—you don't know where the individual necessarily might be.

So as I mentioned in my oral remarks, we did notice that there were phones available. But that doesn't necessarily mean that they are going to be able to communicate because they might not know the telephone number that they would need to be calling to. They might not know the area code and a variety of different things.

Ms. MENG. Right. When—I know that you mentioned the ability to access phones. However, when many of us were at the border Port Isabel and McAllen, we spoke with moms who said that they hadn't been able to make phone calls.

Many of these moms had the piece of paper with the phone numbers of relatives in this country that they wanted to call and it was very inconsistent across the board. Some moms were allowed to call once a week, some mom hadn't—moms hadn't been able to make phone calls for weeks on end.

Mr. KELLY. I know some of the detention facilities that we went into there were phones in the areas where the mothers were at. Whether or not they could get through to those locations, I can't tell you the answer to that.

Ms. MENG. Okay. Thank you. I yield back.

Ms. ROYBAL-ALLARD. Mr. Aguilar.

Mr. AGUILAR. Thank you, Madam Chair.

Mr. Kelly, thank you for your service and for being here today. I am concerned about the second point in your testimony regarding technology. The OIG report published in September 2018, you noted that DHS did not have readily the technology infrastructure that was needed to track family separations when the President's zero-tolerance policy was created.

You also note that there is inoperability between HHS, CBP and ICE that have all separate information technology systems to track immigrants entering the United States. The big issue was that CBP did not have a category for family units, as we understand, and unaccompanied children in their records, including allowing a system that didn't match those records.

Last week, I attended a meeting with the Congressional Hispanic Caucus and HHS Assistant Secretary Johnson. And during the meeting, she expressed that she would like DHS to share with HHS the list of parents who were separated from their children and that contact information. Can you share with us whether DHS has access to the I.T. portals that currently house information related to undocumented parents and children who were separated specifically between CBP, and ICE and ORR?

Mr. KELLY. As a result of that report, I ordered an audit of the information technology systems that exist within CBP and ICE to

see if they can—how well they can track the—both parents and the children that were—that came across through to—into the United States. That is an ongoing audit and as soon as that is completed we can get that to the Department. We expect it to be completed sometime this summer.

Mr. AGUILAR. And how long will the Department have to comment on that before it's released?

Mr. KELLY. Thirty days.

Mr. AGUILAR. Will your report also talk about the operability between ORR and CBP and ICE?

Mr. KELLY. We have worked with ORR when we are down at the border. We did see the individuals from HHS. And there has been a recent HHS-OIG report addressing the—also the challenges with the data that is sent to them.

Mr. AGUILAR. In your opinion, should there be one portal that is—that can be accessed by HHS and ORR as well as CBP and ICE?

Mr. KELLY. Ideally? Personally the answer is yes. And we are trying to—we are—we have an audit going on that is addressing some of those challenges, though—

Mr. AGUILAR. Okay. Will your audit—will the result of that audit shed better light on this issue and whether that is possible?

Mr. KELLY. I intend—I expect that the answer is yes.

Mr. AGUILAR. Thank you, sir.

In January of 2019, there was an HHS-I.G. report that indicated that the total number of children separated from their parents is unknown. With that in mind, do you anticipate that report will also shed some light on—on that number moving forward?

Mr. KELLY. The answer is yes, but I do not know if we are going to be able to give a definitive answer to the—your question.

Mr. AGUILAR. But you might get to some of the issues that cause the answer being unknown?

Mr. KELLY. That is the goal of that work, yes.

Mr. AGUILAR. Okay. Would you say that the President's—that President Trump's decision to announce a zero-tolerance policy with little notice highlighted the existing weaknesses between the information systems related to unaccompanied children? And would you say that DHS is prepared to handle any other surprise policies that the president may announce with?

Mr. KELLY. I am on record for saying that they were unprepared for the zero-tolerance policy. And that caused difficulties. I am also on the record that the Department was not prepared for the travel ban that was established in January of 2017. And I—our major management challenge report that we issued late last year talks about the challenges that the Department has addressing some of these policies that they don't get an adequate time to plan for the consequences of.

Mr. AGUILAR. I appreciate your answer. Following up on Mr. Newhouse's point, when the secretary went on TV and said, quote, we do not have a policy of separating families at the border, period. And she indicated that that was misreporting, that it was irresponsible and unproductive, what was—what was your reaction to that?

Mr. KELLY. I don't know. I don't have an answer to that question.

Mr. AGUILAR. I appreciate it. Thank you.

Thank you, Madam Chair.

Ms. ROYBAL-ALLARD. Mr. Cuellar.

Mr. CUELLAR. Thank you, Madam Chair.

Mr. Kelly, thank you for what you do. Let me talk to you about the staffing model for Border Patrol.

Mr. KELLY. Yes.

Mr. CUELLAR. I believe in 2011, this committee directed CBP to submit a five-year staffing and deployment plan for Border Patrol. They came up with a plan but it did not meet the goals for border security. So again, the committee requested them to come up with a staffing and deployment plan by December 1st, of 2013. I believe we still don't have that plan, is that correct?

Mr. KELLY. That is correct. We issued a report just recently that pointed out that you did require them in 2011 to prepare a plan. The plan that they provided to you in 2013, that was delivered to you, the committee said was unacceptable or not—it did not satisfy their needs.

And our report that we just issued said that the plans are still not adequate to satisfy the needs of the committee. The Department concurred with our recommendations; however, they tried to minimize our findings. But we also, in our response to their comments, told them that we think that our findings are solid and that they need to get a plan to satisfy the needs for the committee, and it is not simply to satisfy the needs of the committee, it's actually to satisfy the needs of what their—their responsibilities.

Mr. CUELLAR. Yes. And I think under a recent report, you said that you found that Border Patrol lacks the data procedures needed to determine whether it is meeting workload requirements related to investigative law enforcement activities, and Border Patrol officials are not consistently schedule agents work duties, or accurately document actual work hours and duties completed.

Mr. KELLY. Yes. And I think we identified a large number of hours that they couldn't account for.

Mr. CUELLAR. Did they respond to that?

Mr. KELLY. They concurred with our recommendations. They did—we are seeing an uptick in concurrence with our recommendations, but then tried to address the message to say that they are doing a better job than we are portraying. And I don't think that that is an accurate assessment.

And you will see in our reports, when they tried to take that approach, we point out that their positions are—they are doing improvement—they have improvements. But it is not adequate to address the challenges. And so we are not saying that they are not trying to improve and we are not making—we are not saying that they are not making any improvements, but they are just not up to what they needed to do.

Mr. CUELLAR. Right. And as you know, Border Patrol is short I think about 2,200 personnel.

Mr. KELLY. Yes.

Mr. CUELLAR. CBP or, you know, the folks at the ports are doing a little better. In fact, we added money to hire—what is it, about 600 and then if they use some of the fees they can double the amount. Air Marine, there are three uniforms down there—

Mr. KELLY. Yes, yes.

Mr. CUELLAR. I keep telling my friends that. They said it—there are three colors there, the green Border Patrol, blue the folks at the ports of entry—

Mr. KELLY. Right.

Mr. CUELLAR. And then the brown—not UPS as one of my friends said, but it's actually Air Marine. And Air Marine is short on pilots also.

Mr. KELLY. And we have a report out that points that out. We pointed out that the request—CBP requested flights from Air and Marine, and over fiscal years 2015, 2016 and 2017 Air and Marine was only able to provide—I believe it was 18, 20 and 17 percent of the requested number of flights.

Mr. CUELLAR. Right and that is—we see at the border, Border Patrol is asking for more air coverage and—but they just don't have the hours or the personnel to cover that.

Let me ask you a quick question. Based on your evaluations of compliance with ICE detention standards, how do ICE detention standards fare compared to other U.S. law enforcement agencies?

Mr. KELLY. I can only evaluate what DHS is doing and what ICE is doing. We have not initiated a review that goes across to look at what is going on at the Justice Department or for the Bureau of Prisons. That is something that is probably beneficial but we have not done that. We would have to do that in concert with the Inspector General up at Department of Justice.

Mr. CUELLAR. If you all decide to do that, let us know.

Mr. KELLY. Okay.

Mr. CUELLAR. Thank you so much.

Ms. ROYBAL-ALLARD. All right, Mr. Price.

Mr. PRICE. Thank you, Madam Chairman.

Good morning, Mr. Kelly, glad to have you here and I appreciate your responding to what appears to have been a wide array of topics.

Mr. KELLY. I try to answer them. Some of the questions, I don't have answers to but we will try to get back to the members on the questions we don't have answers to.

Mr. PRICE. Well, your, of course, your mandate covers the entirety of the Department and I am going to ask you about another subject that we have actually asked you to investigate.

And I am not—this was in December, I am not going to ask you to anticipate the results of that investigation, although I would appreciate some kind of timeline as to when we might expect an answer. And also, I want to ask you about a couple of questions the investigation involves that perhaps you do have a ability to respond to at this point.

Just very quickly, I won't go into the details of the case except to say that that this involves an arrest and deportation of one Samuel Oliver-Bruno in November 23 of last year, a decades-long resident of North Carolina, no significant criminal history, U.S. citizen, teenage son, a very seriously ill wife. He received a stay of deportation in 2014, the use of prosecutorial discretion by ICE in subsequent years but he was denied further relief by ICE under this administration in 2017.

Forced into taking sanctuary in a local church to avoid being deported and being separated from his ill wife. His second stay of de-

portation was denied by ICE in 2017, so he decided to seek deferred action status from USCIS, from another agency. He was given strict instructions to appear at a USCIS office to provide biometrics for that application. But when he did so, guess who was waiting there, ICE. And he was sent to a detention facility in Georgia and—to await what looked like a sham appeal and he was shipped out of the country.

This was, of course, an obvious case where prosecutorial discretion, and compassion and commonsense might have been applied. But I want to ask specifically about this interagency aspect which is unique and, I think, needs to be addressed.

It appears that ICE officials used the CIS request to lure Mr. Bruno—Oliver—Bruno out of sanctuary and to apprehend him. Now, the ICE officials say they learned about this from social media, they may or may not have. But in any case, when he went to CIS, there—there they were. And they took him—took him into custody and all appeals up the line have failed.

So you can imagine, coupled with the—these random and unnecessary ICE raids proliferating throughout North Carolina, we just have a significant erosion in public trust. So I am very concerned about this. But I know you will have particular focus on this interagency problem. And so that is what I want to ask you about.

Are there any protections within the overarching DHS framework to ensure that two DHS agencies don't coordinate arrests in a fashion that seems to entrap immigrants? What more needs to be done to establish a clear separation between these two different legal processes?

The man in good faith is leaving sanctuary to go to CIS and there they are waiting for him. That certainly looks like entrapment, but I am not asking you to judge that. I am asking you to judge if there is any protections within the existing law or practice to prevent that kind of coordination.

And then, when this does exist, can you point out where in—where this may exist or where there is a double interest and interest in a person from two agencies, who says ICE prevails? ICE's interests prevail or ICE priorities are given more weight than the laws that are guiding USCIS? So why—why should that be or is it so?

So not anticipating your investigation, although I do want to know when we can expect some evaluation from you, I wonder if you could address those two issues.

Mr. KELLY. I am familiar with your request. The—I am not familiar with the specifics of what we have done on your request, so I will have to get back to you at a later date. And—but I don't know the answer, nor do I know the answer to whether or not—how the two components within Department of Homeland Security are sharing information.

Mr. PRICE. So you have never dealt with this in prior investigations, or?

Mr. KELLY. I have not. We have—I am not familiar with that issue.

Mr. PRICE. As far as you know, is this a unique case? Any other similar situations that have come to your attention? That—see, I

think if they did come to your attention probably you would know about it. It is a—quite a striking set of circumstances.

Mr. KELLY. It coming to my attention, the answer is no. But that does not mean that it—that other people within my organization are not aware of that and can speak more to the point on that. Right—so I would—I would have to get back to you on that question. I can't give you a definitive answer.

Mr. PRICE. All right. Well, my—I know my time is expired. But to the extent you can respond to my two questions regarding the provisions for coordination between these two agencies and which agency takes precedence in a situation like this, I—it is obviously pertinent to this case, but it also is more broadly pertinent. So I would appreciate your response.

Mr. KELLY. I agree with you. But I can't give you a definitive answer. I will have to get back to you at a later date.

Mr. PRICE. All right. Thank you.

Thank you, Madam Chairman.

Ms. ROYBAL-ALLARD. That completes round one and we do have time for a second round—

Mr. KELLY. Okay.

Ms. ROYBAL-ALLARD. Mr. Kelly.

Mr. Kelly, as you know, the mission of the DHS is vast. And carrying out its mission ranges from disaster relief grants to states to massive procurements of aircraft and vessels, to developing cutting-edge technologies to protect the public. And your office produces a number of documents, including a five-year strategic plan, and annual performance plan and semi-annual reports, which ideally outline your priorities and performance.

How do you assess DHS's major vulnerabilities and allocate your resources to ensure you are focused on the best use of the Department's funds? And is there a direct relationship between the strategic documents that you produce and the priorities of your budget request?

Mr. KELLY. As an oversight agency, we have our most—the only reason why we exist is to keep you, the Congress, and the administration timely informed about problems that exist within programs under their purview. So within our strategic plan, our goal is to make sure that is basically three issues. Is the Department operating efficiently and effectively? Are we hiring the right people? And do we have the right tools to execute our mission?

The issue concerning the work that we do, as I mentioned earlier, we have recently revamped and established a new start process where we are looking at what is the most important issues that affect the Department. When I took responsibilities as the Acting Inspector General—actually, my predecessor stopped the annual work plans that they had because they basically represented what was important 2 years before they started work. And in a dynamic agency like Homeland Security 2 years is almost a lifetime.

We can't decide what was important 2 years ago for what we are doing right now because we would be doing completely different things. So we are taking all the requests coming in from Congress, we are taking the requests that we get in from the department and we also take the subject matter expertise of the people that have been doing this work for an extended period of time and blend that

and have all the senior executives sit down on a weekly basis to make sure that we are doing the right work.

I think that has been very beneficial. We have been operating this—in this fashion for nearly a year and it enabled us to immediately go down to the border last summer. And to address some of the ICE detention facilities that we believe are a higher risk and that—they are the facilities that you need to hear about, such as the facility in Newark, New Jersey and Adelanto, California, as I mentioned in my oral statement.

Ms. ROYBAL-ALLARD. You mentioned that your primary mission is to keep Members of Congress informed.

Mr. KELLY. Yes.

Ms. ROYBAL-ALLARD. So are your resources sufficient to effectively carry out that mission and if you had more resources where would you focus?

Mr. KELLY. If we had more resources we would focus those efforts on the highest risk areas and those right now are some of the border issues and also some of the disaster issues that we would be that are important issues to get into.

We do appreciate the funding that the department—I am sorry—that the committee provides to us. But we could use more resources and each year both my predecessor and I have petitioned for additional resources to address our needs.

We do appreciate the supplemental funding that we received for the 2017 disasters. That enabled us to do some very important work in those areas; it has kept our criminal investigators very active and—but we certainly can use more resources. The issues that affect the department are high-risk areas, they are very dynamic and they need to be addressed quickly, not the typical I.G. audit that talks about issues that are 3 or 4 years old and said that things didn't go well. That is not a very effective way of running an I.G. shop and I have tried to modify that process.

Ms. ROYBAL-ALLARD. And just finally, do you communicate directly with OMB or does your budget request always flow through the department?

Mr. KELLY. We communicate and I have had meetings with OMB. We do submit our budgets to the department but we also have separate meetings with OMB, I have met with them personally on a number of occasions and I know my predecessor has. And then we also have special meetings just with your staff and I have worked with member—a number of the staff that are sitting behind you on what our needs are.

So that is one of the nice things about being an Inspector General that if we—the department doesn't give us what we need we have the authority to come directly to you and let us know—and let you know what we need.

I often point out to the members of the staff and the members that you are usually our biggest proponents because we are your eyes and ears to find out what is going on and we are the quickest way of getting information to you about the challenges that the department is facing.

Ms. ROYBAL-ALLARD. And we appreciate your responsiveness to us. Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you again, Madam Chairman.

Mr. Kelly, thank you again, sir. Next week the subcommittee is holding a hearing with FEMA regarding the recovery efforts in Puerto Rico and the U.S. Virgin Islands after 2017 storms. In your testimony you highlighted your work with the affected areas, such as deploying staff and establishing joint field offices. And you state that as a result of that deployment your staff identified several areas where additional more comprehensive, traditional audit work was needed.

Can you share what areas that worked you have identified in Puerto Rico and are challenges you see in Puerto Rico different from what you are seeing in Texas and Florida, sir?

Mr. KELLY. I also went down to Puerto Rico shortly after the disaster and I was quite shocked at the devastation that existed on that island. I have spent—visited numerous islands, lived in Hawaii for a period of time. I spent an extensive amount of time in Guam and I was extremely surprised to see how vast the island of Puerto Rico is, it is much larger than either of those two islands— or Hawaii, the chain of islands.

And the challenges that they were facing were far more difficult than I have experienced—I have seen FEMA have to experience in some of the mainland disasters that they have dealt with. So it is a very difficult thing for them to do. But FEMA's responsibility—when your name is Federal Emergency Management Agency you are expected to be able to manage emergencies.

And the—if you are a U.S. citizen, you are expecting the Federal Government to provide the assistance that is necessary when you go through a level of disaster that is—was pretty unprecedented.

Mr. FLEISCHMANN. Thank you, sir. I am sure you are working closely with the department and FEMA on programs and efforts underway in Puerto Rico, when we meet with FEMA next week what questions should we be asking the agency on the record in regard to the 2017 storm recovery.

Mr. KELLY. I would ask them to compare their response and recovery rate to other disasters and see if their metrics for Puerto Rico and the Virgin Islands compare favorably to other disasters that they have dealt with.

Mr. FLEISCHMANN. Thank you. Your testimony highlights 8 listed persistent and systematic vulnerabilities with FEMA programs. Are these challenges you see across the country with respect to the disaster programs? Are they limited to one state, one storm, or one type of disaster? What is your view?

Mr. KELLY. The biggest problem that we have with FEMA is that they don't hold states accountable. And that is the—that is the most significant problem that we have with FEMA because by not holding the states accountable they basically tell everyone that the policies that they are—that exist, you know, you can do them or you can't do them—or you can comply. If you don't comply with the policies, we will find a way out of it.

And it is a lot like the waivers question that I had earlier at ICE detention facilities. It is not good to basically waive a lot of things because then you are creating a culture in which individuals believe that they don't have to comply with the requirements, the requirements that were setup to protect the tax dollar—the taxpayer

and the people that were affected by disasters. That balance is important.

And when you do waivers or don't hold people accountable, the taxpayer is the one who loses. Because the American taxpayer is very generous, they want to make sure that people that are affected by disasters are made whole. But what they don't like is when people are getting away with things that they shouldn't be getting away with.

Mr. FLEISCHMANN. Thank you, sir.

Madam Chairman, I will yield back.

Ms. ROYBAL-ALLARD. Ms. Meng.

Ms. MENG. Thank you, Madam Chairwoman.

On June 27, 2018, ICE's New York field office announced that starting immediately removal proceedings at the Varick Street Immigration Court in New York City would be conducted exclusively by video teleconferencing. Immigrants detained by ICE would appear by video feed from the county jail at which they are held, disconnected from the court, their lawyers, evidence presented by the government and their case.

ICE's policy of denying in-person hearings when immigrants' liberty, family unity and potential exile is at stake is a cruel extension of the Federal administration's aggressive efforts to deny immigrants equal justice and due process. What steps can you take to ensure that immigrants and their families have meaningful access to due process?

Mr. KELLY. The facts and circumstances of the—of what you just described to me, I am not aware of. The—that is doing some more work in those areas are the kind of things that if we had more resources we could probably do some more work in those areas. If we get requests from members of Congress, we consider them to be a—things that we try to do. We do get—I probably get a letter from members almost—probably it average nearly once a day for various different issues.

But what you just described does not sound very nice. It doesn't sound to be the kind of principles that the United States wants to stand for. It is very similar to the issues that Congressman Price mentioned earlier about teaming up and going after individuals. But I am unaware—I was unaware of what you just described.

Ms. MENG. So would it help if you did receive letters—

Mr. KELLY. Yes.

Ms. MENG. And communication information—

Mr. KELLY. We—

Ms. MENG. About lawsuits that might be going on?

Mr. KELLY. Communications from Members of Congress to our office are always desired because our statutory requirement is two-fold. It is to keep Congress and the administration timely informed about problems.

We take our dual reporting relationship very seriously and if anyone in my office—they joke how often I bring up our statutory authority and what we need to do in our responsibilities. Because it is, you know, here he goes again talking about the dual reporting relationship, it is very important to us.

Ms. MENG. Thank you, sir.

And another situation that is going on around across New York state courthouses, reports by the Immigrant Defense Project reported that ICE arrests across New York courthouses increases by 1,700 percent in 2018 compared to 2016. ICE arrests at courthouses impede the ability of the courts to effectively deliver justice, deter victims from seeking justice and compromise public safety. We have heard from so many public defenders and defense attorneys about agents showing up in the courthouse, in public areas where folks are trying to be with their families.

This figure is astounding. And in 2018, as you know, ICE had issued guidance on civil immigration enforcement actions inside these courthouses. Will the OIG investigate or audit the immigration enforcement actions at courthouses and its effect on public safety?

Mr. KELLY. Again, I was unaware of what you were just describing. We do annually meet with the NGOs to have them talk to us about some of the issues of their concern because we don't want to be tone-deaf to issues of various different groups.

They have—I don't remember them talking to us about those issues, they were typically talking—their biggest concerns were border issues and also the travel ban. They were not just—I don't remember them mentioning these issues to us. So again, you are telling me things that I am a little unaware of and the best I can do is try to get back to you on some of these things.

Ms. MENG. Sure. Thank you. As you know, families are being separated and defendants are not showing up to court because of this issue. So we will make sure that they are getting you the proper information.

Mr. KELLY. Okay.

Ms. MENG. Thank you, sir.

Ms. ROYBAL-ALLARD. Okay. Mr. Kelly, I think you will be getting a letter of request from us on these issues. [Laughter.]

Mr. Newhouse.

Mr. NEWHOUSE. Thank you, Madam Chair.

Mr. Kelly, part of your testimony and your written testimony in particular, they talk about FEMA and the responsibility to manage disasters.

Mr. KELLY. Yes.

Mr. NEWHOUSE. And I just wanted to further the thinking—or the—some of the questioning Mr. Fleischmann was asking you about. You reading between the lines, you—it seems to me you are expressing some frustration, some of the systemic problems and operational challenges that FEMA has.

Mr. KELLY. Yes.

Mr. NEWHOUSE. And it is across administrations, it has been a situation for quite some time. But you state that they remain ineffective at holding grant recipients accountable for properly managing disaster funds. You cite 2016, 2015, 2014, even back as far as 2010 issues with accountability holding states accountable for managing grants. All of those, if they are not frustrating to you, they are certainly—reading that is frustrating to me.

And in your comments you talk about encouraging FEMA to take steps to—for corrective action. And I guess, you know, part of this is on Congress, too. Is Congress not listening to some of the rec-

ommendations of the Inspector General on what could be done or other things? I would just like to have a further conversation so that we don't just measure things after the—after all this money goes out the door and then—and then the same thing happens the next year.

Mr. KELLY. Yes. I am very much against the types of recommendation or the types of FEMA audits that basically are spilt milk type of things. I am looking at more systemic problems that exist and how to correct those systemic problems and that is holding states accountable.

My predecessor wrote a letter, and I will share that with the committee, to Chairman Johnson about some basic challenges that FEMA really needs to take to correct their longstanding problems. That letter is about a year and—maybe two years old and it is still current. It is something that really needs to be addressed and some of it could probably take legislative changes to—to hold people more accountable.

Mr. NEWHOUSE. Okay. Yes, I would appreciate seeing that.

Mr. KELLY. Yes.

Mr. NEWHOUSE. And if there is something that we should be looking at doing or at least having that conversation, Madam Chairman, it seems like it is incumbent upon members of this committee to do so—

Mr. KELLY. Yes.

Mr. NEWHOUSE. And so—because inevitably we will have more disasters and can—

Mr. KELLY. It is—yes, you can't stop them.

Mr. NEWHOUSE. Yes. And so we need to get better at this. Because, as you say, we are—we have precious taxpayer dollars that we are responsible for, and want to make sure that people that need the help, and that—

Mr. KELLY. Yes.

Mr. NEWHOUSE. The money is used as efficiently as possible.

Mr. KELLY. It averages more than \$10 billion a year that—

Mr. NEWHOUSE. Ten how many?

Mr. KELLY. \$10 billion a year we spend on disasters.

Mr. NEWHOUSE. Billion, 10 billion. Yes.

Mr. KELLY. So it is a sizable investment that we make and it is an investment that we need to make. And I think our citizens and communities deserve to be made whole. But they also—FEMA needs to be held accountable and to make sure that the people that they are giving the money to are—are also held accountable.

Mr. NEWHOUSE. Absolutely. Because that—any money wasted is money that can't go to help the next—

Mr. KELLY. Correct.

Mr. NEWHOUSE. Group of people out of their disaster situation, so. Thank you very much, again. I appreciate you being here today. I yield my time back, Madam Chair.

Ms. ROYBAL-ALLARD. Mr. Aguilar.

Mr. AGUILAR. Thank you, Chairwoman Roybal-Allard.

Mr. Kelly, I wanted to talk with you a little bit about the I.G. issue in a report in November that highlighted some of the management challenges that DHS faces, and specifically mentioned the acquisition program that is—that is high risk. And the report stat-

ed that building the—the planned wall along the Southern Border will highlight continuing challenges that DHS faces in its acquisition program, which frequently incurs cost overruns as a—and as the report stated, quote, contributes little to the mission-related outcomes.

A separate GAO report published last year recommended that DHS analyze costs associated with the barrier segments. And the report concluded that, without key information on cost, acquisition baselines, and the contributions of previous barrier and technology deployments, DHS faces an increases risk that the border wall—end of the quote, that the border wall program will cost more than expected and take longer to build. The report highlighted that DHS agrees with the recommendation.

Based on GAO's findings and your work within the acquisition space, my feeling that key information on the—these programs is missing. How do we know that the budget request that DHS is submitting to us are in line with projections? And based on those reports, it seems like the agency isn't working with the best data, how should Congress respond in your opinion?

Mr. KELLY. Our major management challenge report highlights acquisitions as being a difficult issue. The biggest challenge that the Department has in acquisitions is the components operate often by themselves and it is difficult for the Department to hold those components accountable for—for what they are submitting and actually executing.

The Department does not have—and the entire Federal Government does not have a very good track record of delivering acquisition projects on time or within budget. The types of things that you should be looking for are the performance metrics and the underlying support that is being used to come up with the—with those cost estimates to see if they are going to get things done in a timely fashion.

Mr. AGUILAR. The larger the project, the more risk associated as well, correct?

Mr. KELLY. That is correct.

Mr. AGUILAR. Thank you, I appreciate it.

In your testimony, you also talked about the Essex County Correctional facility issue in New Jersey. And the Fiscal Year 2019 bill that the chairwoman worked incredibly hard on provided over \$400 million in additional humanitarian relief that is supposed to be spent for food for detainees, medical care, infant formula, diapers and those humanitarian expenses.

Looking forward, how can the OIG help us to keep DHS accountable for using these tax dollars in the manner in which Congress prescribed and what are some of the priority areas that we should be looking for?

Mr. KELLY. The continuation of doing unannounced inspections. Unannounced inspections at ICE detention facilities is a very good way to identify deficiencies because they don't know when we are coming. So if we—if they know when we are coming, they can get everything nice and clean or make sure that people are fed, they have got good food.

But if we just show up there unannounced, there is always that element of surprise that a facility needs to be in good shape be-

cause the—the I.G. might be showing up and identifying some significant deficiencies, as the one in Newark and in the one in Adelanto, California, so.—

Mr. AGUILAR. Thank you. Thank you, I appreciate it.

And just building off of what you said earlier, I hope you feel from us you are hearing that you don't just have the authority to come talk with us if you need additional budget dollars to carry out these inspections, but we hope you feel the obligation to do that as well.

Mr. KELLY. I appreciate that support.

Mr. AGUILAR. Yes, thank you.

Building off of what Mr. Price and Ms. Meng mentioned as well, I did want to highlight one article that I will happily send to you—to you and your team. A young man named Hector Baca Gutierrez, who I have met, at the age of 17 came to the United States from Nicaragua. He was given a notice to appear and didn't show up in the 1990s. He adjusted his status in 2001 and—by his father and it was approved in 2018. So he was on his path to become a lawful permanent resident.

He was sent a letter by ERO, by ICE, asked to show up and then when he showed up he was detained for 25 days. No criminal record, hard worker, worked two jobs, husband, father, detained 25 days. So when the department comes to us and asks for authority, and there are cases like this, where individuals who don't have a criminal record are detained it—it frustrates us. And when they are sent letters that seem to lure them come check in with the sole purpose of detaining them it gives us concern.

So I will share that article with you, just building on what my colleagues indicated. Those types of policies I think need to be reviewed. Thank you so much.

Mr. KELLY. Okay. Thank you.

Ms. ROYBAL-ALLARD. Mr. Price.

Mr. PRICE. Mr. Kelly, I want to stay on the subject of ICE enforcement, the policies and practices attendant to that. Again, focusing on what you may have studied or encountered in the course of your particular responsibilities. But I must tell you I do have a prompt. I had a recent occasion in my district—recent occurrence in my district that makes this a matter of special urgency for me.

We, on this subcommittee, I think it is fair to say, have focused over the years on the priority enforcement program and other efforts to prioritize dangerous people for detention and deportation, to make certain that prosecutorial discretion was—which must be exercised one way or the other—to make sure that it is exercised to prioritize dangerous people for removal.

And you know very well that the administration currently has been moving in the opposite direction with—once again, workplace raids, a lot of seemingly random pickups of individuals and the percentage of those who are criminals who are being deported is down.

But we had an example of this in North Carolina in just the last few weeks. The new wrinkle was this though, and this frames my question: ICE justified these raids as the direct result of several counties lawfully ending their engagement in voluntary immigration enforcement agreements with the agency, 287G agreements.

These are voluntary agreements. Multiple Federal courts have ruled that ICE detainers are either voluntary or that they—blanket detainers exceed ICE's own statutory authority. So I have two narrow questions and two broader questions. But it—they are rooted in this recent experience.

First of all, just practices that ICE is bound to honor. What is the responsibility of ICE officials during enforcement actions to identify themselves as Federal immigration officials?

And, secondly, are there internal rules or guidelines that prohibit or discourage ICE officials for traveling in vehicles that say Police on them? Sure it's not the first time you have heard those questions. I would like to clarify what the responsibilities are.

And then two broader questions: Is it department policy, as far as you know, to conduct more enforcement operations in localities that have recently ended 287G programs? Very simple question but an important one.

And then, finally, what about prosecutorial discretion? Is the department focusing any longer on arresting dangerous criminals? President Trump says they are, says it many times. But nearly 1/3 of the individuals taken into custody by ICE in these raids in North Carolina were collateral arrests, wrong place wrong time. And, in fact, there's a quote from the Atlanta ICE Field Office Director, if they are in the wrong place at the wrong time, my officers will take enforcement action.

Is that where we are? Is that ICE policy as far as your observations would confirm it?

Mr. KELLY. I will have to get back to you on that. I don't know a definitive answer. I apologize.

Mr. PRICE. Get back to me on which of the questions?

Mr. KELLY. On—you basically had four questions. I don't know the answers to any of those questions.

Mr. PRICE. Well the two are very narrow questions about what the responsibilities are when raids are being carried out. The question about identifying themselves as Federal immigration officials and using the Police designation—these have been debated for year and—and—you know—as you know, charges have gone back and forth about what the practices are.

You—can you tell us that?

Mr. KELLY. I don't know the answer to your question.

That—whether or not they can or cannot use Police on—

Mr. PRICE. Well that of course doesn't require an investigation. That would be a simple statement of department policy and I would appreciate you getting back to me on this. And then these broader issues, is there or is there not a department policy to target jurisdictions that have recently terminated 287(G) agreements?

Mr. KELLY. I do—we have issued a number of reports on the 287G program. Most of—all of those departments did not paint the department in a positive light. But to—I don't know the definitive answer as to know—as to whether or not they are targeting communities that have terminated those programs.

Mr. PRICE. Well we might need to request a more formal inquiry on that.

Mr. KELLY. Okay.

Mr. PRICE. But to the extent you can respond to these broader issues as well, that question and also the one about how discretion is being exercised.

We obviously would find that information useful and then we can maybe follow up with you as to what kind of specific inquiry to your office we should frame.

Mr. KELLY. Okay. All right, to the best of my knowledge we have not looked into those specific issues. But if we have I will get a definitive answer back to you. If not, we will see what we can do on that.

Mr. PRICE. Yes, thank you. Thank you, Madam Chairman.

Ms. ROYBAL-ALLARD. Mr. Kelly, I have one final question that I would like to add to the record. As you are aware, the Sandy Recovery Improvement Act of 2013 authorized FEMA to establish a pilot program for public assistance alternative procedures. And we understand from FEMA there have been at least 7,800 projects with over \$14 billion in grant funds approved under this pilot program.

The law specifically tasks the Inspector General to look at the effectiveness of the program and focus on six specific areas of interest. In 2018 the OIG issued a brief report with some recommendations but it largely concluded it was too early to evaluate the program's effectiveness.

Do you believe the report that was issued complied with the statutory mandate and, in the near future, do you plan to issue a follow up report that more fully evaluates the effectiveness of the pilot?

Mr. KELLY. The answer to your second question is we are going to be doing an additional work that answers all those questions. To—answer to your first question is: To the best extent possible with the limits of data. We couldn't make a determination as to whether or not—as to the true benefit of the 287G program—I am sorry the 428 alternative procedures program because there were only, I believe, about 10 percent of the projects completed.

A lot of the projects were very multi-year, expensive, complicated projects that are going to take awhile to complete and to make a determination on 10 percent of the projects that were completed would—would not be a sound decision. So we—we have to see what FEMA has completed on some of these more complicated to give a true answer.

As a general rule, the alternative procedures, which is basically a fixed priced type of grant—as a general rule as what the—the Federal acquisition regulations say is that straightforward uncomplicated projects should be done using a fixed price method. More complicated, more sophisticated issues require—are better done if there are cost type of contracting or the type of—or types of grants that FEMA does traditionally.

So for—for the very complicated multi-year issues, the FAR recommends that it is being handled though cost type of contracting, or this would be cost type of grants, so. But for smaller projects fixed priced are much better.

Ms. ROYBAL-ALLARD. Since there are no further questions, the hearing is concluded.

Mr. KELLY. Thank you.

[Material submitted for inclusion in the record follows:]

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE Lucille Roybal-Allard**John V. Kelly, Acting Inspector General****Department of Homeland Security**

Committee on Appropriations

Subcommittee on Homeland Security

DHS Office of the Inspector General

March 6, 2019

Sandy Recovery Improvement Act Review (OIG 18-66)

Background: During the hearing there was a discussion of a report *Sandy Recovery Improvement Act Review (OIG 18-66)*. During the hearing Mr. Kelly acknowledged that this report did not adequately address the specific questions called for in the statute that required this report, section 428 of the Stafford Act, due to limited information available at the time. Mr. Kelly did state that DHS OIG is working on “additional work” to address the questions that Congress asked the IG to report on when section 428 was enacted.

Question: Can you please tell us what additional work DHS OIG is performing to address assessment that Congress required in section 428(h) of the Stafford Act? Will this be in the form of one or more reports? Can you advise when you expect this report or reports to be issued?

Answer: DHS OIG has not conducted any further audit work in this area to date; however, we plan to assess the pilot program again in the future to address the requirements included in Section 428 of the Stafford Act. We will keep the Committee informed as our plans develop with more specificity.

QUESTIONS FOR THE RECORD SUBMITTED BY**THE HONORABLE Grace Meng****John V. Kelly, Acting Inspector General**
Department of Homeland Security
Committee on Appropriations
Subcommittee on Homeland Security
DHS Office of the Inspector General
March 6, 2019**U.S. Customs and Border Protection (“CBP”) Contractor Accenture Federal Services (“Accenture”)**

Background: In November 2017, CBP awarded Accenture Federal Services a \$297 million contract to help meet the demands of recruiting and hiring agents and officers under the President’s January 25, 2017 Executive Order, Border Security and Immigration Enforcement Improvements.

In December 2018, OIG issued a management alert, CBP Needs to Address Serious Performance Issues on the Accenture Hiring Contract, to CBP Commissioner Kevin K. McAleenan on the appalling results that about a year after CBP awarded Accenture a \$297 million contract to hire 7,500 qualified applicants over a five-year period, Accenture processed two accepted job offers. In the first 10 months into the contract, CBP paid Accenture \$13.6 million. Awarding \$13.6 million of taxpayer money to a private contractor to hire two federal employees is simply unacceptable and fiscally irresponsible.

Question: *Does Accenture have other contracts with DHS or any components of DHS? If so, what are they? Is the OIG auditing those contracts? When will those audits be initiated or completed?*

Answer: Yes, as reported on USAspending.gov, Accenture currently has other active contracts with DHS and its components (see the table below for additional details). DHS OIG is not auditing those contracts at this time.

Table: Active Accenture Contracts within DHS

Accenture Client	Contract	Award Value
DHS-wide (Currently used by TSA and USCIS)	<p>DHS Eagle II Contract ID: HSHQDC-14-D-E2005 In May 2014, DHS Information Technology Acquisition Center within DHS's Office of Procurement Operations awarded 68 companies (to include Accenture) contracts under the Eagle II Contract - to provide a full range of Information Technology services, technical management expertise and solutions.</p> <p>Multi-Awards: Contract ID: 70T02018F2FOIA164 (TSA) Obligated Amount - \$17,049,521</p> <p>Contract ID: HSSCCG17J00089 (USCIS) Obligated Amount - \$25,240,970</p> <p>Contract ID: 70T02018F2AOIA015 (TSA) Obligated Amount - \$14,299,414</p> <p>Contract ID: HSTS0316JCIO585 (TSA) Obligated Amount - \$43,960,450</p> <p>Contract ID: 70SBUR18F00000049 (USCIS) Obligated Amount - \$6,701,965</p> <p>Contract ID: 70SBUR18F00000183 (USCIS) Obligated Amount - \$8,504,508</p>	\$22 B
TSA	<p>TSA Hiring Contract ID: HSTS01-16-D-HRM037 Obligated Amount - \$66,039,077</p>	\$290 M

	To assist hiring Transportation Security Officers, Federal Air Marshals, and Field Management, Administrative, and Professional Positions.	
USCIS	USCIS Design and Implementation Services and Project Management Support Contract ID: GS00Q14OADU101 - 70SBUR19F00000103 Obligated Amount - \$956,380 For design and implementation services and project management support.	\$3.5 M
CBP	CBP Data Center Support Services Contract ID: HSBP1017C00137 Obligated Amount - \$92,743,317 For data center support services for the office of information and technology.	\$307 M
CBP	CBP Development and Support for e-SAFE Contract ID: GS00Q16AEA1000-70B04C18F00001129 Obligated Amount - \$1,789,312 For web based software application development and support for Electronic Secured Adjudication Forms Environment (e-SAFE).	\$1.8 M

Source: USAspending.gov

QUESTIONS FOR THE RECORD SUBMITTED BY**THE HONORABLE Debbie Wasserman Schultz****John V. Kelly, Acting Inspector General****Department of Homeland Security**

Committee on Appropriations

Subcommittee on Homeland Security

DHS Office of the Inspector General

March 6, 2019

ICE Detainee Care

Background: In your written testimony, you state that your 2017 audit of ICE detention facilities raised significant concerns about the treatment and care at four of the facilities visited, citing potentially unsafe and unhealthy conditions. While I am gravely concerned about any conditions that may put individuals in the government’s care at risk of harm, I was particularly appalled by the assertion that all detainees entering one facility were strip-searched.

Question:

- 1.) Mr. Kelly, please explain for the Subcommittee what factors led to all detainees entering an ICE facility being strip-searched in violation of ICE’s own protocols?

Answer: In DHS OIG’s December 2017 report, *Concerns about ICE Detainee Treatment and Care at Detention Facilities*, OIG-18-32, we reported that all detainees entering the Santa Ana City Jail were strip searched and the searches were not documented as required. ICE’s 2011 *Performance-Based National Standards* (PBNDS) prohibit routine strip searches unless there is a “reasonable suspicion” based on “specific and articulable facts that would lead a reasonable officer to believe that a specific detainee is in possession of contraband.” Without

documentation, there is no way to ascertain whether these searches were justified or whether they infringed on the privacy and rights of detainees.

We also recently issued a report, *ICE Does Not Fully Use Contracting Tools to Hold Detention Facility Contractors Accountable for Failing to Meet Performance Standards*, OIG-19-18, that found that ICE issued waivers to facilities with deficient conditions, seeking to exempt them from having to comply with certain detention standards. Some of these otherwise applicable standards related to strip searches. ICE had no policies, procedures, guidance documents, or instructions to govern the waiver process, including those waivers related to strip searches. While ICE prepared sample memoranda for Enforcement and Removal Operations Field Office Directors to use to request waivers of strip search-related standards, it did not identify factors to consider in deciding whether to approve the waiver. Instead, ICE just described what the scope of any approved waiver should be.

2.) Are you confident that ICE now has the oversight mechanisms in place to prevent this type of abuse from happening again?

Answer: ICE no longer uses the Santa Ana City jail facility that DHS OIG discussed in our December 2017 report. However, during various subsequent inspections our teams conducted, we found that other jails ICE uses for detention through Inter-governmental Service Agreements (IGSA) do not comply with the 2011 PBNDS standard to not routinely subject detainees to strip searches. When this issue comes up as a deficiency, the jails communicate to ICE that conducting strip searches is their established protocol and they continue to strip search all persons entering the facility, whether they are inmates or detainees. In fact, ICE issued waivers to facilities that would otherwise have to comply with this detention standard or a similar standard under the 2000 *National Detention Standards*. While ICE informed us that it will develop new protocols on waivers and review all current waivers to determine whether they should remain in effect, with an estimated completion date of April 30, 2019, we have not yet received an update on these promised actions. Hence, it is possible that the practice of strip searching all detainees is still in place at some facilities.

Government Shutdown Impact on OIG Audits and National Security

Background: During the recent Trump government shutdown the DHS Office of Inspector General audit teams that perform a critical national security function were furloughed, and thus unable to do their vital work. In a letter to the relevant Committees, you wrote that a portion of the critical work they were unable to perform during the Trump shutdown included:

- A review of TSA's use of canines as a layer of security in airports;
- Reporting on OIG covert testing of access controls to secured airport areas;
- Unannounced inspections of detention facilities operated by ICE and CBP;
- A review of CBP's treatment of asylum seekers at ports of entry; and
- CBP, ICE, TSA, and Secret Service handling of employee allegations of sexual harassment.

Question:

- 1.) Mr. Kelly, does the work of DHS OIG auditors, such as their covert testing efforts at our nation's airports, make our country more secure against a potential terrorist attack?
- 2.) Does the work of DHS OIG auditors, such as their unannounced inspections of detention facilities operated by ICE and CBP, help hold DHS accountable and ensure the Department is acting within the law and internal policy?
- 3.) Mr. Kelly, is it fair then to say that the recent Trump government shutdown had the effect of harming our national security posture and limiting DHS accountability given that

DHS OIG auditors were prevented from doing their jobs during the shutdown?

Answer: Yes, the work of DHS OIG employees helps DHS achieve its important missions and helps ensure that DHS is effective, efficient, and operating within the bounds of applicable law and policy. Anytime there is a lapse in appropriations, it has a negative effect on DHS OIG's oversight work, given that the majority of our staff perform day-to-day duties that are deemed "non-essential" during a shutdown. During the shutdown, DHS OIG leadership was acutely aware that approximately 85 percent of DHS employees in other components were performing exempt and/or excepted functions and remained working, many in high-risk areas where DHS OIG oversight may have been warranted but could not continue due to the furlough of the majority of our staff. During the shutdown, DHS OIG continued to monitor our Hotline for complaints in these areas and would have notified Congress and the Department of any concerns or allegations that presented an imminent threat.

Given the majority of our staff was furloughed during the shutdown, however, our ability to monitor all the risk was significantly hindered. This could be addressed legislatively by allowing offices of Inspectors General to retain a workforce commensurate with that of the departments and agencies they oversee during a shutdown. This would allow Inspectors General to continue essential oversight and keep Congress informed of emerging issues and threats, as well as provide real-time information about how a lapse in appropriations is impacting agency operations.

Audit of Debris Removal Contracts in Monroe County, Florida

Background: Following Hurricane Irma debris removal contracts were entered into by the State of Florida at extraordinarily inflated prices. Specifically, contracts in Monroe County were handed out by state officials that raised significant concerns about potential waste and fraud. I am pleased to see that your work on an audit of those contracts is underway.

Question:

Mr. Kelly, when can we expect the DHS OIG audit of debris removal contracts in the wake of Irma to be completed?

Answer: We expect to publish the audit in the fall of 2019.

Child Separations

Background: In your prepared testimony you describe observations derived from unannounced visits to Customs and Border Protection and ICE facilities between June 26 and June 28, 2018, during the Trump Administration's Zero Tolerance Policy for family separations. You note that DHS was not fully prepared to implement the Zero Tolerance Policy or to deal with certain effects of the policy following implementation. You also note that a lack of a fully integrated Federal immigration information technology systems made it difficult for DHS to reliably track separated parents and children.

Question:

Mr. Kelly, to your knowledge, does DHS know where each of the children separated from their parents during the Zero Tolerance Policy are today? It breaks my heart to ask you this, but are parents still missing their children due to the actions of the Trump Administration?

Answer: DHS is required to transfer unaccompanied children and children separated from their parents to the Department of Health and Human Services (HHS) within 72 hours unless there are "exceptional circumstances." DHS does not track the location of children separated from their parents once they are transferred to HHS. It is HHS' responsibility to keep track of the children after DHS transfers them to a relative other than the parent they entered the country with or to Office of Refugee Resettlement custody.

With respect to DHS efforts to track individuals in its custody, DHS struggled to identify, track, and reunify families separated under Zero Tolerance due to limitations with its information technology systems, including a lack of integration between systems. As we noted in our report “*Initial Observations Regarding Family Separation Issues Under the Zero Tolerance Policy*,” (OIG-18-84), ICE officers reported that when the Zero Tolerance Policy went into effect, ICE’s system did not display data from CBP’s systems that would have indicated whether a detainee had been separated from a child. We since initiated an audit to determine the effectiveness of DHS’ IT systems for tracking detainees and supporting efforts to reunify unaccompanied alien children with separated families. We expect to publish that audit by the end of 2019.

DHS OIG Funding and Workload

Background: A review of the DHS OIG website, shows that your office currently has 125 ongoing projects. These projects range in scope from a review of debris removal contracts in Monroe County, Florida in the wake of hurricane Irma, to unannounced spot inspections of DHS detention facility conditions.

Question:

Mr. Kelly, does the DHS OIG receive sufficient funding from Congress to conduct all of the oversight and investigations necessary to be the watchdog for a Department as large and diverse as DHS?

Answer: We are grateful for the funds that Congress has appropriated to the Office of Inspector General, including the supplemental funding for disaster oversight after the major hurricane and wildfire season of 2017. However, we can always do more oversight with more resources.

The funds that Congress appropriates to the DHS OIG buy mostly people, in the form of salary and personnel benefits. For DHS OIG, more funding equals more people; more people equals more oversight, more OIG reports, and more OIG

reports responsive to congressional requests. In recent years, the majority of our work has been driven by congressional mandates and required disaster oversight. In fact, over the past three fiscal years, this work accounted for approximately 65% of our reports. We are also seeing an increased number of congressional requests. Without adequate funding, our ability to respond to these congressional requests will be limited.

Given that DHS is the third-largest Cabinet agency with a critical and diverse mission, we have the constant challenge of determining whether we are auditing and reviewing the most high-risk areas. By allowing us to do more audits, investigations, inspections, and special reviews, additional funding would help the OIG ensure a more robust and balanced oversight coverage.

Government Shutdown Impact on TSA Screening Procedures

Background: During the recent Trump government shutdown we saw multiple reports of Transportation Security Officers calling out sick because they did not have the funds necessary to work without pay. You referenced these reports in the letter you sent to the relevant Congressional Committees in January. In 2015 it was reported that DHS OIG covert testing revealed that TSA was unable to stop 95% of the prohibited items DHS OIG covert testing teams attempted to get through security check points at airports.

Question:

- 1.) Mr. Kelly, are you familiar with TSA's expedited screening program (Risk Assessment) that allows people not enrolled in PreCheck to receive expedited screening based on age, sex and itinerary?
- 2.) Given that there were reports of sick outs by TSOs but no noticeable impact on wait times at security checkpoints during the Trump government shutdown, have you inquired with TSA

about whether they altered the criteria for expedited screening during the shutdown via the Risk Assessment program?

- 3.) Would you be willing to conduct an audit of how TSA may have manipulated its expedited screening programs during the shutdown?

Answer:

Yes, we are familiar with TSA's Risk Assessment rules that allow those not enrolled in TSA PreCheck to receive expedited screening. Based on our body of work, we believe that TSA's use of risk assessment rules, which grant expedited screening to broad categories of individuals unrelated to an individual assessment, create an unacceptable risk to aviation security. In our 2015 report, *Allegations of Granting Expedited Screening through TSA PreCheck Improperly* (OIG-15-45), we recommended that TSA limit TSA PreCheck screening to known passengers that TSA determines to be members of trusted populations. This recommendation is currently open.

DHS OIG has not asked TSA whether they altered the criteria for expedited screening during the shutdown. We seriously considered taking a closer look at the challenges TSA faced during the shutdown when workers were unpaid and according to news reports, morale was low. We were very concerned about the potential safety vulnerabilities created by a workforce diminished by the sick-out. Ultimately, we did not undertake this review. However, we are always willing to consider a request from Congress to conduct work on this topic.

DHS OIG Transparency in Reporting to Congress

Background: In the wake of Trump's Muslim ban the DHS OIG conducted a review of the implementation of the ban, and the chaos that ensued at airports across the nation. Unfortunately, the Administration deemed aspects of the report confidential, citing executive privilege and the deliberative process.

Question:

- 1.) Mr. Kelly, is the Department of Homeland Security continuing to prevent the DHS OIG from providing information to Congress on the basis of executive privilege and the deliberative process?

Answer: In January 2018, DHS OIG issued our report, *DHS Implementation of Executive Order #13769 "Protecting the Nation From Foreign Terrorist Entry Into the United States"* (January 27, 2017). This report contained redactions made by the Department of Homeland Security pursuant to the deliberative process, attorney work product, and attorney client privileges. At the time that we were having discussions with DHS regarding its possible assertion of the privileges, the DHS OIG was very vocal with Congress with respect to our concerns that the Department would invoke the privileges, thereby shielding information from disclosure to Congress and the public. As we noted at the time, unlike a civil litigant, OIG had no recourse to have a court or other disinterested party determine the issue and we had to instead rely on the good faith of the Department. Other than our experience with this particular report, we have not recently had a situation where we redacted material in a final report due to the Department's assertion of one of these privileges.

- 2.) Will you commit to this Subcommittee that you will do everything in your power to make us aware of your findings regardless of DHS' efforts to prevent you from reporting your findings, whatever they may be?

Answer: The DHS OIG absolutely commits to making Congress and the public aware of our findings and to be transparent in all of our reporting. In cases where information is appropriately redacted from a public report—such as information that is properly classified in the interest of national security—we always provide unredacted versions of the report congressional committees and staff with the requisite clearances. With respect to information that is not specifically protected from disclosure by statute or Executive Order—such as information marked “For Official Use Only” or “Law Enforcement Sensitive”—DHS OIG's policy is to require that the redaction request come directly from the head of the component and articulate the actual, specific harm that would result from public disclosure of the information. The Inspector General or Acting Inspector General then personally reviews each request and weighs the gravity of the potential harm against the importance of releasing the information under the *Inspector General Act*. If the

component head disagrees with the IG's analysis, they may appeal the decision to the Secretary, who is empowered to bar the IG from publishing the information under the procedures set forth in the *Inspector General Act*, Sections 3(a), 8I(a) and 8I(c).

The DHS OIG firmly believes that publishing our reports in full helps us accomplish our mission, provides a valuable service to the public, and accomplishes the intent of Congress. The DHS OIG is only willing to consider redaction requests in specific instances when high-level DHS officials believe that release of specific information will compromise DHS programs and operations. Only in those rare cases do we entertain these redactions. And even in these cases, congressional committees and staff will receive copies of the unredacted report.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE David Price**John V. Kelly, Acting Inspector General****Department of Homeland Security**

Committee on Appropriations

Subcommittee on Homeland Security

DHS Office of the Inspector General

March 6, 2019

MR. SAMUEL OLIVER-BRUNO

Background: On December 20, 2019, I sent a request to DHS OIG regarding the enforcement action taken against Samuel Oliver-Bruno by Immigrations and Customs Enforcement (ICE) agents inside the United States Citizen and Immigration Services (USCIS) office in Morrisville, North Carolina on November 23, 2018. I have requested an investigation to determine whether the actions taken to apprehend Mr. Oliver-Bruno were appropriate and consistent with existing law and Department of Homeland Security (DHS) regulations and guidelines.

Question: When should I expect to hear back from the Department about my request for an investigation?

Answer: A response was sent to your office on April 10, 2019.

Question: Outside of the specifics of the case of Mr. Oliver-Bruno, how are the two components within the Department (ICE and USCIS) sharing information?

- What are the provisions for coordination between ICE and USCIS?
- How does the Department which agency takes precedence?

Answer: The DHS OIG has not completed any audit or evaluation work specific to information sharing and coordination between ICE and USCIS in this context. We are currently considering a systemic review of the communication and coordination

between ICE and USCIS and whether it is consistent with existing law and Departmental regulations and guidelines.

ICE ENFORCEMENT

Background: In North Carolina, there are reports that ICE agents are engaging in deceitful tactics, such as impersonating local law enforcement, to force individuals to disclose their immigration status.

Question: What is the responsibility of ICE officials during enforcement actions to identify themselves as federal immigration officials?

Question: Are there internal guidelines or rules that prohibit or discourage ICE officials from traveling in vehicles that say “Police” on them?

Answer: The DHS OIG has not completed any audit or evaluation work specific to these policies and respectfully refers you to ICE for its response.

287(g) PROGRAMS

Background: ICE has justified a series of recent enforcement actions taken in North Carolina taken as the “direct result” of several counties lawfully ending their engagement in voluntary immigration enforcement agreements with the agency.

Question: Is it Department policy to conduct more enforcement operations in localities that have recently ended 287(g) programs?

Question: Can you quantify, in either total numbers or percentage increases or decreases, your enforcement actions in North Carolina jurisdictions that have recently ended voluntary immigration enforcement collaboration agreements with ICE as compared to before these agreements were ended?

Answer: We respectfully refer you to ICE for its response to this question.

PROSECUTORIAL DISCRETION

Question: How is ICE exercising discretion when it comes to deportation enforcement?

- What are the current guiding criteria in the administrative exercise of discretion?
- What is ICE's order of removal strategy?
- Is every undocumented person a priority for deportation? How does this work with ICE's limited resources?

Answer: The DHS OIG does not have any recently completed audit or evaluation work in this area and respectfully refers you to ICE for its response.

Office of the Inspector General, Department of Homeland Security
Fiscal Year 2020 Questions for the Record
Congressman Pete Aguilar
Subcommittee on Homeland Security
House Committee on Appropriations

Detention Center Compliance

On January 29, 2019, the Office of the Inspector General (OIG) published a report indicating that “ICE fails to consistently include its quality assurance surveillance plan (QASP) in facility contracts.” QASP is critical to ensuring that facilities meet Performance-Based National Detention Standards (PBNDS), which require that detention facilities are safe for detainees and staff. However, QASP was only included in 28 out of 106 detention contracts.

ICE provided waivers to facilities that exhibited deficient conditions and that did not include QASP in their contracts. Between October 1, 2015 and June 30, 2018, ICE imposed only two financial penalties for not meeting standards.

Question: What are examples of deficient conditions found at facilities that did not comply with QASP?

Answer: Examples of deficient conditions have been found during inspections performed by DHS OIG, ICE Office of Detention Oversight, and Nakamoto (ICE contractor), as well as by ICE’s on-site Detention Service Managers, at detention facilities without a QASP. We have not reviewed the entire population of inspection and deficiency reports issued to these facilities. Some examples of deficient conditions from the sample of reports we have evaluated include: strip searching all detainees upon entry to the facility; failure to timely reassess the classification of detainees placed in disciplinary segregation; failure to provide recreation for detainees held in disciplinary segregation; suspension of visitation and telephone privileges for detainees held in disciplinary segregation; failure to maintain detainee medical grievances in detainee medical files; failure to respond timely to detainee grievances; failure to document responses to detainee grievances; automatic cut-off of detainee telephone calls, including legal calls, after 15 minutes; failure to forward detainee requests to the ICE/ERO field office within the required timeframe; failure to audio visually record calculated uses of force; failure of ICE Field Office staff to perform weekly visits to the facility; failure of the detainee handbook to adequately describe the facility’s policies and procedures; opening and inspecting detainee mail outside the detainee’s presence; failing to provide detainees with pillows; and dirt and mildew on the walls and floors of cells and showers.

Question: What policy allows ICE to distribute waivers to facilities with deficient conditions?

Answer: In reviewing ICE’s waiver process, we did not identify any formal policies or procedures that governed that process.

Question: What recommendation do you have to Congress on how to ensure that detention centers achieve compliance with QASP and PBNDS standards?

Answer: In our report on ICE contracting tools, we recommended that ICE develop a process to decide when to seek to include a QASP in existing contracts and IGSAAs that are not subject to a QASP and all future detention contracts and IGSAAs. We also recommended that ICE develop protocols to guide contracting officer's representatives and contracting officers in correcting identified deficiencies and in imposing appropriate financial penalties against detention facility contractors in response to contract noncompliance. As to waivers, we recommended that ICE develop protocols to ensure, among other things, that all existing and future waivers are consistent with contract terms, including those related to detention standards. ICE agreed to implement these recommendations.

Homeland Security Investigations

There are reports that Trump Organization employed undocumented immigrants and that they faced mistreatment while working for the organization. Specifically, more than 30 former employees report incidents of physical abuse and coercion. Additionally, there are allegations that the Trump Organization recruited undocumented workers and helped them acquire fake work authorization forms to work in the US. Despite multiple requests from Members of Congress to Homeland Security Investigations (HSI) to launch an investigation to the Trump Organization's hiring practices, it appears that an investigation has not been initiated.

Question: Does the Office of Investigations plan to look into HSI's decision to not investigate the Trump Organization?

Answer: Given our other work priorities, DHS OIG does not have plans to look into ICE HSI's apparent decision to not investigate the Trump Organization.

Question: Is the OIG aware of a threshold that must be met before HSI can launch an investigation? Does the OIG recommend that a threshold be established to ensure that investigations are determined fairly?

Answer: DHS OIG does not have any recently completed work on this topic; therefore, we do not have the basis to make any related policy recommendations. As part of our ongoing work planning process, we will consider a review of ICE's policies and procedures related to worksite enforcement, which could include the recommendation you suggest if our work supports it. We will keep the Committee informed as to any decisions we make about work in this area.

TOPIC: Border Wall

On November 9, 2018, OIG published a report that highlights major management challenges that DHS faces. The report states that the acquisition program is at high risk of overspending. The report specifically notes that building the planned wall along the southern border will highlight

continuing challenges that DHS faces in its acquisition program management, which frequently incurs cost overruns and as the report states, “contributes little to mission-related outcomes.”

A Government Accountability and Oversight (GAO) report published in July 2018 recommends that DHS analyze costs associated with securing various segments along the southern border. The report concluded that “without key information on cost, acquisition baselines, and the contributions of previous barrier and technology deployments, DHS faces an increased risk” that the border wall project will cost more than projected and take longer to build. The report highlights that DHS agrees with this recommendation. Based on GAO’s findings, key information on the most cost efficient and effective way to build a wall along the southern border is missing.

Question: How do we know that budget requests from DHS to construct a border wall along the southern border are using accurate and reliable data?

Answer: The DHS OIG does not have any completed audit or evaluation work related to the development of budget estimates for construction of the border wall. We do currently have an ongoing audit with the objective of determining the extent to which Customs and Border Protection (CBP) has executed the second phase of the Acquisition Lifecycle Framework, the Analyze/Select phase, for the acquisition of the barrier along the southern border. We plan to issue this audit by the end of 2019.

Question: What policy recommendations does the OIG have to ensure that DHS has access to the most accurate data related to border security at the southern border?

Answer: In February 2017, DHS OIG issued a report, *CBP’s Border Security Efforts—An Analysis of Southwest Border Security Between the Ports of Entry*, that resulted from a review of numerous previously published GAO and OIG reports on border security. The conclusion of our review was that to ensure CBP is continually improving its capabilities and securing the border in an evolving threat environment, it needs to consistently and accurately measure effectiveness and carefully manage its programs and operations. The ability to accurately measure effectiveness requires complete and accurate data. The reports we reviewed identified this as an ongoing issue — data is often unreliable and incomplete and statistics are sometimes subject to misinterpretation. Program management includes building in measures of effectiveness, planning thoughtfully, getting feedback on performance, and carefully acquiring infrastructure and technology. Given CBP’s vast mission and widely dispersed operations, as well as evolving threats, these efforts are herculean, but essential, to ensure the border is secured through responsible use of financial, technological, and human resources. Full transparency and accurate accounting of costs and spending in program planning and operations are also vital to the effort. Without these elements, CBP risks investing in expensive technology and infrastructure that is neither justified nor useful in accomplishing its mission.

TOPIC: Family Separation

The OIG published a report in September 2018 that states DHS did not readily have the technology infrastructure needed to track family separations per President Trump’s zero-

tolerance policy. The report explains that there are interoperability issues between the Office of Refugee and Resettlement (ORR), CBP and ICE. All three agencies have separate information technology systems to keep track of immigrants entering the US. A challenge CBP faced is that the agency did not have a category for “family units” and “unaccompanied children” in their databases records. To address this, CBP created a new category called “deleted families.” DHS attempted to send information about separated families to ORR. However, ORR did not have the “deleted families” category in its database, leaving thousands of records to be inputted manually.

Question: Does OIG have access to all the information technology portals that house information related to undocumented parents and children that were separated?

Answer: The DHS OIG does not have direct access to the various information technology systems used by CBP, ICE, and ORR. Following the release of our September report, we initiated a full-scale audit in October 2018 looking at the effectiveness of DHS’ IT systems for tracking and supporting efforts to reunify unaccompanied alien children with separated families. As part of this audit work, we have obtained full access to all relevant data within each system. This should enable us to fully assess DHS’ tracking of family units and to review the practice of categorizing “deleted families” as a means to unlink family members before sending children to ORR. Our final report, which we expect to publish by the end of 2019, will further detail the technology systems and databases used to record all information on separated parents and children, as well as the accuracy of the data previously reported by DHS.

Question: Does ORR have access to CBP’s information technology base that stores contact information for separated families? If not, is there a team of staff people at CBP that can readily provide that information to ORR quickly?

Answer: As mentioned above, we are currently drafting a report that will further detail the technology systems and processes used to record all information on separated parents and children. This report will also further describe the coordination efforts within DHS and between DHS and HHS. It will also identify specifically which DHS systems ORR can access.

Question: In January 2019, there the Health and Human Services OIG published a report that indicates the total number of children separated from their parents is unknown. When taking this into account, what deficiencies currently exist within each agency’s database?

Answer: As mentioned above, we are currently drafting a report that will further detail the technology systems and processes used to record all information on separated parents and children. This report will describe DHS’ efforts to reach agreement on the total number of children separated and will identify deficiencies that currently exist in DHS systems and processes that hindered family tracking and reunification efforts.

TUESDAY, MARCH 12, 2019.

FEDERAL EMERGENCY MANAGEMENT AGENCY

WITNESSES

PETER T. GAYNOR, ACTING ADMINISTRATOR

Ms. ROYBAL-ALLARD. The Subcommittee on Homeland Security will come to order.

I welcome everyone to the first Department of Homeland Security Subcommittee hearing with the Federal Emergency Management Agency of the 116th Congress. I especially welcome Mr. Gaynor. I believe this is your first hearing as acting administrator, so welcome.

Mr. GAYNOR. Thank you.

Ms. ROYBAL-ALLARD. This subcommittee has a long bipartisan tradition, and emergency management issues are a prime principle as to why. Disasters do not distinguish where they strike by party affiliation, and helping disaster survivors and their communities in the wake of a disaster is a goal we all share.

Most of the members of this subcommittee come from States that are frequently struck by disasters. My home State of California is a prime example. Our State has been struck by catastrophic and deadly wildfires, and now is being affected by rains and floods that can be devastating, especially in the burned areas. We greatly appreciate FEMA's efforts to help disaster survivors and their communities in California.

FEMA has a demanding job. Congress has given FEMA very broad and flexible authority and a difficult mission. We ask FEMA to help people in communities prepare for, respond to, and recover from some of the worst days they will ever face. FEMA employees do this frequently, and with long periods away from home and family. We fully recognize that no matter how many times FEMA does amazing things, it is usually the things that don't go well that get reported in the media and to Members of Congress.

While this subcommittee is very supportive of FEMA, its employees and its mission, that does not abrogate our responsibility for vigorous oversight. During this hearing, as we work with you going forward, we intend to ask tough questions. This is not to make things more difficult, but to ensure we are fully informed as part of our responsibility to see that FEMA carries out its mission in a fast, efficient, and effective manner.

Next month, members of the subcommittee and the Subcommittee on Transportation and Housing and Urban Development will travel to Puerto Rico to see firsthand how recovery efforts are faring. While that will be the focus of our trip, it is not the exclusive focus of this hearing or our oversight activities.

I would be remiss if I did not convey our thoughts and concerns to those impacted by the recent tornadoes in the southeast, especially in Alabama. Mr. Gaynor, I understand you were recently there and that your colleagues at FEMA have been working with State and local partners in response to these disasters. We look forward to your assessment of the situation during this hearing.

Again, thank you for appearing before the subcommittee today. And now I will turn to my colleague, Ranking Member Fleischmann, for his opening marks.

Mr. FLEISCHMANN. Thank you, Madam Chairman. I want to thank you, and let everyone know on both sides of the aisle that, Ms. Roybal-Allard, it has been an honor working with you in your capacity as chairman. I am the ranking member, but we have had several visits so far, and I appreciate the way that things are going so far. Thank you very much.

Ms. ROYBAL-ALLARD. Thank you.

Mr. FLEISCHMANN. Mr. Gaynor, thank you for joining us today. I represent the people of the Third District of Tennessee, Chattanooga all the way up to the Kentucky border. And in my tenure in Congress, FEMA has done an outstanding job in dealing with the disasters. We have had tornadoes, now we are going through floods, but FEMA has always answered the call, and I want to thank you on behalf of my constituents.

Whenever a disaster hits one of our communities, sir, we all hope that FEMA and the first local responders will be on the scene to bring a sense of order and safety to the chaos. And then with the rebuilding, a process that can take months, in some cases even years, we look to FEMA and your partner agencies. We devote a lot of money to recovery and rebuilding, sir, and we expect FEMA to show communities and States the way to get up and running. We expect a lot, the communities expect a lot, but we also expect FEMA to be good stewards of the billions of taxpayer dollars we provide every year. We are looking forward to hear that FEMA did both, effectively and efficiently, help communities out of the worst thing that could have happened, got them back on their feet, and can say to the taxpayers and the Congress, we were good stewards of the funds.

I look forward to your testimony, sir. And I thank you again for being here today.

Madam Chairman, I yield back.

Ms. ROYBAL-ALLARD. Thank you.

Before we begin with the testimony, a few housekeeping items. The order in which members will be called for questioning will be based on seniority of those who are present when the hearing was called to order, alternating between majority and minority members. Also, to ensure everyone has ample opportunity to ask questions, I would ask each member to keep their turn to the allotted 5 minutes per round.

So, Mr. Gaynor, we look forward to your testimony and we will submit the full text of your testimony for the record.

Mr. GAYNOR. Good afternoon. Thank you, Chairwoman Roybal-Allard and Ranking Member Fleischmann and members of the committee. My name is Pete Gaynor, and I am the acting administrator of FEMA. And on behalf of Secretary Nielsen and the admin-

istration, I would like to thank you for this opportunity to provide this committee with an update on the 2018 and 2017 disaster recovery efforts.

The United States experienced six major hurricanes and five historic wildfires across these 2 years. Between January 2017 and December 2018, the President approved 143 major disaster and emergency declarations. Additionally, FEMA supported 202 fire management assistance grants. These two disaster seasons were significant in their devastation of life and property, as well as the cost to the affected communities and taxpayers.

Specifically, in Puerto Rico and the U.S. Virgin Islands, we faced many unique challenges throughout the long-term recovery process. FEMA supports the government's recovery plan and will work to continue with our partners in Puerto Rico, the U.S. Virgin Islands, other Federal agencies, and with Congress to find strategic solutions.

After working closely for several months, I am pleased to announce that FEMA and the government of Puerto Rico came to an agreement last week on the government's financial control plan. The government of Puerto Rico has certified that they have the required fiscal controls, accounting procedures, and project administration in place to assume responsibility to facilitate their financial—disaster recovery.

We have found that success in emergency and response and recovery depends on a response that is locally executed, State-managed, and federally supported. We must work with State and territorial governments to ensure that they are planning and budgeting for emergencies now and building the necessary capability to handle such disasters.

We continue to support recovery efforts from Hurricanes Katrina, Rita, and Wilma nearly 14 years ago. FEMA and our partners recognize that this legacy recovery model is no longer acceptable and fiscally unsound. We will continue to work deliberately and methodically to ensure the outcome of any recoveries is to build a more resilient and prepared Nation.

A cultural shift towards outcome-driven recovery was a recommendation from FEMA's 2017 After-Action Report. We are working hard to meet those findings and make all necessary improvements to our internal processes. This unprecedented scale, rapid succession, and intensity of disaster in recent years has stretched response recovery capabilities across the whole emergency management community, to include our private sector and voluntary partners. It will take unity effort across this community to ensure we are prepared and able to help people before, during, and after disasters.

FEMA helps build capacity through providing preparedness in other grant programs to support our citizens and first responders. Such efforts are critical in allowing States and local governments to focus on small disasters while FEMA focuses on catastrophic disaster response. Eighty percent of all declared disasters incur obligations of \$41 million or less, while 50 percent of all disasters cost less than \$7 million.

Aligned with the key focus areas in the After-Action Report, FEMA's 2018 to 2022 Strategic Plan was published 1 year ago this

week. This plan builds on existing best practices and identifies new initiatives geared towards our mission to achieving three overarching goals: build a culture of preparedness, ready the Nation for catastrophic disasters, and reduce the complexity of FEMA.

As part of our goal of readying the Nation for catastrophic disasters, FEMA took the initiative to update the National Response Framework. This rewrite focuses on the stabilization of critical lifelines in coordination across infrastructure sectors. Lifelines provide an indispensable service that enable key businesses and government functions that, if not properly restored, could risk the health and safety of communities impacted by disasters.

FEMA continues to build a culture of preparedness by focusing on pre-disaster mitigation to build resilient communities. In 2018, Congress took significant steps to support this effort with the passage of the Disaster Recovery Reform Act. This transformational legislation will assist the Nation in reducing risk and increasing preparedness in a more meaningful and tangible way.

Thank you for support in passing this bill. I look forward to our continued partnership and support from this committee, and we will continue to meet the disaster needs of the Nation and ultimately help people in their time of greatest need. So thank you for the opportunity to testify today, and I look forward to any questions you may have.

[The prepared statement of Mr. Gaynor follows:]

71

STATEMENT

OF

PETER T. GAYNOR
ACTING ADMINISTRATOR
FEDERAL EMERGENCY MANAGEMENT AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

“Update on Recovery Efforts for 2017 and 2018 Disasters”

Submitted

By

Federal Emergency Management Agency
500 C Street SW
Washington, D.C. 20472

March 12, 2019

Introduction

Good afternoon, Chairwoman Roybal-Allard, Ranking Member Fleischmann, and Members of the Committee. My name is Peter Gaynor and I am the Acting Administrator of the Federal Emergency Management Agency (FEMA). On behalf of U.S. Department of Homeland Security Secretary Nielsen, I'd like to thank you for the opportunity to discuss the evaluation of federal disaster response and recovery efforts, to include lessons learned from the 2017 and 2018 historic hurricane seasons, and the devastating California wildfires, as well as the ongoing progress made under FEMA's strategic plan.

I am proud to continue to be part of an agency that, every day, helps communities before, during and after disasters. The historic disaster seasons over the last two years were a true test of the Nation's ability to respond to and recover from multiple concurrent disasters.

More than two years later, FEMA remains steadfast in its commitment to support the needs of disaster survivors. We continue to work tirelessly to support state, local, tribal, and territorial (SLTT) partners to respond to and recover from disasters and to mitigate against future disasters. We overcame many challenges, and we have gained invaluable knowledge which we have incorporated into our strategy going forward, but we are not finished. We will continue to adapt and expand our understanding of emergency management to ensure that we can best support our partners' ability to build more resilient communities, lessen the impacts of disasters, and ultimately help individuals get back on their feet quickly.

On February 9, 2018, the President signed into law the Bipartisan Budget Act of 2018. Thanks to the authority that Congress has given to FEMA in this law, FEMA may, in Puerto Rico and the U.S. Virgin Islands, provide Public Assistance funding for critical services to replace or restore the function of a facility or system to industry standards without restrictions based on their pre-disaster condition. The law further allows FEMA to provide assistance for critical services to replace or restore components of the facility or system that are not damaged by the disaster when it is necessary to fully effectuate the replacement or restoration of disaster-damaged components to restore the function of the facility or system to industry standards.

In Puerto Rico, we are facing many unique challenges throughout the long-term recovery process. We continue to work with our partners in the Commonwealth, other federal agencies, and Congress to find joint, outcome-driven solutions to: (1) develop cohesive, solutions-oriented strategies to maximize federal funding while building a more resilient Puerto Rico; (2) build Puerto Rico's capacity to manage the incoming tens of billions of dollars in grant funding; and (3) continue internal controls to ensure appropriate use of taxpayer funding.

Key Themes & Lessons Learned

Hurricanes Harvey, Irma, and Maria caused a combined \$265 billion in damage and were each among the top five costliest hurricanes on record. In response, FEMA coordinated large deployments of federal personnel, both before and after the hurricanes' landfalls, to support response and initial recovery efforts across 270,000 square miles. These deployments included more than 17,000 FEMA and federal Surge Capacity Force personnel, and nearly 17,000 personnel from various offices of the Department of Defense. FEMA facilitated logistics missions that moved more than \$2 billion worth of commodities and supplies across several

states and territories, using multiple modes of transportation. FEMA Urban Search and Rescue Task Forces, comprised of state and local emergency responders, saved or assisted nearly 9,500 lives across the three hurricanes. In total, the hurricanes and California wildfires affected more than 47 million people—nearly 15 percent of the nation’s population. FEMA registered nearly 4.8 million households for assistance.

The unprecedented scale, scope, and impacts of the complex combination of disasters tested the improved capabilities that were developed as a result of lessons learned from Hurricanes Katrina and Sandy.

Following the 2017 and 2018 disasters, FEMA thoroughly reviewed preparations for the immediate response and initial recovery operations with the goal of identifying lessons learned which collectively benefit future operations undertaken by FEMA, the emergency management community, and the nation. Key themes which emerged include:

- **Sustained Whole Community Logistics Operations:** The scale and duration of life-saving and sustainment operations showed that FEMA must be ready to support logistics missions that span weeks or months, particularly in remote locations where commodities and equipment are transported by non-traditional methods. Plans and procedures for resource movement, sequencing and transportation logistics, including the last mile of delivery when requested, must be effectively coordinated and prioritized with the supported state, territory, or tribe, other government agencies, non-profit organizations, and the private sector supply chain.
- **Federally Supported, State Managed, Locally Executed:** FEMA’s ability to provide support in disasters builds on, and is subject to, the capacity of SLTT governments. If these governments are well resourced, well trained, and well organized, the effectiveness of FEMA’s assistance is enhanced. If the SLTT government’s ability to respond—for example, the ability to provide law enforcement, medical support, or commodity distribution—is diminished, then FEMA and its partners must find ways to deliver and support these critical services. FEMA is not traditionally a first response organization but had to play a more direct response role following Hurricane Maria.
- **Staffing for Concurrent, Complex Incidents:** When Hurricane Harvey made landfall in Texas, FEMA had staff deployed to 32 presidentially declared disasters across 19 field offices. By the time Maria made landfall following Harvey and Irma, decisions regarding personnel made in support of one incident impacted ongoing disaster operations. FEMA and our federal government partners rapidly surged and deployed personnel to support immediate response operations. FEMA also relied on mission assignments and the Surge Capacity Force to supplement our existing disaster workforce, pulling resources and personnel from across federal government departments and agencies.
- **Survivable and Redundant Communications:** Following Hurricane Maria, Puerto Rico’s communications infrastructure was so devastated that assessing the needs and the capability of the Commonwealth and its municipalities proved extremely difficult. FEMA provided satellite phones to each of the 78 municipalities in Puerto Rico to gather

information on municipality impacts and critical needs. However, this short-term solution had limited success in addressing overall communications challenges. The private sector played a key role in restoring communications, including cell towers and allowing open roaming services, and remains a critical partner for restoration of communications.

- **Responding during Long-Term Infrastructure Outages:** Too often, we assume the loss of power, communications, and water infrastructure following disasters will be limited in duration. The extreme degradation of critical infrastructure in Puerto Rico and the U.S. Virgin Islands created significant challenges. We need to be prepared for long-term outages of these critical systems, while our SLTT and private sector partners work to mitigate future damages to these vital systems.
- **Disaster Sheltering and Housing:** Providing housing for survivors following the 2017 and 2018 disasters was a challenge, especially when a disaster devastates a community that already had limited affordable housing. Regardless of the readiness of a SLTT government, when dealing with the displacement of tens of thousands of survivors from their homes, there is no easy or one-size-fits-all solution. FEMA has authorities to provide sheltering options including Transitional Sheltering Assistance (TSA) that provides assistance to SLTT governments for survivors to stay in hotel rooms, as well as a program that provides for basic and temporary home repairs to make a home safe to live in while the survivor makes arrangements for more permanent repairs.

Any sheltering option is, by design, a temporary and short-term solution, designed to be a bridge to middle- and longer-term solutions. We have other programs and authorities that assist with housing, including rental assistance, repair assistance, multi-family lease and repair, and manufactured housing units. With all of these options, we partner with our SLTT stakeholders to identify the sheltering and housing solutions that make the most sense for each state, each event, each community, and each survivor.

States have a much better familiarity with the needs of their residents, the local laws and ordinances that can impact some of the FEMA housing options, and are better situated to design and administer to the survivors in their communities. Regardless of the tools we are able to provide, however, permanent housing solutions and full recovery needs are best addressed by insurance. FEMA assistance programs are not designed to return a survivor's home to its pre-disaster condition. As we know, though, there are too many people in our nation that are underinsured or not insured at all.

FEMA's 2018-2022 Strategic Plan

Incorporating the knowledge gained from the 2017 disaster season, FEMA's strategic plan builds on existing best practices and identifies new initiatives geared toward achieving three overarching goals. The three main goals of FEMA's Strategic Plan are to: 1) Build a Culture of Preparedness; 2) Ready the Nation for Catastrophic Disasters; and 3) Reduce the Complexity of FEMA.

Build a Culture of Preparedness

FEMA is just one part of the team. During a disaster, citizens in the impacted communities also become the first responders. Do they know how to shut off water and gas? Do they check on their neighbors? Do they know CPR? Are they financially prepared to deal with the impacts of disasters in their communities, including having the right insurance for the specific threats they face, including flooding, earthquakes, and tornadoes? Do they have some modest level of savings to allow them to miss a few days of work without ending up in financial ruin? We need to empower individuals to help speed the response and recovery efforts.

Developing resilient communities before an incident occurs reduces loss of life and economic disruption. When communities are impacted, they should ensure that they rebuild infrastructure better, tougher, and stronger to protect taxpayer investment and promote economic stability. FEMA is exploring ways to encourage additional investments in mitigation that reduce risk, including pre-disaster mitigation, to help reduce disaster costs at all levels.

While we will never be able to eliminate all risk, we must mitigate the known risks as much as possible. FEMA will work with communities and insurers to close the insurance gap across the nation. Managing risk through insurance, including the National Flood Insurance Program, helps communities to recover faster following disasters and reduces overall costs for taxpayers.

Ready the Nation for Catastrophic Disasters

As this past year has shown, communities must increase their capacity to respond to smaller-scale disasters on a local level. We continue to work with our SLTT partners to increase their capacities to respond to and recover from smaller-scale disasters so FEMA and its federal partners can focus more on readiness and support for catastrophic events.

No level of government can continue to plan, train and exercise for what is easy. We need to prepare for catastrophic events that stress our capabilities. In 2017, FEMA announced our intent to embed FEMA staff within SLTT partner offices to help provide a continuous and more coordinated FEMA presence to improve customer service and provide targeted technical assistance to help build capacity and address capability gaps. The first FEMA Integration Team (FIT) was placed in North Carolina in 2018. Prior to Hurricane Florence, the North Carolina FIT developed an understanding of the state's capabilities, gaps, and processes, and helped to develop and share potential needs. Because of the team's proximity and co-location, the FIT began incident preparations for Hurricane Florence much sooner and with a better understanding of issues, prior to landfall. Currently, FEMA has FITs embedded in 16 states with more to follow.

As part of FEMA's initiative to ready the nation for catastrophic events, FEMA is emphasizing the stabilization of critical lifelines and coordination across critical infrastructure sectors. Lifelines provide indispensable services that enable the continuous operation of critical business and government functions, and that would risk health and safety or national economic security if not promptly restored. Solutions to stabilize lifelines do not fit within a single construct (i.e. an Emergency Support Function [ESF] or Recovery Support Function [RSF]), so we must provide cross-sector coordination to effectively stabilize critical lifelines. For example, the critical lifeline of food, water, and sheltering crosses many agencies, community partners, and ESFs, but must be addressed holistically in order to support a community's

recovery. Focusing on these lifelines and related impacts will allow decision-makers to move rapidly and will allow better utilization of limited resources to target towards the restoration of critical functions.

Reduce the Complexity of FEMA

FEMA is committed to simplifying our processes and putting survivors first. We are looking at ways we can streamline our assistance programs to make FEMA's programs as clear and easy as possible for survivors and grantees to navigate.

Reducing administrative and bureaucratic burdens will allow survivors and communities to receive federal assistance quicker. Throughout the federal government, there are a number of programs that offer assistance to survivors. We are working with our partners to improve some of these activities to ensure survivors can better navigate these various programs. For example, FEMA is consolidating and updating all FEMA Individual Assistance (IA) policies and program guidance to simplify and streamline information about IA programs.

FEMA employees must have transparency and clarity in the processes and resources they deal with. We cannot implement any of these priorities and initiatives without ensuring that they meet the needs of our survivors. We also need to make sure that we continue to capture lessons learned by FEMA and our partners to meet the needs of survivors with disabilities and others with access and functional needs.

These are the priorities and vision of this Agency. As we examine and further develop these initiatives, we will find that some can be accomplished by existing authorities Congress has already provided to us. There will be some challenges that cannot be solved by administrative action alone. As we identify these challenges, we will work with this committee and the rest of Congress to ensure we move forward in close partnership. I look forward to working with you on our shared goal to help people before, during, and after disasters.

Preparing for the 2019 Hurricane Season & Ongoing Initiatives

The 2017 Hurricane Season FEMA After-Action Report (AAR) outlined 18 key findings across five focus areas, and it made recommendations for improvement moving forward. In 2018, Congress took significant steps to help FEMA pursue many of the changes recommended by the AAR when it passed transformational legislation in the Disaster Recovery Reform Act. The law represents the most comprehensive emergency management reform since the Post-Katrina Emergency Management Reform Act, and will meaningfully assist the nation in reducing risks and increasing preparedness.

The 2017 AAR also discussed the need to improve FEMA's ability to respond to catastrophic events while simultaneously building partner response capacity. Eighty percent of all declared disasters are small (meaning total obligations of \$41 million or less); and disasters below \$41 million have cost FEMA, on average, \$100 million total per year in administrative costs over the past 15 years. FEMA's focus needs to be building the capabilities of our partners to manage smaller disasters so that the Agency can improve our capabilities to respond to the larger and potentially catastrophic disasters our nation faces.

As we continue with recovery operations, FEMA is also focused on making sure we are as prepared as possible for this year's hurricane season. Combining the lessons learned from 2017, as well as the goals outlined in FEMA's Strategic Plan, the Agency took immediate actions to prepare for the 2018 hurricane season. These steps will continue to prepare the Agency for the 2019 hurricane season. These steps included:

- **Updating Plans** - FEMA has updated hurricane plans, annexes, and procedures for many states and territories.
- **Maturing the National Response Framework (NRF) & the National Disaster Recovery Framework (NDRF)** – FEMA updated the NRF and NDRF to incorporate community lifelines construct, enhanced coordination with the private sector, and other best practices and lessons learned.
- **Staff Movement Prior to & During Responses** - To improve staffing for incidents, FEMA created Standard Operating Procedures for a Personnel Mobilization Center (PMC), a central location for equipping and training staff prior to disaster deployments. To support the PMC, FEMA is also establishing three permanent PMC core teams in its Field Operations Directorate and training regional personnel on PMC operations.
- **Logistical Improvements** - FEMA made improvements in logistics operations in preparation for the 2018 hurricane season, including increasing disaster stocks and supplies for the Pacific and Caribbean such as meals, water, tarps, sheeting, cots, blankets, infant and toddler kits, durable medical kits, consumable medical kits, and generators. FEMA is also adding 300 new emergency generators to the inventory.
- **National Level Contracts** - FEMA updated high priority national level contracts, including the National Evacuation Contract, Caribbean Transportation Contract, and National Ambulance Contract.
- **Disaster Communications** - FEMA Disaster Emergency Communications is refining tactical and long haul communications, from land mobile radios to satellite communications. We're working to update emergency communications support plans for each state, incorporating best-practices and lessons learned across both the government and private sector based on each state's unique geographic, infrastructure, and operational requirements or risks to provide the nation with an accessible, modern, reliable, and resilient communications infrastructure.

FEMA installed new FEMA National Radio System (FNARS) high power stations on Guam, Saipan, and American Samoa, and refreshed the FNARS high frequency antenna farm at the FEMA Alternate Operations Center to increase resiliency and survivability. FEMA added more than 200 agencies to the list of state, local, territorial, and tribal authorities with access and ability to use the Integrated Public Alert and Warning System (IPAWS) to send emergency alerts and warnings to the public. We also provided technical alert and warning assistance and support to multiple state and local agencies

including for wildfires in California and for hurricanes and volcano in Hawaii, and live public alert tests for the Navaho Nation.

FEMA assisted Puerto Rico Emergency Management Bureau to restore the territory's capability to send alerts and warnings by installing and training staff to use an IPAWS compatible alert origination system, conducting two live tests of the system distributing test messages to the public through radio, television, and cellular phone, and installing a new IPAWS compatible siren system at the Guajataca Dam to warn people below the dam of flood emergencies.

- ***Housing Inspection Process*** - FEMA will modernize housing inspections to improve the survivor experience and streamline the process to lessen the inspection burden for the disaster survivor and better leverage similar efforts across the federal government.
- ***Exercises and Training*** - In May 2018, FEMA sponsored National Level Exercise (NLE) 2018, based on a scenario of a Category 4 hurricane on the mid-Atlantic coast. This exercise brought together more than 12,000 individuals across the whole community to examine the ability of all levels of government, private industry, and non-governmental organizations while testing and validating plans and initial lessons learned from last year. FEMA also coordinated with the Commonwealth of Puerto Rico on a series of workshops, seminars, and functional exercises in June to prepare for this hurricane season.

On October 5, 2018, the President signed the Disaster Recovery Reform Act into law. Key provisions in this law enable greater investment in pre-disaster mitigation; support efforts to reduce risks from future disasters after fires; increase state capacity to manage disaster recovery; and provide greater flexibility to survivors with disabilities. FEMA looks forward to continuing to work with our Federal, SLTT, and private sector partners as we continue to implement this legislation.

Conclusion

The 2017 and 2018 hurricane and wildfire season continue to shape the future of FEMA and emergency management. By utilizing best practices, adopting new response concepts, and training all emergency management partners to the same standards, we can achieve the goals of building a culture of preparedness and readying the nation for catastrophic disasters. Thank you for the opportunity to testify, and I look forward to any questions you may have.

Ms. ROYBAL-ALLARD. Thank you, Mr. Gaynor.

I would like to begin by asking a couple of questions with regards to what is happening in California. It is my understanding that there are several residents in my home State that were impacted by the 2017 Tubbs wildfires who are still not back in their homes and are approaching FEMA's 18-month limit on temporary housing assistance. What is FEMA doing or what can it do to help survivors who have been unable to rebuild within the timeframe allowed by FEMA's Housing Assistance Program?

Mr. GAYNOR. Yes, ma'am. Just as background, I think post-disaster housing for this country is a big problem, and I think it is even more problematic in locations where wildfires occurred and especially in the most recent wildfires in Butte County. I don't think FEMA will ever be able to deliver all the post-disaster housing needs that may be incurred in a disaster, and this is where we need partnership from States and locals to help us deliver that housing disaster requirement.

I spent almost 10 years as a local emergency management director and a State director, and I think the solution is not for the Federal Government to say this is a housing solution that we place upon you, but to have the local and State governments develop their unique housing needs, and we will help meet those needs with Federal support.

So with the specifics of your question, I don't know all the details, but I will find out if there is a hangup in that, and I will be happy to follow up with your staff.

Ms. ROYBAL-ALLARD. Okay. We would appreciate that.

Mr. GAYNOR. Thank you, ma'am.

[Mr. Gaynor responded for the record.]

On March 19, 2019 FEMA approved the State of California's request to extend the period of assistance for Direct Temporary Housing under the Individuals and Households Program for DR-4344, California. The period of assistance for pre-disaster owners is extended to July 10, 2019, and the period of assistance for pre-disaster renters is extended through May 10, 2019.

Ms. ROYBAL-ALLARD. Also, Mr. Gaynor, California, including Los Angeles, has been struck by devastating wildfires over the last 2 years, as we have discussed. Wildfires are sometimes only the first part of a disaster cycle that can later include flooding and mudslides with heavy rainfalls on the burned areas. In fact, I understand from emergency managers back home that there have been recent evacuations in California due to flooding in these previously burned areas.

The recently enacted Disaster Recovery Reform Act provided FEMA additional authority to mitigate these risks. Can you provide an update on the situation in California, steps FEMA and the State are taking to mitigate against the occurrence of future wildfires, floods, and mudslides, and how FEMA's new authority is being used in that regard?

Mr. GAYNOR. Thank you, ma'am. And I think you are referencing the DRRR section about post-disaster or hazard mitigation post-fire. The new authority gives us the ability to add specifically to FMAGs, a post-disaster mitigation. I think what we love about DRRR is it also tags on 6 percent of the total disaster cost for pre-disaster mitigation.

If you looked at the numbers today, I think California will have access, when all the costs are in, to somewhere between \$400 million and a billion dollars of pre-disaster mitigation funds that they could apply across the State to reducing fire risk. I know the State has taken actions over the recent couple months; they have a new fire plan that is really their roadmap about how they are going to attack fire risk. They also passed some laws to improve, the reduction of biomass and trees in the forest to, again, reduce that fire risk.

I think we are all in sync about pre-disaster mitigation. And from our point of view, we would rather invest in pre-disaster mitigation than pay that bill after. It is all tied together with landslides and mudslides. It is management of this risk that is really what is at the heart of this. But I think now with funding from DRRRA, we are in much better shape to address that problem.

Ms. ROYBAL-ALLARD. Okay. And just quickly in the time I have left, I mentioned in my statement what was happening in Alabama, that you had recently visited there. Can you provide an update on what you saw and how FEMA is assisting disaster survivors and their communities?

Mr. GAYNOR. Yes, ma'am. I had the great honor to fly down with the President and the Secretary on Friday. Senator Shelby and Rep. Rogers accompanied us down there. Lee County was impacted by an EF-4 tornado, 170 mile an hour winds. Actually, I had never been to a tornado of that scale ever. And if you can just imagine taking your house, the contents of your house, your clothes, your car, your trees, everything that you own, times 300 of your neighbors and put it all into a blender and then pouring it back out on the Earth, that is what this place looked like. Pretty devastating.

The President signed an emergency major declaration for Lee County, and within a couple hours, we had about 171 FEMA employees down there trying to deliver assistance to those survivors. A very devastating tornado. And that was just one of six or seven tornadoes that touched down between Alabama and Georgia that day or early that week.

Ms. ROYBAL-ALLARD. OK.

Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you, Madam Chairman.

And, again, Administrator Gaynor, congratulations in your appointment. We look forward to working with you, sir.

Acting Administrator Gaynor, as you have probably heard, many counties in Tennessee, my home State, have been hit hard in recent weeks with historic levels of flooding. In some neighborhoods, in Hamilton County, my home county, the flood waters continued to rise as recently as last week. In response, several counties in Tennessee are applying for grants from FEMA to mitigate the impact of this disaster. And our Governor, Bill Lee, is closely evaluating the situation to determine the strain on State resources.

In cases where the governor, working with State and local officials, determines that more help is needed, can you describe the process FEMA utilizes to make a recommendation concerning a Presidential disaster declaration?

Mr. GAYNOR. Yes, sir. And I will just use my experience as a local and State director. What usually happens after disaster, there

is a series of data collection to see what amount of disaster is actually out there. They call them preliminary damage assessments. So it is a team of local, State, and Federal partners going out there to assess damage. From that, the State or the county or the locals will write a request for disaster assistance. The governor and the State's emergency manager will probably evaluate that to see if it stands up to the law and on merit. And then the governor has the discretion to forward that to the President for action.

It comes through the FEMA region, so the FEMA region responsible for Tennessee will look at it and they will forward it to FEMA headquarters. We will evaluate it again, and then ultimately we send it to the President for disposition.

Mr. FLEISCHMANN. Thank you, sir. Is the process more challenging when the damage is more spread out and not concentrated?

Mr. GAYNOR. It is challenging in trying to tally up what is damaged and what is private, what is public, what has insurance, what doesn't have insurance. All those things go into economic factors. So it really depends on the uniqueness of the location, but I am sure the emergency management director in Tennessee has been through this a few times. We offer technical assistance if there is any problems trying to assess the status of their initial assessments.

Mr. FLEISCHMANN. My final question on this part, sir, is are there steps that the agency can take to reduce the holding period and expedite the process, sir?

Mr. GAYNOR. The holding period as in relation to?

Mr. FLEISCHMANN. I guess the holding period in regard to on your all side.

Mr. GAYNOR. It typically doesn't take too long, and I will just use Alabama as an example. I think within a few days the President approved it. So, again, not every disaster is equal. They are all unique in its own way. Some take more because they are more complicated, some are pretty straight forward and gets a little faster.

Mr. FLEISCHMANN. Yes, sir. Mr. Gaynor, last week, this subcommittee heard from the Acting Inspector General, Mr. Kelly, on a number of topics across the department, including FEMA. When I asked the IG what questions we should include in today's hearing with FEMA and the 2017 and 2018 disasters, he did not pause when answering. Ask him to compare their response and recovery rate to other disasters and see if their metrics for Puerto Rico and the Virgin Islands compare favorably to other disasters they have dealt with.

So I ask you, sir, how do your metrics compare to Puerto Rico and the Virgin Islands? And should I assume from Mr. Kelly's response that the numbers were not good?

Mr. GAYNOR. I can't reference if there is a report or some document that Mr. Kelly is talking about. But I can say in what I do know about the scale of Puerto Rico and U.S. Virgin Islands from Hurricane Maria. It is a disaster on a scale that we have really never seen. And it is not your typical disaster, it is complicated. It is obviously on an island. There are lots of thorny issues that predated the disaster that we are trying to work through.

It is one of our biggest risks, I think, for FEMA. We are all in with the government of Puerto Rico and the U.S. Virgin Islands. We have committed a major part of our resources at FEMA to be on the island advising them. So it is at the far end of the scale when it comes to complexity and recovery.

Mr. FLEISCHMANN. Thank you, sir.

Madam Chairman, I will yield back.

Ms. ROYBAL-ALLARD. Mr. Cuellar disappeared.

Mr. Ruppertsberger.

Mr. RUPPERSBERGER. Thank you for being here. And we know you have a very difficult job, and we are just here to help you out and give you oversight and ask you some questions.

So, first thing, I want to talk about, in the last 2 years, the 2017 Atlantic hurricane season I know caused 3,300 fatalities. You know, we had in 2018, the wildfires, and killed a hundred people, and, you know, I know how much time that you spent on that. But I want to talk about—I guess we are getting a little parochial here, but that is who we represent there, and I represent the State of Maryland and the Port of Baltimore. And I have a lot of water in my district also.

But I want to talk to you about the issue of the grant program, which is really important, I think, in my district, Port of Baltimore, and every port, I think, in the Nation. And FEMA's Port Security Grant Program is a lifeline to both large and small seaports across the country. And my—and for this reason, I was discouraged at the administration's deficient funding request at \$36 million for this Federal assistance program.

Now, this program was included in the original Department of Homeland Security authorization, and was funded at \$100 million, was a cut from \$100 million to \$36 million in the recently passed minibus. And this is a clear evidence that Congress recognizes the need to support our ports.

Now, each year, America's ports generate about \$4.6 trillion of revenue and employ over 23 million people throughout the country. And the Port of Baltimore, which I represent, alone generates \$310 million in State, county, and municipal tax revenues, and that is not including all the other amount of moneys that—it is one of the biggest employers in our State and a lot of other States.

Now, with the expansion of the Panama Canal, which are a lot larger ships, you know, coming in, we don't expect to see an increase in containers moving in and out of our country, especially the East Coast. The bottom line is that the economic impact of seaports cannot be understated, and according to the Brookings Center for 21st Century Security and Intelligence, it would only take a small attack on our ports to grind U.S. Congress to halt within days. I think we saw that in the L.A. Port strike years ago. Thus, the need for port security cannot be understated.

So for this reason, I feel strongly that we need to protect our maritime infrastructure. And my question, do you believe the Port Security Grant Program has been a valuable tool in combating terrorism and drugs and building infrastructure resiliency?

Secondly, I can say the Port of Baltimore, which received about \$1.18 million in 2017, they put these Federal dollars to use improving their cybersecurity and upgrading their physical access points.

And, finally, to me, a cut in this program implies the ports have shored up all their vulnerabilities, which they have not. So, basically, the question, you know, what is—do you feel that it is a valuable tool? What is the status? Where are we? And we are going to look at this issue on our committee.

Mr. GAYNOR. Yes, sir. And I am going to go back to my time as a local emergency manager in the city of Providence, we had a port, and I was—

Mr. RUPPERSBERGER. Is that why you talk a little bit differently than—I am teasing.

Mr. GAYNOR. Perfectly fine for me, sir. It sounds perfectly logical.

Mr. RUPPERSBERGER. Boston. Boston-type.

Mr. GAYNOR. I was a recipient of port grants, and I know how important those can be to any port. I think if you go back to 9/11 and draw a line on non-disaster grants, especially in Homeland Security grants, there has been a steady decline in funding over those years. I do think that the port grant is a valuable tool to all ports.

There is a great demand on Homeland Security grants. Ports are one of those risks in a big portfolio. I was not part of determining how much each grant got, really above my pay grade, but it is an important tool for States and local ports to buy down their risk and be more resilient.

I will be happy to look into the status of the current grant year, where we are on that. And it is a competitive grant, so the better program that you put forth, the better results you will yield on the far end.

Mr. RUPPERSBERGER. Okay. And we know, you know, the drug issue we have now, I think the majority of our ports, a lot of the fentanyl from China is coming in through the ports. And you know how many people are dying every day in our country, hundreds and hundreds. Thank you.

Mr. GAYNOR. I will be happy to follow up on the number.

[Mr. GAYNOR responded for the record.]

Yes, the Port Security Grant Program (PSGP) has been a valuable tool in reducing security risks and increasing the resilience of the Nation's seaports. Since 2005, DHS has awarded more than \$2.7 billion through the PSGP to port authorities, facility operators, and state and local government agencies that are required to provide port security services. This funding has been directed toward the implementation of Area Maritime Security Plans, Facility security Plans, Vessel Security Plans, and Port-Wide Risk Management Plans as a means of addressing identified vulnerabilities.

In fiscal year 2018—the most recent awards under PSGP—recipients within the Baltimore port area received a total of \$2,749,948 in funding. The FY 2019 PSGP was funded at \$100 million, the same amount appropriated for the program in FY 2018. The FY 2019 PSGP application period opened on April 12, 2019. Applications are due by May 29, 2019 and final awards and allocations are expected in early August 2019.

Mr. RUPPERSBERGER. Thank you. Okay. Good. Appreciate it.

Ms. ROYBAL-ALLARD. Mr. Newhouse.

Mr. RUTHERFORD. He is gone.

Ms. ROYBAL-ALLARD. Mr. Rutherford.

Mr. RUTHERFORD. Thank you, Madam Chair.

I would like to talk a little bit about the Federal contracting regulations versus State and local. And just to give you an idea of some of the problems that that has created, including the reimbursement procedure, obviously.

Keys Energy in southern Florida still has a \$42 million FEMA filing from Hurricane Irma. However, Key Energy to date—and FEMA’s released \$15 million to the State so far, yet Key has only received \$1 million of the \$42 million that they are owed. And in the meantime, they have to take out loans to make up for those costs, and now they are paying interest on those loans and the—so the storm is still getting more expensive every day, to the tune of \$2,400 every day it is costing Key Energy.

And so my question is, is there any way we can break this logjam where FEMA gives money to the State, who is then supposed to disburse it to the locals, those with the loss? Yet oftentimes what comes back is FEMA says, well, your contract doesn’t fit our regulations exactly, so you have to, you know, redraft all these contracts. Well, they fit the State and local contracts regulations when they were drafted.

Is there some way we can agree that if they have—if they have met the State and local requirements, that they have met Federal requirements?

Mr. GAYNOR. Congressman, I don’t know the particulars about this exact issue, but, in general, if you receive Federal money, you have to follow Federal purchasing guidelines. I mean, that is in the statute. We encourage recipients of all types of grants, whether it is disaster grants or non-disaster grants, to make sure they follow the rules when they use that money. We pay particular attention to not only following the rules, but documenting along the way what you did to make sure that the State can reimburse you. So this is all by reimbursement.

If the State contracted Key Energy to do something, the contract is between the State and Key, and the first response is to make sure that the paperwork and the contract and all the things are right. We will reimburse them based on the document they submit. We take a hard look at it because we are concerned about waste, fraud, and abuse, and if there is some irregularity, it may get kicked back. But I would be happy to look into the details of this. I mean, I just don’t know them.

[Mr. Gaynor responded for the record:]

There are 10 Project Worksheets for the Key West Utilities Board for Hurricane Irma (DR-4337). The status of each project, as of April 5, 2019, is provided below (for exact payments that have been made through the state to the utilities board, please contact the Florida Department of Emergency Management).

Mr. RUTHERFORD. Why are these contracts that are—you know, why can’t they be accepted, number one?

But let me ask you another question too, because another issue that we have is, you know, these cities—for debris removal particularly. They enter into a contract with a provider for that removal, and so, you know, they give a pretty good price, you know, per ton of debris. Yet when the storm hits, they get a price from somebody in south Florida for twice as much as that contract. They pull all their people out of that contract area and they go south or wherever that other location is and make twice the money. Somehow we need FEMA to help us hold these people accountable for the contracts that they have.

Do you have any recommendations on how we might be able to address that issue?

Mr. GAYNOR. Yes, sir. There is a lot of money in debris, and the bigger the disaster, the more money there is, and it can be pretty competitive. There is not many major debris contractors around the country that can perform large-scale missions, and so they probably look for the top dollar.

We advocate for State and locals to have pre-disaster contracts with some of these vendors or service providers—

Mr. RUTHERFORD. The contracts are worthless, though, because they leave you and go elsewhere.

Mr. GAYNOR. I am not sure what we can do about that. I am just saying the best practice is, we are trying to convince and encourage State directors and local directors to have these pre-disaster contracts. Better to have a contract than to have no contract at all. I would rather be on their list than not on their list.

Mr. RUTHERFORD. Maybe they can't get FEMA dollars if they violate a contract. That would be a great idea.

And let me close with this real quick, because I know my time is running out. On your sustained whole community logistics operation, I know that for Irma, there was an amazing amount of prepositioning of goods for Puerto Rico and the Virgin Islands and Jacksonville, particularly. Mike Crowley and TOTE, two of our Jones Act maritime vessels. That worked exceptionally well when—as soon as the port opened, those goods and services were pouring into Puerto Rico there in San Juan. The problem was distribution throughout the country, you know, because of roads and bridges.

Was FEMA actually part of that staging or did they do that on their own?

Mr. GAYNOR. I can't speak to the exact specifics of that storm. I will tell you what we have, we have a very robust logistics capability within FEMA. Food, water, generators, tarps, you name it, we have it.

Mr. RUTHERFORD. It was very impressive. If you guys were part of it, I don't know.

Mr. GAYNOR. I would like to think that we were a part of it. And, again, I will go back to my local and State director hat. The hardest part to getting those whether it is a bottle of water or an MRE, into a hand of a survivor, is that last mile. That is the hardest part.

Mr. RUTHERFORD. That is the hardest part.

Mr. GAYNOR. And we are built on locally executed, State-managed and federally supported. So if the local is broken and the State is broken, it comes to us.

Mr. RUTHERFORD. Thank you. My time has expired.

I yield back.

Ms. ROYBAL-ALLARD. Mr. Price.

Mr. PRICE. Thank you, Madam Chairman.

Welcome, Administrator. I come from a State that has had many disasters in recent years, and we are having recovery—we are undertaking recovery efforts now and appreciate FEMA's cooperation. It has been a good relationship, and we, of course, want it to continue.

And one question that has arisen, I want to raise specifically with you today, which has to do with the STEP program. That is a funded—that is a program funded jointly by the State and

FEMA, and what it is aimed at is residents who might, with some temporary repairs, continue to live in their homes while the longer term repairs are being made. That is a good idea for them. It keeps them in the community, it keeps them able to work and so on, and it also saves the government money in resources, not having to put people in congregate shelters and hotel rooms and other disaster housing.

Now, I know FEMA hasn't standardized the STEP program across the States, and so there is a certain lack of predicability that makes the program difficult to administer for emergency management officials. At least that has been the experience in our State. For example, we were denied a recent extension request, and given an April 22, 2019, deadline to complete STEP repairs on between 3,000 and 4,000 homes, mind you, hit by Hurricanes Florence and Michael last fall.

I am sure you know, Hurricane Florence was the Nation's second wettest storm in 70 years. It killed 31 people. It caused an estimated \$17 billion in damage. Our emergency officials, believe me, are making good progress, good progress on the STEP program. But the sheer magnitude of the hurricanes that hit our State have to be considered, or at least we think they should be considered. So I will ask you a couple of questions in light of this experience.

First, can you explain your process for determining the length of time States have to implement their STEP program? And, secondly, what factors do you consider when a State needs an extension or applies for one?

Mr. GAYNOR. Yes, sir. Thank you for the question. This goes back, I think, to the original housing question. Post-disaster housing is a problem. It would be our preference to keep people in their homes, and I think that is why we created the STEP program. It is relatively new. We are using it in Puerto Rico and U.S. Virgin Islands to great success.

On this very issue, I talked to Governor Cooper last week about this extension, and I heard him loud and clear about why he needs it. And so we are going to reevaluate the program. Typically, it runs 180 days. We are going to look at it again and, hopefully, we will resolve it to everyone's satisfaction.

Mr. PRICE. Good. I appreciate that.

Is there anything in the interim? Maybe I should just take that as a good answer and leave it at that.

What are the questions you are dealing with here as you consider how to deal with extension requests?

Mr. GAYNOR. Again, I think each disaster is uniquely different. Some jurisdictions are more capable than others. Weather gets in the way of repairs. I think we are experiencing this out in USVI and Puerto Rico. Weather gets in the way of repairs, and it is out of the applicant's control, so we take all that into consideration. We are trying to assess our risk, making sure that we spend the money correctly within the statute that directs it. All of this goes into making, hopefully, a good, reasonable decision that benefits both parties.

Mr. PRICE. Thank you. Thank you. That sounds like a good approach.

Secondly, I want to ask you about the Disaster Recovery Reform Act of 2019. I was pleased when the Congress passed the Disaster Recovery Reform Act last year, the first comprehensive emergency management reform package since Hurricane Katrina. The law included a number of reforms. That should be very helpful to North Carolina and other States hit by disasters, especially some of the changes made to the Hazard Mitigation Grant Program. The DRRRA established new rates for program—for the program and expanded the definition of allowable management costs, and that is what I want to focus on.

Can you please tell me when FEMA will release the new management cost guidance? And I also understand FEMA is working to implement this policy with a goal of having a system to allow States to submit applications for management costs by early 2019. Can you please share a timeframe for when you expect to have the grant management system fully functional?

Mr. GAYNOR. Yes, sir. Like I said in my opening statement, we believe DRRRA is transformational. And building a more resilient Nation, I think the hazard mitigation 6 percent based on a disaster is going to be groundbreaking to actually invest those dollars pre-disaster. When it comes to management costs, we are trying to work through the 49 unique sections in that act. We actually had a meeting a couple weeks ago with congressional staffers on our progress. I would like to think we are making great progress on many of the sessions.

I don't know the exact status of the management cost section, but I would be happy to follow up with you on that on where we are. But overall, I think we are in a positive trend to get some of those DRRRA sections on the street and implemented.

Mr. PRICE. Let me just say, Madam Chairman, just to respond, that we would appreciate that material on those timeframes. That will be very helpful.

[Mr. Gaynor responded for the record:]

FEMA published interim guidance in November 2018 implementing DRRRA 1215. Interim guidance and supporting documentation for the Public Assistance and Hazard Mitigation Grant Programs can be found on FEMA's website, at <https://www.fema.gov/media-library/assets/documents/174133>.

Hazard Mitigation Grant Program (HMGP)

The HMGP Management Costs Interim Policy was published in November 2018 implementing DRRRA 1215. The Interim Policy applies retroactively to major disaster declarations on or after August 1, 2017. On February 28, 2019, FEMA deployed system updates to allow application submissions for management costs.

The Interim Policy provides greater flexibility to state, tribal, territorial, and local governments. Specific changes include:

- A revised definition of management costs to include indirect costs and direct administrative costs.
- Revision of the maximum management costs rate of up to 15%, including up to 10% for the Recipient and up to 5% for the Subrecipient.
- Elimination of the \$20 million cap.

FEMA will evaluate this interim policy as it is implemented and will incorporate management costs into the next version of the Hazard Mitigation Assistance Guidance (2015).

Further, job aids and training development/delivery are underway. Currently, FEMA is evaluating the need for developing a reasonable cost policy for HMGP.

Public Assistance Grant Program (PA Program)

The PA Management Costs Interim Policy was published in November 2018 implementing DRRRA 1215, and additional supporting documentation and resources were published in early 2019. The Interim Policy applies retroactively to incidents declared on or after August 1, 2017. Recipients and Subrecipients with incidents de-

clared from August 1, 2017, to October 4, 2018, may choose between using the Interim Policy or continuing to use existing FEMA regulations and policies related to management costs. The Interim Policy provided recipients and subrecipients until March 15, 2019, to notify the Agency of their selected option. The deadline was extended to April 15, 2019, for Puerto Rico emergency and disaster declarations for Hurricanes Irma and Maria.

The Interim Policy provides greater flexibility to state, tribal, territorial, and local governments. Specific changes include:

- A revised definition of management costs to include indirect costs and direct administrative, costs.
- Revision of the maximum management costs rate of up to 12%, including up to 7% for the Recipient and up to 5% for the Subrecipient.
- Elimination of the \$20 million cap.
- Elimination of lock-in amounts and the associated process for determining the lock-in amount.

Further, a Standard Operating Procedure and fact sheet on the Interim Policy were issued on February 11, 2019, and job aids, system changes, and training development/delivery are underway. Currently, FEMA is evaluating the need for developing additional reasonable cost guidance. In the interim, FEMA will continue to apply the current reasonable cost job aid for PA projects until a working group can analyze and recommend more holistic, fulsome guidance.

Ms. ROYBAL-ALLARD. Mr. Palazzo.

Mr. PALAZZO. Thank you, Madam Chairman.

Thank you, Mr. Gaynor, for being here today. And I agree, you started off saying sometimes it is the local and State solutions are the best fit for communities, because all States and communities are different, and you know, those are the professionals on the ground, and, you know, and one size doesn't always fit all, especially if it is coming from this city.

I would like to first start out by thanking you for the 12 storm shelters that FEMA has provided to Forrest County in the State of Mississippi. You know, we attract tornadoes, hurricanes, ice storms. You name it, we get it. And I want to thank FEMA, especially the Hazard Mitigation Program Grant for that. I know the supervisors and the community are especially appreciative of that, because if we can save one life, it is really much worth it.

I would like to shift to something. In about 60 days, NFIP is going to expire again. And I don't know how many times it has expired since we reauthorized it. I know in 2013, the Biggert-Waters Act was introduced, and soon thereafter, when communities all across the Nation started to realize that their rates were not only just going to go up \$25, \$30, but thousands, and in some cases, tens of thousands of dollars on, you know, the homeowners flood insurance policies, we kind of stepped in and realized that—in fact, the author of the bill, Congresswoman Waters, said the unintended consequence were these drastic rate increases.

I am continuously nervous about if any reforms that we make to the flood insurance program, that we get it wrong again. And, you know, if people don't—if they have a mortgage and they are required to have flood insurance and they can no longer afford the flood insurance, that home can be deemed insecure, and the banks are therefore forced to basically begin taking back that property to protect their asset.

I do think there are reforms that can be made to the NFIP program, but, you know, this is a program that Congress created in 1968, and, you know, I am concerned that, you know, when you are messing with people's largest single investment, which is their

home, we got to be very cautious, we got to be very studious on how we approach this.

And I do appreciate what we have done, some of the past actions, some of the reforms weren't good. I know we are trying to inject the private market. At the same time, we are tossing out terms like we need to make the program actuarially sound. Well, that all sounds well and good, but we also got to protect our homeowners. And we do have a homeowners protection caucus that was created as a result of Biggert-Waters, I am one of the co-chairs.

And I would like to ask you, are you seeing, as the efforts of privatization—the private market enter into the flood insurance market, is that taking place? And, if so, what do we do to prevent private companies from cherry-picking, taking the most safe policies and undercutting the government NFIP rate, and then leaving all the more unsafe properties in a reduced premium pool with probably higher and more increased in rates? That is just a concern of mine, and that was a concern of many of my colleagues when we made—we killed the last NFIP reform bill.

Mr. GAYNOR. All great questions, Congressman. First, at FEMA, we believe an insured home is a valuable home. To answer your first question how many extensions has NFIP had, 42. It is time for some reform, we believe that. This past year or these past 2 years, we added about 200,000 new policies.

I think part of the issue with NFIP is when it comes to giving insurance policies, we are the only insurer in those locations; there is no other insurers to divide that risk up into. So when there is a disaster that requires NFIP, it really hits hard.

Now, 1 inch of water in a home is \$25,000 worth of damage. FEMA gives individual assistance or you can get up to \$35,000 of assistance if you meet all the different wickets. On average, we only give out about \$2,600. But if you look at insurance, what we have given out for the same kind of damage, you get \$109,000. So, we would rather have insured homes, because, first of all, insurance pays first, but it is better for everyone.

FEMA will not make you whole. FEMA is a bridge to get you to the next, safe, warm, and dry location, but we are not going to make you whole. So insurance is infinitely important for us.

Last—in 2017, we bought reinsurance for NFIP, and we saved the taxpayers a billion dollars. And I think we are going to try to do that again. So we are all in on making sure we try to rethink flood insurance, because it rains in every State, right? It floods in every State. Look at Houston, it flooded where, it had never flooded before. So, again, an insured home is a valuable home.

Mr. PALAZZO. And we have seen this in a lot of the storm events over the past several years, Madam Chairwoman, where, you know, the rivers never flooded out the communities; it just seems to be happening more and more, and that is why perhaps in the second round of questions I will ask you about all perils insurance as well.

Ms. ROYBAL-ALLARD. Ms. Meng.

Ms. MENG. Thank you, Madam Chairwoman.

And thank you, Administrator, for being here today. I wanted to ask about language access issues during and after a disaster. Language access has often been an issue for limited English-proficient

individuals, including and especially those of the Asian American and Pacific Islander communities.

As evident from Hurricane Katrina, FEMA wasn't equipped to communicate with the Vietnamese American community then in New Orleans. When Hurricane Harvey hit, an API organization such as API Vote had to step in to translate information that FEMA officials were releasing because it was only available in English and Spanish.

Hurricane Katrina occurred in 2005, Harvey in 2017, which is about 12 years. What had FEMA done in between to improve language access since Katrina?

Mr. GAYNOR. Ma'am, I think we recognize that making sure we get our message out to the entire community is important. I can't speak to the specifics of what we have done to improve that. I will get back to you on that. But I will just use an example; if the U.S. military can have a piece of technology in their hand to translate, it would seem that we could do the same thing for meeting survivors in a disaster area. But I would be happy to get you some information about our strides in that and what we are doing and maybe what we plan to do.

[Mr. Gaynor responded for the record.]

FEMA ensures all applicants receive critical, accessible, and understandable preparedness and disaster assistance communications, regardless of language proficiency. To best assist all survivors, FEMA provides the following:

- Disaster information in languages identified through demographic analysis of the impacted area;
- FEMA continuously works with the 12 languages as identified by the Post Katrina Emergency Management Reform Act (PKEMRA), but life-saving information in plain language to the public, including printed materials can be translated into more than 200 languages, Braille and large print. Video products that are produced includes captioning (multilingual), American Sign Language (ASL) and audio description and accessible on FEMA's website.
- Staff to identify language needs and connect disaster survivors to applicable translation services;
- Video Remote Interpreting for American Sign Language or on-site translation at Disaster Recovery Centers;
- Appropriate referrals for applicants with disabilities and others with access and functional needs who also have Limited English Proficiency.
- FEMA's Community Partners Branch in Intergovernmental Affairs works with over 100 organizations whose constituencies include diverse populations who require products and materials in various languages. These partnerships help FEMA further increase our distribution of preparedness materials in multiple languages and utilize their relationships with these populations and increase preparedness in these communities. Preparedness publications in seven top tribal languages have been produced and will be posted on fema.gov this summer.
- FEMA has also increased the availability and visibility of preparedness brand, materials, and messages through its Ready.gov and Listo.gov (Spanish-version of Ready.gov) pages. Preparedness information and materials are also readily available in more than 10 other languages besides English and Spanish.
- We are striving to increase accessibility even more. In 2018, FEMA provided translations in 18 languages and delivered more than 700 translated documents in support of requests across various disasters.
- During the last two years, FEMA staff has worked to include an American Sign Language interpreter on several pre-scripted videos to update the video library and FEMA's YouTube page.
- The Ready Campaign partnered with USFA to leverage their pictogram contract to develop hurricane preparedness materials in a pictogram format, and will continue to look for opportunities to expand this capability further in meaningful ways.

- Additionally, the FEMA Puerto Rico Facebook page routinely posts preparedness information in Spanish for not only Puerto Rico, but all Spanish-speaking audiences. This included a major 2018 hurricane awareness campaign.

Ms. MENG. Okay. Yes, I would love to work with you to make sure that we are working with organizations around the country and to help you and FEMA do as good a job as possible.

My other question is, there were reports in the media that following President Trump's public declaration, he wanted no more disaster funds going to Puerto Rico, and that administration officials started telling agencies, HUD specifically at the time, to block money appropriated by Congress for Puerto Rico.

Do you have any direct or indirect knowledge of any actions taken by the Trump administration to block disaster recovery money from going to Puerto Rico?

Mr. GAYNOR. Ma'am, what I do know is that the approved disaster money through disaster process is how we deliver services to those impacted. Other conversations with HUD, I am not familiar with. But we have money appropriated through the process and we are using that to deliver the best disaster relief to our survivors.

Ms. MENG. So as far as you are concerned, you don't have any knowledge of those actions taken by the Trump administration?

Mr. GAYNOR. I do not.

Ms. MENG. Do you or your team staff have any knowledge of any communications made with the Trump administration on the same topic?

Mr. GAYNOR. I do not, ma'am.

Ms. MENG. Okay. Thank you. And then back to—sorry. So I know that in July, FEMA issued an After-Action Report assessing its response to the 2017 storm season. This report included recommendations to address staffing needs, increase FEMA readiness stocks outside the continental U.S., et cetera. What actions has FEMA taken to meet these recommendations?

Mr. GAYNOR. When it comes to what we call the CAD or the Caribbean Area Division, which is how we manage Puerto Rico and the U.S. Virgin Islands, we have done significant work to make sure that we have commodities on island. Between the islands of Puerto Rico and the U.S. Virgin Islands, we now have eight warehouses for commodities on island, and more commodities stateside that we can tap into.

So we are trying to learn our lessons from Maria and making sure that we don't repeat that again. But we have taken significant steps to improve our commodities.

Ms. MENG. And that would help get supplies out to people around an island more efficiently than had happened after Maria?

Mr. GAYNOR. That would be the theory. Again, I think the hardest part for a local emergency manager and State emergency manager is that last mile; you can have it, but you have to transport it or you have to get it in the hands of the survivors. So the last mile is the hardest mile. But there are adequate resources and commodities on the islands for a disaster.

Ms. MENG. Thank you. I yield back.

Ms. ROYBAL-ALLARD. Ms. Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. Thank you, Madam Chair.

I have a quick question that is more locally focused. According to NOAA, Hurricane Irma was the strongest hurricane ever observed in the open Atlantic Ocean. After barreling through Florida, 6½ million customers in my State were left without power, and the winds, rain, and flooding left a trail of destruction and debris.

Memorial Healthcare System, a safety net provider which operates six hospitals in south Florida, including a level one trauma center which is headquartered in my district, cleaned up the mess around its facilities, spent money on clearing road debris, extra labor and mitigation. However, 15 months after their initial application with FEMA for the total reimbursement request of approximately \$7 million, Memorial Healthcare has received not \$1.

Mr. Gaynor, you discussed in your testimony the actions that FEMA is taking to consolidate and update your individual assistance policies, but what is FEMA doing to simplify and streamline the process for reimbursements for emergency healthcare providers like Memorial? Because 15 months is far too long, far longer than is reasonable to expect them to have to wait.

Mr. GAYNOR. Yes, ma'am. Again, I don't have the exact details of the Memorial Health issue. I would be happy to look into that and see why it is taking so long. Again, I will just go back to each disaster is very unique and—

Ms. WASSERMAN SCHULTZ. My question specifically is what is FEMA doing to simplify and streamline the process for reimbursements for emergency healthcare providers like Memorial? I certainly am familiar with the complexity of dealing with the aftermath of a storm, since I live in south Florida.

Mr. GAYNOR. Yes, ma'am. We have implemented the grants management system. It is—or I should say, part of the new public assistance delivery to better account for paperwork, track reimbursements, and make sure that the paperwork is all correct before we go down a long road and decide that something is missing early on in the process and have to go back again and back again. I think this is part of the frustration with locals and States that we get to the end and we realize that something is missing. This new PA policy project and GMM will track these initiatives to make sure that we try to speed it up as fast as we can.

Again, it can be complicated in certain circumstances, but our goal is to deliver the fastest relief to our survivors.

Ms. WASSERMAN SCHULTZ. I will be honest with you, your response doesn't really give me a lot of confidence that you have got a system in place that is headed towards improving the situation.

FEMA was plagued with contracting problems following the 2017 disaster season. In October 2017, FEMA terminated a contract after just 20 days with Tribute Contracting, which was supposed to deliver 30 million meals in Puerto Rico. The contract was reportedly worth \$156 million dollars. Tribute delivered only 50,000 of the 30 million meals it was supposed to. According to media reports, Tribute was a single-employee business with no large-scale disaster contracting experience, and had already been barred from contracts with the Government Publishing Office when FEMA entered into its contract with the company.

Similarly, FEMA had to cancel a \$30 million contract for tarps or plastic sheeting when a newly formed company called Bronze Star failed to deliver the urgently needed supplies.

Mr. Gaynor, in the aftermath of these failed contracts for supplies that can mean life or death for disaster survivors, what steps has FEMA taken to make certain that it only contracts for goods and services with companies that actually have the capacity to perform? And do you look to see if a company has been deemed ineligible for contracts with other government agencies before you contract with them?

Mr. GAYNOR. Ma'am, so to your point about the contracts, we executed for Maria approximately 2,000 contracts. Of those 2,000 contracts, three of those contracts failed to work and we just cut them off at no expense to the Federal Government. The Tribute contract, they supplied, I am going to say, 50,000 meals at about a quarter million dollars. We got the food, we paid them, and then we ended the contract.

Ms. WASSERMAN SCHULTZ. OK. But what are you doing to make sure that mistakes—grave, gross mistakes like that don't happen again?

Mr. GAYNOR. So we have increased our cap on contracts to make sure we have more capacity among the contracts that we do have. And we have plenty of commodity contracts available. So if one—

Ms. WASSERMAN SCHULTZ. Okay. I am sorry. Before my time expires, I just have one more. Following Hurricane Irma, then Florida Governor Rick Scott's office overrode pre-negotiated debris removal contracts and entered into debris removal contracts at extraordinarily inflated prices. Specifically, Governor Scott's office signed contracts in Monroe County that raised significant concerns about potential waste and fraud.

What consequences are there—piggybacking on what Congressman Rutherford asked you, what consequences are for this kind of waste, fraud, and abuse practices? I mean, it doesn't make—your response, frankly, to his question doesn't make any sense to me. You throw up your hands and you just say there is very little you can do?

You control hundreds of millions of dollars in reimbursements, and you can certainly put in place accountability practices that ensure that when rules are broken, when policies are violated, that you prohibit reimbursement from particular entities in the future. Do you not have any policies like that in place?

Mr. GAYNOR. We do, ma'am. We use, for instance, the 270 policy in Puerto Rico, oversight on how a State spends its money through manual drawdown. They can't draw money down until we approve it. There are many different controls that we have. I am not familiar with the Florida issue with Governor Scott, before my time; I would be happy to look into it. I am not sure if we did anything. You know, what actions we took, I just don't know. But I would be happy to get back with you with an answer on that.

Ms. WASSERMAN SCHULTZ. I would appreciate that. Thank you. I yield back.

[Mr. Gaynor responded for the record:]

- Through the Public Assistance program, FEMA reimburses applicants for eligible debris removal projects.

- FEMA does not enter into contracts for debris removal services nor does FEMA remove debris from disaster declared areas.
- FEMA continues to write and approve reimbursement for Hurricane Irma debris removal projects as documentation is received from local officials.
- FEMA's Procurement Disaster Assistance Teams (PDAT) assist applicants with adhering to Federal procurement standards, as well as FEMA policies and guidance associated with Public Assistance grants. In FY19, PDAT has provided 77 training sessions in 8 regions, 18 states, and 43 cities to date.
- We recommend contacting the Florida Division of Emergency Management or the disaster-declared counties for any questions pertaining to contracts they entered for debris removal services.

The CHAIRWOMAN.

Ms. ROYBAL-ALLARD. And now we are honored to have the chairwoman of the full committee, Mrs. Lowey.

The CHAIRWOMAN. Well, I appreciate the honor. I do wish I had roller skates on today, but I am happy to be here. I am so sorry that I missed so much of the meeting, but welcome, and I appreciate the opportunity to have a discussion with you.

In the aftermath of Hurricane Maria, Governor Cuomo directed New York State entities to provide assistance to Puerto Rico, including assistance provided by New York Electric Utilities to repair the electric grid. This effort was coordinated by the New York Power Authority, which happens to have headquarters in my district. NYPA's efforts are an example of mutual aid with State and local governments provide assistance to each other in the aftermath of a disaster.

It is my understanding that the New York Power Authority is continuing this partnership to provide assistance, not only to Puerto Rico, but also to the U.S. Virgin Islands before, during, and after disasters. Can you help me understand how this type of mutual aid supports FEMA's efforts? And is there anything we can do in Congress to better support and facilitate mutual aid?

Mr. GAYNOR. Thank you, ma'am. Thanks for inviting me today. EMAC, the Emergency Management Assistance Compact is a State-to-State agreement between governors to exchange staff, equipment, and commodities during a disaster. So a governor can ask another disaster for help. It is one of the core things that we rely on at FEMA. Kind of a first-level ask before you ask the Federal Government; you know, do you have it within your State? Can you get it from one of your neighbors? Can you get it from across the country? And it really is the core of how we do good emergency management in the United States.

Specifically for the Puerto Rico ask, there were 92 EMAC requests fulfilled by 27 States. Pretty amazing support from fellow governors in Puerto Rico's worst time. I think that is a shining star, on neighbor helping neighbor in this case, to make sure that you have all the necessary things that you need to deliver, to survivors. Commodities or police, fire, all those, resources went to Puerto Rico, and probably to some deficit to a State that let it go and didn't have access to it.

So, again, this business of emergency management is a team effort. So from State to State, from our private partners, from our volunteers, from other emergency management across the Nation, it all has to be a team. No one person has all the capability to do it themselves, and we cannot be successful without it.

What you could do, I am not exactly sure. I think EMAC works pretty well. I know the National Guard has some issues with how they get repaid. I don't know the exact details of it, but I would be happy to see what we can do to improve that.

The CHAIRWOMAN. Good. Are there many other of these helpers, these States, that were sending supplies? Are they still involved or have they all gone home?

Mr. GAYNOR. I don't know if any States are still down there. I can check. I would imagine that most of those resources have gone home, but I will check.

The CHAIRWOMAN. I just wondered. Now, as you know, to carry out its programs, FEMA, as well as State, territorial, and local governments, rely on contractors. Recently, The Washington Post highlighted issues of payments to contractors for the Sheltering and Temporary Essential Power, or STEP program, in the U.S. Virgin Islands. This program provides critical assistance to residents making repairs to their homes, and we understand that it is also being used in Puerto Rico.

The contractors described in The Washington Post article work under a contract with the U.S. Virgin Islands, but they cannot be paid until FEMA approves project worksheets for work they have done nearly a year and a half after these hurricanes. Now, we understand that the U.S. Virgin Islands made a request for the funding in question in fall of 2018.

Now, I understand this is a complex situation. Can you tell me how much funding is currently pending for the STEP program in the U.S. Virgin Islands and Puerto Rico? And what is the status of the project worksheets? Are the project worksheets related to Puerto Rico and the U.S. Virgin Islands taking longer than usual? And, if so, why?

Mr. GAYNOR. Yes, ma'am. So when it comes to U.S. Virgin Islands and the STEP program—which is a success in Puerto Rico. We did 110,000 homes in STEP. We hoped we won't do that many homes, but we hope to have that great kind of success in USVI.

And this, as I understand, is in two parts. The first part of the STEP program, USVI was completed. We reimbursed the Virgin Islands with \$180 million for that program. They have drawn down some of the money, but they still have some money that they have not drawn down, which they could use to pay contractors, approximately \$60 million that is still left.

The second phase is really aimed at roofs in USVI. That project worksheet is called Project Worksheet 100 and is with USVI right now. And they are trying to validate some of the costs in there. As soon as we get that back at headquarters, we will turn it around, and we will make sure that we properly fund that—and reimburse that project worksheet.

The CHAIRWOMAN. So the timeframe is how long from delivery till you can approve it?

Mr. GAYNOR. Just for context, everything over \$5 million has to go to the Department, Homeland Security, and OMB for a review. So we can get it out the door pretty fast if it is all in order. And then we send it to the Department for review and then OMB for final review, and then we will transfer that money.

Can't tell you how long that is going to take. I think when we get it back from them, we will have a better timeline. But I would love to keep you updated on where we are on that.

[Mr. Gaynor responded for the record:]

- In December 2017, FEMA activated the Sheltering and Temporary Essential Power (STEP) program. Through this program, FEMA reimburses the territory for basic emergency repairs while allowing Virgin Islanders to remain in their homes as a form of shelter while permanent repairs are performed.
- More than \$283 million in funding has been provided to the territory for the STEP program through FEMA Public Assistance. The Virgin Islands Housing Finance Authority (VIHFA) administers this program and calls it Emergency Home Repairs VI (EHRVI).
 - More than \$248 million has been obligated to the territory to support all eligible construction expenses.
 - More than \$35 million was obligated to the territory for project management, including costs associated with travel, billeting of off-island labor and central warehousing of materials.
 - As of April 19, USVI has drawn down more than \$220 million.
- At the request of USVI, EHRVI was extended until April 15, 2019. The requested two-week extension of the program will allow the territory to maximize the use of its contractors to complete those homes that are pending completion.
- Understanding the unique needs of the territory, FEMA made several significant policy changes to expand the STEP program to better serve survivors, including:
 - Increasing the STEP program cap per home from \$20,000 to \$25,000;
 - Providing the ability to waive the cap per homes on a case-by case basis under certain conditions;
 - Authorizing roof repairs to residences that received Blue Roof installations;
 and
 - Extending the program period of performance through April 15, 2019.

The CHAIRWOMAN. I would appreciate an update. And I am wondering, is this typical, that kind of—roughly, how much time does this process take?

Mr. GAYNOR. The scale of Maria is mind-boggling how much money that we are trying to deliver. Billions of dollars in both Puerto Rico and U.S. Virgin Islands. This is a project worksheet of \$278 million. This is a large, large worksheet. Typically, they are not that size. So it just takes longer because it is just more complex. But that doesn't mean it has to be slow.

The CHAIRWOMAN. Thank you. Thank you, Madam Chair.

Ms. ROYBAL-ALLARD. That concludes round one, and so we will start a second round of questioning.

Mr. Gaynor, section 20601 of the Bipartisan Budget Act of 2018 gave FEMA flexibility to make repairs or replace certain types of facilities to industry standards, regardless of their pre-disaster condition for disasters in Puerto Rico. We have heard from the Commonwealth government and others that FEMA is implementing this authority in a manner that appears to be much more limited than Congress intended, with a potential result that few projects will fully benefit from this authority.

Can you explain FEMA's interpretation of this legislation and why there is a sense that this is not being carried out as intended?

Mr. GAYNOR. Thank you, ma'am. First, I think we want to thank you from FEMA for passing the BBA, as it is known. It really allows us to do things that we could not do before any disaster. The rules pre-BBA require that we only could restore to pre-disaster conditions. As you all know, in Puerto Rico and the U.S. Virgin Is-

lands, that is not the case. So this allows us to restore to industry standard. So thank you for that.

And our goal in both Puerto Rico and the U.S. Virgin Islands is to build it back better. We believe that we are implementing BBA with the congressional intent. However, we have preexisting other statutes, Stafford Act statutes, that we are trying to blend to make sure we get it right the first time.

I was in Puerto Rico a couple weeks ago and met with our Puerto Rican counterparts, COR3. And I think we are in agreement with more than less. We are still in disagreement about what BBA looks like for certain projects. I think on one end of the scale, one can interpret that BBA says everything is brand-new. on the other end of the scale, maybe it is just a repair. So we are trying to come to some common ground about how we resolve that.

We are full partners with the government of Puerto Rico on this. I don't think this is really going to be a stumbling block as we move forward. Again, some of these projects are so large, it just takes time to get through it. But I think we are in agreement more than we are not.

Ms. ROYBAL-ALLARD. Okay. Do you think that these issues can be addressed administratively by FEMA or is additional legislation needed to reinforce congressional—

Mr. GAYNOR. No. I think we have all that we need. I think now we are just trying to get down to the details. If a school is completely destroyed and the roof is in, well, maybe you need a new school. But if you go to a different school (and there is 1,100 of those schools in Puerto Rico) and maybe the front door and the windows are blown out, now, does that rate a new school? Again, we want to be good stewards of the Federal dollar. So we are having these discussions about, how to get to yes.

Ms. ROYBAL-ALLARD. Okay. I understand that this authority is limited to critical services, which is a specific term in the Stafford Act that refers to facilities, such as you mentioned, schools and utilities, but not others such as police or fire facilities. Do you think an expansion of this authority to additional types of facilities is warranted? And, if not, why not?

Mr. GAYNOR. I am not sure how far we are on discussion on some of these issues. I would have to get details about some of these issues and questions about, will we get to yes on some of those. But I would be happy to get back to you about the status of that. Again, I think we are closer to yes than not.

[Mr. Gaynor responded for the record:]

The current authorities are sufficient. The administration requested the authority provided in Section 20601 of the Bipartisan Budget Act in order to address certain types of critical infrastructure in Puerto Rico and the U.S. Virgin Islands (USVI) that were antiquated or in disrepair when Hurricanes Irma and Maria hit. In particular, this authority was necessary to address the power systems which consist of highly interconnected and interdependent components and would have been impossible to restore without addressing the pre-disaster condition of those antiquated or poorly maintained components. For other types of damaged infrastructure that lack this level of interconnectedness and these types of interdependencies, FEMA believes that existing programs will be sufficient to allow Puerto Rico and USVI to rebuild in a resilient manner. These existing programs include Public Assistance, Section 406 mitigation, the Hazard Mitigation Grant Program, and funds available from other federal agencies, such as CDBG-DR, as well as private resources.

Ms. ROYBAL-ALLARD. Okay. The Commonwealth government has expressed concerns that the 270 process imposed by FEMA has been a cause of delay in disbursing disaster funds, thereby delaying projects. And we understand that this is a manual validation of costs and documentation. We have also heard that FEMA and Puerto Rico have just reached an agreement to have the Commonwealth take over this process.

Can you explain what the 270 process is, its purpose, and how it works?

Mr. GAYNOR. So pre-removal from Puerto Rico was a process where we looked at all the paperwork to make sure it is in order. We had some problems early on in the disaster where an entity drew down money without proper documentation. So typically, you would have to show, invoices for material, supplies, labor costs, all those kind of things, before we actually let you take that money from the treasury. And so we put restrictions on it, because we are allowed to do that, to make sure, again, we do proper due diligence on this funds.

We have been working with the government for a year on their internal control process. We agreed on that last week, and we removed all the controls. So now the government will have the first shot at reviewing all their paperwork. We will sample that as we go to make sure they are doing all the things we want to do. If we think the risk becomes too high, we have the option to go back to 270.

I don't think we will have to do that. I think we are going in the right direction, and I think this is good for both Puerto Rico and FEMA.

Ms. ROYBAL-ALLARD. So you expect, then, that this will improve the pace of recovery in Puerto Rico?

Mr. GAYNOR. I do, yes, ma'am.

Ms. ROYBAL-ALLARD. Okay. Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you, Madam Chairman.

And, Acting Administrator Gaynor, I really appreciate the lines of questioning. It has been very informative for me and for us. Thank you, sir.

I am intrigued, sir, by the idea of working with your local partners to improve local capacity to deal with smaller scale disasters. How do you define smaller scale, sir?

Mr. GAYNOR. That is in the eye of the beholder. I come from the smallest State in the union, Rhode Island. We are just an average-sized county in Texas. So what is big for Rhode Island is not so big for Texas. And this is part—I think this is part of our challenge, to get—to right-size to make sure that we, don't create the California size and we don't create the Rhode Island size; we create the size that works for everyone.

Again, having been a local and State emergency manager, there are some obligations to make sure that you as a local emergency manager can execute the plan for your mayor, and as a State director, that you can execute your plan for the governor. As the FEMA director, I am making sure that I can execute the plan for the President.

But the whole system has to work together. It is just not FEMA. A bigger FEMA is not the answer. It is all of us working together to a common cause.

Mr. FLEISCHMANN. What would be the incentive for a locality to take on the responsibility for response and recovery?

Mr. GAYNOR. I would ask, again with my local hat on, would I want to manage my own disaster or would I want the Federal Government to manage my disaster? I think I would rather chart my own course.

So we would, I think, conceptually, you know, depending on what size it is, and again, 50 percent of all these assets are under \$7 million, we could just block-grant the agreed-upon disaster cost to a local, and they would manage it under all the Federal rules and regulations and they would be responsible for their—what we call now is outcome-driven recovery. Their recovery, not necessarily our recovery.

And just as you know, this is the governor's plan for his recovery. We support the governor's plan. We don't implement a Federal plan at the local or the State level. Again, I think it is just good business.

Mr. FLEISCHMANN. Thank you, sir.

The FEMA integration teams, or FITs, are in 18 States. I would ask you to kindly provide the committee with a copy of the 18 States that are participating.

Does FEMA approach the States to participate or do they come to you all?

Mr. GAYNOR. It is a little bit of both. I think at first, Administrator Long was trying to sell this program, we had to go out there and sell a little bit. Right now, there are 18 active FIT teams. All 50 States and territories have signed up for FIT teams, and we are trying to meet that goal.

And, part of the goodness in this FIT team is, typically, you only see the Federal Government when a disaster occurs, and that is not a good time. So we want to embed our FEMA team to make sure that the plans and the processes are integrated from State to Federal and from State to local. And those FIT teams are there. They act as consultants for the State, when it comes to Federal programs, to make it more streamlined. There is a lot of goodness in FIT teams, and we fully support them.

Mr. FLEISCHMANN. Yes, sir. Does FEMA assume the cost of the teams, and how long does a team stay with the State?

Mr. GAYNOR. It is. We just realigned what kind of people we assign there. So it comes at a high, basically. So what we are doing is something else, but I think this is more valuable to the agencies to have these FIT teams in these States.

Mr. FLEISCHMANN. Thank you, sir.

[Mr. Gaynor responded for the record:]

These are the 18 States that have FIT teams:

1. Arkansas
2. California
3. Guam
4. Hawaii
5. Idaho
6. Indiana
7. Louisiana

8. Missouri
9. Nevada
10. New Jersey
11. New Mexico
12. North Carolina
13. Oklahoma
14. Oregon
15. Rhode Island
16. Tennessee
17. Utah
18. Virginia

Madam Chair, I will yield back.

Ms. ROYBAL-ALLARD. Mr. Ruppertsberger.

Mr. RUPPERSBERGER. Well, first, I just want to go over a background. Now you have done all the work. You have had so many different plans really working very hard in different areas. You had the wildfires, the hurricanes. All those issues.

When you start to rebuild some of your, I guess, standards or whatever, do you teach or talk about rebuilding so that you are not going to have the same problem again? As an example, I am hearing from a lot of people on the waterfront, Chesapeake Bay area, and from now on when you have to rebuild, you can't have your home on the water. It has to be on a garage or whatever it is underneath.

So where are you as far as standards on rebuilding to make sure that we don't continue to put money into the same areas that have the same problems, unless someone changed their mind, like global warning?

Mr. GAYNOR. Yes, sir. Great question. You know, part of the difficulty is some of these repetitive issues. You have a home, you have a disaster or a flood, you get money from the Federal Government, you rebuild in the same place. That happens a couple times. It doesn't really make a lot of sense for us. The challenge is most of these changes are local code changes, and locals really own their own domain. So whether it is a city, a town, or a State, building codes, zoning codes, it really has to start with them. I think we can try to pressure best practice. And there are some great best practices around the country. But it really has to start locally.

We would prefer not to keep paying for the same disaster over and over and over. To me, that is insanity. And so we need to work a little bit harder on making sure that locals have a program to make sure that they build in a resilient way so you avoid that risk.

Mr. RUPPERSBERGER. (Off mic) you had some leverage there. We were going to be building back in those areas (off mic) insurance companies or other groups other than just the locals.

Mr. GAYNOR. And I will have to check my facts. But I think if you use hazard mitigation money for a repair and it happens again, (I will—I may be half right on this) you are prohibited from using that again, I think, for a repetitive disaster. So you would have to do something to actually improve that property to make it more resilient before you got another disaster handout.

Mr. RUPPERSBERGER. Okay. Thank you.

Ms. ROYBAL-ALLARD. Mr. Palazzo.

Mr. PALAZZO. Thank you, Madam Chair.

Jumping over—you know, being from Biloxi, Mississippi, living my entire life on the Mississippi Gulf Coast, of course, you know,

I hear a lot of references to Hurricane Katrina. I think that was the first bad storm to have hit America, and it was unprecedented. And I think the level of the storms since then are matching in some cases, maybe exceeding the severity of that storm. But that is pretty much a benchmark storm.

And I don't know, but where would I go to find the best practices for FEMA? You know, I do know, several years after Hurricane Katrina, we were in Congress, and I was asking questions. And it is like, how are we making the same mistakes that, you know, FEMA made during Hurricane Katrina. And it might not have been mistakes. It might have been lessons learned, because it was such a disastrous storm.

Is there a repository for best practices? So I am assuming we are sharing them with the local EMAs and the State EMAs and things of that nature. And where could I find those?

Mr. GAYNOR. We do have a great repository of lessons learned from DHS on down. And we want to be smarter about how we are thinking about recovery, the legacy of Katrina. And I will give you some context. This week—or over the past 6 months, we found out this week that we are still spending money, 13 years later for recovery at the tune of, for this particular project worksheet, \$4.5 million for disaster recovery 13 years ago.

What we want to do is not do actual cost anymore. We want to do fixed cost. And this is what 428 alternate procedures is about. This is how business is done in America. You want something done, I give you a price, I perform the work, I get paid.

You know, legacy recovery is not that way. It is actual costs. And if you have no incentive to move faster or move smarter, 13 years later, you are still paying on a disaster. We just need to change the way we do this recovery. But I would be happy to supply, in a tangible way, all the after-action resources that we have.

[Mr. Gaynor responded for the record as follows:]

- FEMA has many best practice repositories available to the public on our website, including our Mitigation Best Practices Portfolio, and our Incident Public Alert and Warning System Best Practices webpage. FEMA also posts various disaster After Action Reports online that highlight best practices and lessons learned related to each disaster.

- FEMA Program Areas and Cadres also maintain disaster SharePoint sites with toolkits that provide updates related to policies and processes learned from disasters. FEMA Regional Operations with Continuous Improvement Working Groups maintain internal trackers that identify lessons learned and issues that arise during disasters. Additionally, the Continuous Improvement Program tracked observations containing best practices from initial response to recovery for the 2017 Hurricane Season.

Mr. PALAZZO. I know after Hurricane Camille, there was actually a congressional report produced on the recovery efforts by the Federal Government. I think I lost those during Katrina, but maybe I can get a set from the Library of Congress or someplace, Archives.

Now, obviously, Mississippi is grateful for the financial assistance post-Katrina recovery to the tune of over 3-point something billion dollars. We would not have been able to recover as near as well as we have. And our whole mind-set was not to just build back, but build forward. You know, mitigating against future storms and be smart with the money, because we knew it was a gift from the Federal Government and the American people. So please trust

me, I mean, we are extremely grateful to everyone that supported our recovery.

Now, I do have something that has been—some concerns that have been popping up lately, is that FEMA is kind of like second-guessing. Years after the work has been done, they are asking for money to be returned. And I know continuously there has been a lot of turnover amongst FEMA staff. So there may have been a FEMA project director onsite in 2007, work may have been done. And then, you know, in 2013, someone is looking at the paperwork and saying, well, oh, why did they do this? That is not right.

But at the time, we feel like some of these projects where, you know, we followed FEMA's guidance, we did it to the T, we did exactly what they want, and now they are kind of being unfair changing the rules after the money has been expended and spent and asking for it back.

Is that something that you are seeing or hearing from other, maybe, storms? And what can we do to alleviate that? Because there has got to be some documentation to say, yeah, we approved it. We can't go back 10 years later and say, hey, city, you know, you owe us, you know, \$30 million because we don't think it is—you spent it right, second-guessing what was done during the initial recovery.

Mr. GAYNOR. So I have personal knowledge of this as a State director of FEMA trying to take money back from the States, so I know the pain of that. And this goes to the legacy of how we did recovery. If you can imagine, if you started a project in 2007 and it doesn't close out until 2014, and you have all that paperwork that you have to go through to actually get reimbursed, it can be an impossible task.

What we have done, learned from those lessons learned is what we have implemented across the country, but specifically in Puerto Rico and the U.S. Virgin Islands, is validate as you go, right? So, maybe there is a big payment that happens. Take all that work that was done, all that paperwork, all those forms, and validate it and call it closed. And then we will never go back to that. And then move on to the next chunk.

So it is a new program. I think it is going to prevent clawbacks in the future. That is what we call it, a clawback. And we want to avoid that, because it is not good for us and it is not good for the community that was impacted by the disaster.

Mr. PALAZZO. All right. Well, thank you.

And, Madam Chair, I don't know how much time I have, but can I just ask one quick question in terms of Puerto Rico?

You know, I have heard from several people on the island that they would like to see the category A bucket extended, because there is so much more work to be done. And we know if we go to the local match, Puerto Rico just doesn't have the money.

Can you tell me a little bit about category A? Is there a chance that it will be extended? Just your thoughts on that.

Mr. GAYNOR. Recovery is difficult. And we found that recovery happens best when all partners, and specifically the government—so whether it is a State government or the Commonwealth, has skin in the game where you use your local or State dollars to con-

tribute to the end result. And we are calling it outcome-driven recovery.

So when you have incentive—and this goes to the actual cost and the fixed cost, if you have a fixed cost, we believe that you have more incentive to do it faster. If you have actual costs but no skin in the game, you are just going to hand the bill to the Federal Government, it goes on forever and ever and ever.

I think the administration gave Puerto Rico a lot of time on categories A and B. I want to say 8 months. And I think the 10 percent share that they have is well within their means to fulfill. They can use HUD money. It is actually in this plan on how to make up that 10 percent.

So we think it is reasonable. We think it is going to achieve a faster outcome when the State or the Commonwealth has skin in the game and invest their own dollars in it. Without it, it just keeps going on and on and on.

Mr. PALAZZO. Mr. Gaynor, thank you. Thank you for your public service, and thank you for being here today.

Thank you, Madam Chairman.

Ms. ROYBAL-ALLARD. You are welcome.

We have just a little bit more time for either additional question or some comments, so I do have one last question.

In 2017, FEMA implemented the new delivery model to administer the public assistance program. And it has been used in most of the recent disasters since then, including, for example, in Los Angeles County. However, it is not being implemented in Puerto Rico or the U.S. Virgin Islands.

Can you briefly explain what this new delivery model is and why it was not used in Puerto Rico or the U.S. Virgin Islands?

Mr. GAYNOR. Yes, ma'am. I think we are not using it in there because it was a pilot program. And by the time we got it online, we had already started the traditional process in Puerto Rico. And to go back, from what I understand, it was going to be too difficult, too time-consuming, and really doesn't and will not get us to the end result faster.

So it is just really a way to make sure you account for all those things that you do in recovery in a systematic way using technology to track all that. We are using it in other places around the country. We are just not using it in Puerto Rico because it was a pilot and it wasn't really ready for prime time, and so we just said, let's not make our life more complicated. Let's just go with what we know, and then we will put that program throughout the country at other opportunities.

Ms. ROYBAL-ALLARD. So have you had time to assess this new delivery model? And, if so, can you share any results?

Mr. GAYNOR. Only anecdotally. I think positive results. One of my former State directors in Massachusetts gave us a demonstration on it. I think it was very positively received. It has been a few years now since I have been updated on that. But I would be happy to go back and see where we are on that, uptake, and what the customer satisfaction rate is on that. I would be interested myself to see how we are doing.

Ms. ROYBAL-ALLARD. Okay. I would appreciate it.

[Mr. Gaynor responded for the record as follows:]

The Public Assistance (PA) Program is FEMA's largest grant program, historically averaging \$4.7 billion in assistance each year and accounting for 51 percent of the grant dollars administered by the agency. In 2014 and 2015, to identify improvements to the effectiveness of the Program, FEMA conducted an in-depth diagnostic review, analysis, and outreach that demonstrated the need for significant changes in the way FEMA implements the Public Assistance program. As a result, FEMA developed a new business model for PA Program delivery and is implementing those changes. The delivery model has three basic elements, which support a simplified and streamlined grant application process:

- Simplified roles and responsibilities, and re-trained Federal staff;
- Cloud-based customer relationship and program management software known as The PA Grants Manager and Grants Portal; and,
- Pooled resources so multiple disaster operations can tap into trained experts when developing PA projects. We call these Consolidated Resource Centers (CRC).

Additional details about the new PA delivery model and related phases in the process are outlined in this fact sheet.

FEMA conducts customer feedback analysis on the PA delivery model to continually improve our processes. From January 2016–April 2019, on the Initial Survey, 594 of the 724 (or 82%) of the respondents reported they were either “satisfied” or “very satisfied” with the initial PA engagement. When asked in the Assessment Survey about their satisfaction with the entire PA process, 1,114 of the 1,358 respondents (82%) were either “satisfied” or “very satisfied.”

Mrs. ROYBAL-ALLARD. Any further questions or comments?

Mr. PALAZZO. I could go on for hours.

Ms. ROYBAL-ALLARD. The subcommittee is adjourned.

[Material submitted for inclusion in the record follows:]

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE Lucille Roybal-Allard

Peter Gaynor, Acting Administrator

Department of Homeland Security

Committee on Appropriations

Subcommittee on Homeland Security

Update on Recovery Efforts for 2017 and 2018 Disasters

March 12, 2019

Office of Legislative Affairs Queue

Background: During the hearing on a discussion of a particular project worksheet (PW) you stated “everything over \$5 million has to go to the Department, Homeland Security, and OMB, for review”. During meetings with local officials we have heard discussion of the “Office of Legislative Affairs (OLA) Queue”.

Question.

- Is this the same thing? If not can you explain what each is and who specifically reviews the project worksheets?
- Is this related to the requirement to provide the Appropriations Committees a three business day notice on grants above \$1,000,000?
- For each of the last three calendar years can you please provide the following?
 - Total number of project worksheets in this queue?
 - The average number of days for a project worksheet in this queue?
 - The average length of time for the longest reviews in the top 10% in terms of time and the top 5% in terms of time?

Answer.

Average Days in the OLA Queue by Calendar Year

Calendar Year	0-15 Days		16-30 Days		31-45 Days		46 Plus Days		Total	
	# of Projects	Ave. Days	# of Projects	Average						
2016	455	4.67	7	21.00					462	4.91
2017	642	4.45	10	20.70					652	4.70
2018	781	5.95	99	20.70	17	37.71	9	51.11	906	8.60
2019**	182	6.24	20	18.60	3	34.67	1	46.00	206	8.05
Grand Total	2060	5.22	136	20.40	20	37.25	10	50.60	2226	6.64

**Through March 31, 2019.

Total number of PWs 2,226
 Average length of time - 10% 22.3
 Average length of time - 5% 28.2

The Department of Homeland Security (DHS) is mandated to notify appropriators for projects over \$1,000,000 under section 507 of the Department of Homeland Security Appropriations Act. Since FEMA is a part of DHS, this requirement applies to our projects as well. FEMA works with DHS to provide the notifications required by law.

- Field-based Public Assistance staff develop a project worksheet that characterizes eligible damages and associated costs.
- Regional Public Assistance staff review and approve or provide feedback.
- Headquarters Public Assistance staff review and approve or provide feedback.
- Office of the Chief Financial Officer staff review and approve or provide feedback.
- Office of the Chief Financial Officer staff submit the project to OMB.
- OMB staff review and approve or provide feedback.
- DHS staff review and approve or provide feedback.
- DHS notifies Congress.
- The grant recipient and/or subrecipient are notified.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE Pete Aguilar
Peter Gaynor, Acting Administrator
Department of Homeland Security
 Committee on Appropriations
 Subcommittee on Homeland Security

Update on Recovery Efforts for 2017 and 2018 Disasters
 March 12, 2019

FEMA Disaster Response

Question. With home inspections not occurring for all fire survivors, how does FEMA determine the FEMA Verified Loss for those survivors who maintain insurance but whose home was not inspected?

Answer.

- A full line item assessment of FEMA Verified Loss (FVL) is not obtained when an inspection is not conducted.
- FEMA often utilizes Geographic Information System (GIS) analysis to give broad determinations of degree of damage, i.e., determinations of “not damaged”, “moderate”, “major”, or “destroyed” for structures that are not inspected or assessed, but a full line item assessment is not assigned in these instances.

- Nevertheless, an applicant may still receive disaster assistance based on the GIS analysis. For example, in Disaster-4407-California, fire perimeter data was utilized to pay expedited rent and to stamp applicant files that were positively identified as being within the fire perimeter hot zone, indicating the home was destroyed and/or beyond repair. For that disaster, dwellings confirmed to be destroyed by fire, indicated by the FEMA GIS data, did not require an inspector to meet with the applicant at the damaged dwelling location since those areas were mostly inaccessible and unsafe. The inspector made phone contact with the applicant and conducted the inspection verification information verbally to confirm:
 - The identity of the applicant;
 - The applicant applied for assistance and the home was their primary residence;
 - Data was collected from the normal inspection process to address the necessary data fields in the Automated Construction Estimator (ACE) software.
- If the GIS fire perimeter data reflected the applicant's home as destroyed, but they reported having insurance that would cover fire damage, the standard insurance comparison processes would still apply.

Question. What percentage of people who apply for FEMA assistance from fires receive housing assistance to repair their damaged homes? How does this compare to flood disasters?

Answer. 2.97 percent of people who apply for FEMA Individuals and Households (IHP) assistance from fires receive housing assistance to repair their damaged homes.

30.33 percent of people who apply for FEMA assistance from flood disasters receive assistance to repair/replace their damaged home. The flood percentage only includes disasters with an incident type of flood, meaning that disasters with incident type of hurricane, such as Hurricane Harvey, are not included in the percentage.

The analysis looked at valid registrations from disaster declared in calendar years 2017 and 2018.

Question. The vast majority of those who perished in during the October 2017 wildfires were either over 65, disabled, or homeless. What is FEMA doing to encourage that evacuation planning gives special attention to individuals in these high-risk groups?

Answer.

FEMA regularly offers and conducts Technical Assistance (TA) deliveries to state and local partners.

FEMA uses a variety of methods to provide TA, including:

- In-person workshops to support implementing the National Preparedness System and opportunities for peer-to-peer learning; and
- Technical assistance for emerging, cross-cutting, or complex topics. This delivery method may include the development of new tools, plans, and processes that are of benefit to jurisdictions nationwide.

Such "TA deliveries" facilitate the development and improvement of evacuation and shelter-in-place plans. These plans are integrated into jurisdictional emergency operations plans and encourage greater collaboration among jurisdictions. Each TA delivery emphasizes the importance of meeting the need of the whole community, including individuals with disabilities and others with access and functional needs,

throughout emergencies and disasters. The TA delivery also facilitates planning for evacuees with limited or no access to transportation who may require government assistance to evacuate safely.

Based on its experience FEMA is developing a guidance document for state, local, tribal, and territorial partners entitled, “*Planning Considerations: Evacuation and Shelter-In-Place*.” The development of the document was also informed by interviews with Los Angeles County and the City of Los Angeles, California, as they assessed their operations during the Woolsey Fire of 2018. Furthermore, FEMA interviewed representatives from Larimer County, Colorado, as that area was impacted by the Beaver Creek Fire in 2016.

FEMA looks forward to sharing *Planning Considerations: Evacuation and Shelter-In-Place* with Representative Aguilar once it is published. It will contain more in-depth guidance on FEMA’s efforts to encourage evacuation planning that gives special attention to individuals in specific communities and populace with evacuation challenges.

Question. Will FEMA allow multiple jurisdictions to submit for single awards to fund multi-jurisdictional infrastructure projects?

Answer. Under the Public Assistance Program, FEMA cannot provide a single subaward to fund emergency or permanent work in multiple jurisdictions. Work eligibility is based in large part on an eligible applicant’s legal responsibility for the work (44 CFR § 206.223). Work across multiple jurisdictions indicates legal responsibility across multiple applicants, and a separate subaward for each applicant, at a minimum, is required by law.

Question. Does FEMA’s damage assessment process differ for fires than floods? And if so, can you explain what those differences may be and the associated justification for those differences?

Answer. No, FEMA inspections do not differ based on peril. During a FEMA inspection, the inspector will determine the cause of damage as well as identify the damage itself. For instance, an inspector will report cause of damage as “wind” and list 500 sq. ft. of roof covering. This process is the same whether the Cause of Damage (COD) is wind, fire, flood, or another hazard. In some events, FEMA will use imagery in place of on-site inspections. In such instances, the imagery must be readily available and provide sufficient delineation and detail as to identify specific areas where homes are destroyed or sustained significant damage. FEMA has utilized satellite imagery to determine destroyed homes during fire, tornado, and flooding events.

Question. What is FEMA’s policy/procedure for working with local stakeholders to develop best practices for “urban” wildfires? Does FEMA have any plans to develop best practices to address unique recovery and mitigation needs of urban areas that have experienced an urban wildfire?

Answer. After a wildfire declaration, FEMA and its partners work with state, local, tribal, and territorial stakeholders to support recovery through applying the principles of the National Response Framework and National Disaster Recovery Framework. The frameworks provide an organized mechanism for FEMA and the state to engage over 30 Federal departments and agencies to provide subject matter expertise and program authorities targeted to the specific requirements of the incident based on initial joint assessments. The level of support from FEMA varies depending on the nature of the incident and the experience and capacity of the affected state and local jurisdiction. The level of FEMA support is also affected by the ability of the state, and local jurisdictions to coordinate and manage recovery. For example, FEMA supported local and state recovery efforts after the 2018 wildfires in the Town of

Paradise and Butte County, California. FEMA's support, which continues today, is focused on helping coordinate other federal agencies to provide targeted support where needed.

Question. Multiple mitigation grant programs (404, 406, Pre-Disaster Mitigation, CDBG-DR mitigation, etc) need to have a strategic connection. Right now, the funding streams and guidance for each are released at different times, and it makes truly strategic recovery difficult. Does FEMA have any plans to integrate these programs?

Answer.

- The statutory and regulatory purpose and requirements for FEMA and the Department of Housing and Urban Development (HUD) federal mitigation grant programs are somewhat different. The statutes and implementing regulations proscribe differing timelines and eligibility criteria for each of the respective federal grant programs. The statutory authorities include the following:
 - The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), Public Law 93-288:
 - Sec. 203 – Authorizes funding for pre-disaster mitigation measures - Pre-Disaster Mitigation Program (PDM)
 - Sec. 404 – Hazard Mitigation Grant Program (HMGP)
 - Sec. 406 – Public Assistance program to include mitigation measures for public facilities and infrastructure
 - Title I of the Housing Community and Development Act of 1974, 42 U.S.C. 5301 authorizes HUD to provide funding under the Community Development Block Grant (CDBG) program. In the event of a disaster where there are unmet needs, Congress may appropriate additional monies to HUD under the CDBG-DR program to fund disaster relief, long-term recovery, restoration of infrastructure, housing, economic revitalization, or any additional purpose specified in the applicable appropriation.
 - Under fiscal law principles and by regulation, FEMA does not allow duplication of programs, meaning two federal agencies cannot apply their funding to the same purpose, if one has more specific authority to do so. See 44 C.F.R. 206.434(f); HMA Guidance (2015), p. 31. However, as mentioned below, in some circumstances, HUD provides statutory authority to allow its CDBG funds to be used as the non-federal share for HMGP projects.
- Though there are differences as outlined above, FEMA continues to work internally and with our partners to align various programs as applicable and feasible:
 - **Sec. 404 and Sec. 406 Mitigation grant funding** - HMGP can be used to reduce risk to communities and their facilities, whether damaged or undamaged, but not to repair disaster damage. HMGP can be used to fund mitigation projects that benefit both public and private structures. HMGP is particularly well-suited to combining with 406 mitigation because HMGP is often most needed and effective immediately after a disaster when a community is acutely aware of its need to reduce future risk from the harm it has suffered.
 - As per Sec. 406, the focus of the Public Assistance (PA) program is on repairs and mitigation of damaged public facilities and infrastructure. Combining the facility-focused 406 mitigation, with the broader risk reduction of HMGP at a critical recovery time post-disaster makes for a more robust and vital mitigation effort. There are significant differences in program authorities and eligibility requirements between the PA Program and HMGP. PA Section 406 mitigation funds must apply to a facility that has been damaged by a major disaster. Undamaged facilities and broader community-level projects

are not eligible for 406 mitigation funding, regardless of vulnerability, even if essential to normal functioning of a community in the event of a disaster. Whereas with HMGP, the program is administered by the state which sets funding priorities and there is no requirement that the funds be applied to damaged facilities.

To be eligible for mitigation funding under the PA Program, the mitigation measure must directly reduce the potential for future, similar damage to the facility. An applicant may use both HMGP and 406 mitigation funds to implement mitigation measures on the same facility, but not for the same work. However, combining funds can be difficult because HMGP funding is administered by the state, it has different requirements, and it operates on a different timeline than the PA Program.

The challenges to combining HMGP and 406 mitigation funding can result in communities not achieving their risk reduction objectives. To help fill coordination gaps such as those identified here, FEMA has recently established the Community Infrastructure Resilience Branch within the Federal Insurance and Mitigation Administration which is dedicated to working across FEMA's programs, especially PA and HMGP. This branch will help communities identify mitigation opportunities and develop processes and tools to assist communities in fully leveraging FEMA's mitigation funding. The Community Infrastructure Resilience Branch will work with Public Assistance and HMGP in developing clear and consistent policy and guidance to describe how communities can identify mitigation opportunities and execute cost effective and technically feasible projects under both programs. In addition, the branch is coordinating with the PA Program to streamline the process and reduce the administrative burden on communities in identifying 406 mitigation opportunities and applying for funding.

- **Pre-Disaster Mitigation Grant funding**, as well as **Flood Mitigation Assistance (FMA)**, is based upon annual appropriations from Congress, therefore the application period and available funding is based upon this annual cycle and not driven by disaster declarations. However, moving forward, Section 1234 of the Disaster Recovery Reform Act of 2018, modified Sec. 203 (PDM) of the Stafford Act to make monies available from an aggregate amount of funding under the Disaster Relief Fund. Because this funding will no longer rely upon annual appropriations, it is anticipated that a more reliable funding source will enhance pre-disaster mitigation capabilities and increase alignment with post disaster grant funding opportunities, including non-FEMA sources. In order to reduce complexity and administrative burden, FEMA provides a Hazard Mitigation Assistance (HMA) Guidance document which details both the similarities and the differences in the HMA grant programs. Similarly, the Public Assistance program provides guidance for use by states, territories, tribal, and local government entities, through the Public Assistance Program and Policy Guide.
- **FEMA and HUD mitigation grant programs** – CDBG-DR funding is not available with every disaster declaration but only with a specific Congressional appropriation in the event of unmet needs in local communities following a large disaster event. As stated above, the statutory and regulatory purpose and requirements for FEMA and HUD mitigation grant programs are somewhat different. The two programs have varying purposes, funding procedures, application timelines, and other administrative parameters. However, there are commonalities between the programs. HMGP regulations at 44 CFR § 206.434 – Eligibility, allow for packaging of programs to facilitate combining funds with other Federal, State, local, or private funding sources in order to develop more comprehensive mitigation solutions. Additionally, CDBG-DR funds may be used for

non-federal match on FEMA grant awards in most situations. This is dependent upon the authorizing statute for CDBG-DR funds and whether it explicitly allows funds to be used as a match for other Federal grants in certain situations. To the extent that common best practices and procedures between the two programs can be articulated and shared with state, territory, tribal and local communities, this may help simplify and streamline mitigation grant program delivery to some degree.

Question. As FEMA and other federal agencies work to improve tools for disaster response and long-term recovery, it's important to ensure we consider emerging technologies to help federal dollars go further and help prepare communities with access to sufficient resources. We saw a successful example of innovation filling a void with FEMA's temporary policy to increase available housing accommodations in a shortage by allowing peer-to-peer lodging for federal workers responding to Hurricane Maria in Puerto Rico. Would you support looking at ways to continue to modernize the agency to help improve response and recovery?

Answer. Yes, FEMA supports continued innovation and modernization to help improve response and recovery. Our Agency, using lessons learned from the 2017 and 2018 disasters and the Strategic Plan, is analyzing and seeking ways to enhance our operations and improve program delivery.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE David Price
Peter Gaynor, Acting Administrator
Department of Homeland Security
 Committee on Appropriations
 Subcommittee on Homeland Security
Update on Recovery Efforts for 2017 and 2018 Disasters
 March 12, 2019

Sheltering and Temporary Essential Power (STEP) Program

Question. Can you please explain your process for determining the length of time states have to implement their STEP Programs?

Answer. The Sheltering and Temporary Essential Power (STEP) pilot program is an emergency sheltering program authorized under Section 403, 42 U.S.C. 5170b(a)(3)(B) and (I), and 5170b(a)(4) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended. Title 44 of the Code of Federal Regulations (44 CFR) § 206.204(c)(1), **Project Performance** establishes the time frame for completing emergency work at six months from the date of the declaration. Within the six-month timeframe, STEP guidance specifically requires:

- identification of potential STEP participants sixty (60) calendar days from the date the disaster is declared;
- that the program recipient must obtain the Right of Entry (ROE) for a property within thirty (30) calendar days after identifying a property for participation in STEP; and
- all emergency work must be completed no later than sixty calendar days from the date the ROE is obtained from the homeowner.

Question. What factors do you consider when a state applies for an extension of their STEP Program?

Answer. The applicant responsible for implementing STEP (typically the recipient, i.e. the state, territory, or tribe) must submit a written request for an extension to the period of performance which is established in the disaster-specific guidance and is typically six months from the date of declaration. The request must include the following information consistent with 44 CFR § 204.204(d):

- Documentation substantiating delays beyond its control (e.g., delays in obtaining Rights of Entry for participating properties);
- A detailed justification for the delay (i.e., describe extenuating or exigent circumstances that exist);
- Homeowner interest in program;
- Status of the work; and
- The project timeline with the projected completion date.

Disaster Recovery and Reform Act of 2018

Background: Last year, Congress passed the Disaster Recovery Reform Act, which included a variety of reforms to FEMA.

Question. The DRRRA established new rates for the Hazard Mitigation Grant Program and expanded the definition of allowable management costs.

- When will FEMA release the new Management Cost Guidance?

Answer. FEMA issued a Management Cost Interim Policy in November 2018 pursuant to the requirements of DRRRA (P.L. 115-254). The Interim Policy defines the framework and requirements of DRRRA Section 1215 as it amends Section 324 of the Stafford Act and requires FEMA to provide HMGP funding for management costs up to a specified percentage of a total award amount.

On February 28, 2019, FEMA deployed system updates to allow Hazard Mitigation Grant Programs (HMGP) applications to include management costs up to the specified amount for recipients and sub-recipients. FEMA will evaluate this interim policy as it is implemented and will incorporate updates into the next version of the Hazard Mitigation Assistance Guidance.

- When do you expect to have the new Hazard Mitigation Grant Program management cost system fully functional?

Answer. On February 28, 2019, FEMA made system upgrades to account for the increased amount for management costs. The HMGP system is currently fully functional. FEMA is in the process of developing additional implementation tools and resources, to include job aids and training.

Question. The DRRRA authored a National Public Infrastructure Pre-Disaster Mitigation Fund, which will fund resilience-focused public infrastructure programs by setting aside 6% of the total amount allocated for certain categories of disaster assistance grants. This will allow for states to fund projects to reduce their risk to public infrastructure before the next disaster, which have been proven to reduce future costs.

- When will FEMA release guidance on how this program will work?

Answer. FEMA is in the process of drafting policy to implement the Building Resilient Infrastructure and Communities (BRIC) program. A guidance document refining the program will follow. FEMA's target for releasing the first BRIC Notice of Funding Opportunity under the National Public Infrastructure Pre-Disaster Mitigation is summer of 2020.

- What projects will be eligible, and how will funds be allocated?

Answer. FEMA is in the process of developing the BRIC program and is actively working over a dozen Task Teams to scope and design different portions of the program. Funding for projects will focus on mitigating risk, building resilient infrastructure, and protecting and restoring important community lifelines (such as transportation, communications, energy, etc). FEMA is working to engage external stakeholders to ensure their input is considered through the program design process. FEMA continues to make progress on the development of program structure, funding award criteria, and project prioritization

guidance, and we intend to share such information with our Congressional stakeholders as soon as we are able.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE Steven Palazzo
Peter Gaynor, Acting Administrator
Department of Homeland Security
 Committee on Appropriations
 Subcommittee on Homeland Security

Update on Recovery Efforts for 2017 and 2018 Disasters
 March 12, 2019

Communications Technologies

Background: As technology becomes more mobile, enterprise IT must follow suit and agencies like FEMA must embrace these advances in technology in order to better serve communities impacted by natural disasters, such as hurricanes, tornadoes, and extreme flooding. Last year, this Subcommittee recognized the importance of embracing new technologies at FEMA, including utilizing existing enhanced communications technologies that integrate telephone, mobile, and web communications to provide real-time feedback through live, interactive, multi-media platforms to better serve those impacted by natural disasters. As a result, the Committee provided FEMA additional funding in FY 2019 for enhanced communications platforms that utilize these technologies. This is critical because it will enable FEMA to more effectively partner with State, local, tribal, and territorial governments by efficiently engaging and supporting the disaster workforce to prepare for all possible hazards and reduce the impact of natural disasters.

Question. How can FEMA Operations and Support, Mission Support, utilize Operational Communications to more to better serve those impacted by natural disasters and more effectively partner with State, local, tribal, and territorial governments before and after major storms?

Answer. FEMA's Approach for Operational Communications in Partnership with State, Local, Tribal, and Territorial Governments.

Operational communications are a critical part of FEMA's mission portfolio. Our response and recovery activities across the depth and breadth of our Stafford and non-Stafford responsibilities would not be possible without the concept. The success of response and recovery efforts may be affected by disconnects that occur when operational communications at the federal level are not synchronized to enable unity of effort among STTL mission partners.

FEMA has developed a new concept of seven Community Lifelines as the primary focus during response. Specifically, the Communications Lifeline is supported by government, non-governmental organizations, and the private sector, including communications infrastructure owners and operators. The Lifelines approach enhances the ability to integrate FEMA preparedness efforts, Regional Emergency Communications Coordination Working Group (RECCWG) initiatives, and SLTT plans development into response operations to identify unmet needs, close capability gaps, and demonstrate progress towards incident stabilization.

Technology Priorities

FEMA strives to ensure robust capabilities are available to SLTT emergency managers, public safety responders, and other federal disaster customers. FEMA also endeavors to continually enhance disaster emergency communications (DEC) capabilities to improve mission performance.

Ensuring that communities have access to the communications capabilities they require is of the upmost importance in the aftermath of a disaster. This operational communications priority aligns to the FEMA 2018-2022 Strategic Plan, *Objective 2.4 – Improve Continuity, and Resilient Communications Capabilities*. Building resiliency into communications solutions improves likelihood that responders can continue to communicate and deliver lifesaving and life sustaining services and survivors have access to information and support. Reducing and mitigating the risks to communications systems at all levels (e.g., technical, systemic, and programmatic) supports operational communications requirements and increases system availability.

Three strategic initiatives drive FEMA’s efforts:

1. Ensure Continuity of Communications

- *Integrate resiliency during the technical engineering of new communications capabilities (e.g. Mobile Office Platforms).*
- *Examine opportunities to increase the resiliency of existing operational systems (e.g. Hardening of HF Radio Systems).*

Resilient communications capabilities are essential for effective disaster response and recovery operations. In the event of a disaster, FEMA must have systems and equipment to support continuity of communications in the absence of the fixed communications infrastructure, network failure or congestion, rugged/remote terrain, and/or harsh weather or operational conditions. FEMA maintains reliable, deployable communications solutions for federal and SLTT response personnel and disaster survivors. FEMA is upgrading its fleet of mobile emergency operations vehicles (MEOV) with state-of-the-art interoperable communications solutions.

2. Increase and Optimize Bandwidth Usage

- *Adopt methods to increase and optimize bandwidth of communications capabilities, with specific attention to tactical use cases in disaster areas during response and recovery operations.*

As technology advances, the demand for multimedia capabilities will continue to grow. However, the use of these bandwidth-intensive applications in a tactical environment heavily strains the network and severely degrades the overall performance of emergency communications during a disaster response. In addition, the number of personnel requiring communications support at an incident site rapidly rises during catastrophic disasters, further limiting the amount of bandwidth available to all users. A focus on increasing and optimizing bandwidth within a disaster area will significantly improve responder capabilities and capacity during response and recovery operations when they are most needed.

3. Pursue Technology Convergence in mobile platforms

- *Pursue technological convergence to streamline or consolidate communications systems while improving the communications capabilities available to customers.*

Equipment manufacturers are continuously working towards developing communications devices that incorporate greater functionality, enabling users to do more with less, even in austere environments. This concept of technological convergence yields single networks and devices capable of supporting multimedia applications, which offer significant improvements over dedicated voice, data, and video solutions. Emergency response personnel need to have the same full-feature voice, data, and video

communications capabilities, as well as access to enterprise networks and applications while on the move.

FEMA's mobile emergency operations vehicles (e.g. MEOVs and Mobile Communications Office Vehicles (MCOVs)) incorporate multiple technologies (e.g., cellular, satellite, Wi-Fi) that enable access to different communications networks for added redundancy and ability to function in multiple SLTT environments. Newer mobile capabilities can offer emergency response personnel greater flexibility to perform tasks more quickly and provide the ability to extend DEC capabilities further into a disaster area in support of SLTT responders. This results in improved command and control, operational support, and situational awareness, resulting in greater overall effectiveness of response operations and personnel safety. Nevertheless, even as newer user devices incorporate the functions performed by several older devices in one package, it is important to have multiple networks available for redundancy in accordance with *Strategic Plan Objective 2.4 – Improve Continuity, and Resilient Communications Capabilities 2.4*.

4. Champion Interoperability

- *Incorporate standards-based interoperability into technical solutions whenever possible. In many, but not all, cases this can best be accomplished via an Internet Protocol-based approach.*

Although significant progress has been made with communications interoperability, SLTT response organizations continue to deploy disparate communications platforms that can often lead to interoperability issues if not coordinated properly. Internet Protocol (IP)-based communications solutions can be interoperable if manufacturers follow a common standard. IP-based communications use the Internet or other network backbones to transmit information via data packets. As a result, IP-based assets can support simultaneous voice, data, and video transmissions over the same communications medium, leading to opportunities to implement “Everything over IP” (EoIP) communications solutions. The availability of alternative non-IP based solutions using technologies such as Land Mobile Radio (LMR) will still be required during a disaster response because an Internet connection is not always guaranteed; however, greater use of IP communications will simplify response and recovery operations because more users are comfortable operating IP-based mobile devices (e.g., laptops, cellular telephones). IP communications have been integrated into FEMA mobile emergency operations fleet, enabling users to take advantage of the many mobile applications and analytical tools available to access, share, and analyze data to better inform decision-making. IP communications provide increased functionality, scalability, and interoperability, potentially at lower operational costs than non-IP/legacy communications systems.

Summary

New communications technologies and novel innovations provide FEMA with opportunities to improve or replace existing systems, mobile platforms, and processes to meet communications requirements in the aftermath of a disaster. Recognizing these opportunities requires that FEMA keep abreast of developments across government, academia, and industry while keeping an eye toward how technological improvements can be realized to advance mission partner needs.

Question. How is FEMA using social media and publicly available information during disaster response?

Answer. During disaster response, FEMA's Office of External Affairs uses social media and public information on social media platforms in the following ways.

- **Social listening:** During times of disaster, FEMA uses publicly available social media posts to better understand the situation unfolding on the ground. FEMA's social listening program has four primary purposes:

- Better understand the needs and concerns of disaster survivors.
- Increase operational situational awareness and recognize potential unmet needs.
- Identify rumors and misinformation early.
- Improve our strategic messaging to ensure survivors have the information they need.

Our social listening program also coordinates closely with FEMA's crowdsourcing program. The crowdsourcing program partners with external groups using publicly available information to fill operational information gaps by building data visualizations.

- **Public engagement:** FEMA maintains public social media profiles such as Facebook, Twitter, Instagram and LinkedIn. FEMA staff members monitor the accounts daily for comments and inquiries from the public and respond as necessary. During times of disaster, there is often a sharp increase in the number of inquiries on social media from disaster survivors. We respond to those inquiries with relevant and up-to-date information and resources related to disaster response and recovery. We also analyze inquiry topics to identify common questions or topics that can further inform FEMA's overall messaging strategy.
- **Messaging and information distribution:** FEMA's social media accounts share information and messaging related to the agency mission and programs on a regular basis. During times of disaster, we use the social media accounts to provide affected communities with timely and accurate information about how to prepare, stay safe, get disaster assistance and access resources. We also highlight information and resources from federal, state, local and tribal partners by re-sharing their social media posts and directing people to the best accounts for information. All of the information shared on FEMA's social media channels is coordinated through Emergency Support Function (ESF)-15: External Affairs procedures to ensure consistency among partner agencies and throughout all communication channels.

Question. Does FEMA have any specific compliance policies that guide how they treat the information?

Answer. FEMA follows compliance policies set by each individual social media platform. Additionally, FEMA conducts a Privacy Threshold Analysis of all social media platforms, and all social media tools used within the Agency. FEMA follows the guidance provided by the *DHS Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007, Revision 3*, to define and protect personally identifiable information online.

Question. What are the opportunities and challenges associated with using social media/publicly available information?

Answer.

Opportunities

- Identifying rumors and misinformation related to the disaster that are spreading on social media so that they can be addressed and corrected in a timely manner.
- Building trust among the general public by providing valuable, relevant public information during times of disaster.
- Identifying challenges faced by survivor communities by analyzing common issues and concerns raised through social media inquiries.
- Maintaining high level situational awareness in times when it may be difficult or too early to get boots on the ground.

Challenges

- Policies and laws related to records management and IT security are often not modernized enough to account for the latest social media technology.
- The increased number of “bot” accounts on social media can sometimes skew online conversation.

Flood Insurance

Background: Flood Insurance Rate Maps are used by FEMA to delineate both the special hazard areas and the risk premium zones applicable to a community. This has a significant impact on community recovery and development after a storm. As you know, many communities in Coastal Mississippi are still recovering from Hurricane Katrina that devastated the area in 2005. It is encouraging that the Coastal Counties in my district, and the State of Mississippi, are investing a significant amount of time and funding to ensure that the coast has maps that reflect the true, accurate flood risk in these communities. The Mississippi Coastal Map Revision Project is following the FEMA Guidance for Flood Risk Analysis and Mapping and recently submitted Intermediate Data Submittal #1 for review by the regional office.

Question. How does FEMA prioritize mapping projects and how are you ensuring that those who are going through the established guidelines receive equal attention from your regional offices? Additionally, how does FEMA in DC conduct oversight of its regional offices to ensure they are working with communities in a timely fashion?

Answer. FEMA is required to re-evaluate all flood hazard studies at least once every five years. FEMA inspects flood hazard studies against a variety of possible changes to the physical environment, climate patterns, or engineering methodologies that may have occurred since the flood study was performed, including new or removed bridges or culverts, or new gage data for recent flood events. FEMA identifies map update needs for areas that do not meet current engineering and mapping standards and coordinates with the states and communities about their priorities. FEMA prioritizes maps that need to be updated and works with the state and the community to start the process. FEMA leverages allocated resources to identify areas of need in a process that is coordinated at the Regional level with state and local partners.

Flood Insurance Rate Maps are adopted by communities to inform land use and construction decisions. Communities can request changes to the maps at any time. The community can provide technical data to FEMA and FEMA will update the flood map as warranted. NFIP participating communities are required by regulation to inform FEMA of changes within a community and provide supporting technical data to update a community's flood map. The mapping process is a partnership between FEMA, the state, and the community. All partners have a role in ensuring that the maps reflect accurate flood risk.

FEMA has mature processes in place to examine continually the nation's flood hazard data inventory. Changes in topography and land use, or the occurrence of significant meteorological events, all have the potential to impact the evaluation of flood risk. The reporting of New, Valid, or Updated Engineering (NVUE) statistics are used to measure data quality by ensuring that flood hazard data are new, have been updated, or are deemed to be still valid through a continuous review and update process. FEMA has a target of progressing toward a maintenance phase of its map inventory, where the map inventory is assessed within a 5-year cycle and 80 percent of the miles are identified as meeting current engineering and mapping standards. FEMA Headquarters (HQ) oversees progress towards the NVUE target and ensures that maps are prioritized and updated with this target in mind.

FEMA has developed an oversight strategy that includes the necessary policies and procedures to enable mapping projects to move forward on a timely and consistent basis. FEMA has established a strategy to

monitor the status of projects, which includes the institution of quarterly joint performance review meetings. The Regions have performance metrics to ensure progress in moving projects forward to completion. In addition, FEMA developed annual planning guidance that addresses how HQ and the Regions will collaborate to advance priorities, measure success, and track progress. The Fiscal Year 2019 Planning Guidance equips HQ and regional staff to meet our common objectives. It facilitates the alignment of efforts to enhance the understanding of risk, orient cross-programmatic processes and resources to better meet customer needs. The guidance also change risk reduction decisions and behaviors across the whole community.

Question. While my coastal counties are doing an excellent job of working to meet the set standards, I would also like to bring to your attention that other maps throughout the United States have not been updated in decades. Where Hurricane Harvey devastated the coast of Texas, maps from the area have remained untouched since 1983 and unfortunately this isn't an isolated issue in the United States. I know that your agency is set to review flood maps every 5 years to ensure true flood risks are reflected for local residents. How does FEMA incentivize communities to update their maps? And if there is no incentive, how does the agency penalize those who have not complied with these guidelines?

Answer. Participation in the NFIP is based on an agreement between local communities and the federal government: if a community adopts and enforces a floodplain management ordinance to reduce future flood risks to new construction in Special Flood Hazard Areas, the federal government will make flood insurance available within the community as a financial protection against flood losses. According to Section 65.3 of the National Flood Insurance Program regulations, the community has the responsibility to notify FEMA if changes take place that will affect an effective Flood Insurance Rate Map (FIRM). The community must submit data regarding these changes as soon as possible, but no later than 6 months after the project is complete, so that the FIRM can be revised to reflect current conditions. Communities can be placed on probation if they do not adequately enforce floodplain management regulations meeting the minimum requirements. Failure to correct floodplain management violation will result in the community losing eligibility for the NFIP.

The mapping process is a partnership between FEMA, the state, and the community. All partners have a role in ensuring that the maps reflect accurate flood risk. FEMA works with states, communities and other partners to ensure local knowledge, areas of concern, and data sources are integrated into mapping studies and into a community's FIRM. At any time, community officials can submit scientific or technical data to FEMA to support a local FIRM revision. FIRM changes could be driven by things like construction projects, surface erosion, or the impact of natural events that affect the community's floodplains. Erosion, construction projects, and natural events can dramatically affect how water flows and drains. We depend on communities to tell us about these local changes, to keep their flood information precise and up to date. To ease the map update process, FEMA has established administrative procedures that allow communities to request a map revision as they implement their land use ordinance.

Flood maps are often compared to actual events like Hurricanes Harvey or Sandy. However, flood maps do not predict where flooding will occur, they identify where the highest risk areas are that are required to have flood insurance. It is important to keep in mind that the maps reflect the required minimum standard (the 1-percent-annual-chance flood) and are not intended to show absolute lines where flooding will and will not occur. Anywhere it can rain, it can flood, which means that even the areas depicted on flood maps as having a low or moderate flood risk are at risk of flooding. Floodplains nationwide are both unique and dynamic, and the flood maps that depict them represent a snapshot in time.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE John H. Rutherford
Peter Gaynor, Acting Administrator
Department of Homeland Security
 Committee on Appropriations
 Subcommittee on Homeland Security
Update on Recovery Efforts for 2017 and 2018 Disasters
 March 12, 2019

FEMA Reimbursement to Local Municipalities

Background: Hurricanes Irma and Michael, just 13 months apart, were unprecedented events, impacting every utility in Florida, including all 34 municipal power systems. Hurricane Michael was the worst storm to ever hit the panhandle—400,000 customers lost power, including 122,000 from five public power communities. Despite the devastation, power restoration efforts proved exemplary, including the largest and most successful mutual aid efforts ever assembled—600 public power personnel from 16 states for Michael alone. Yet, both federal and state bureaucratic problems persist. Even when FEMA releases money, it doesn't go to the local communities who need it. It goes to the state agency to disburse the funds. For example, Keys Energy, a municipal electric utility base in Key West, still has a \$42 million FEMA filing from Hurricane Irma. FEMA released \$15 million of that to the State back in May of last year. However, Keys Energy to date has only received \$1 million of that \$42 million they are owed. In the meantime, they have to take out a loan to make up the costs. The interest on this loan – just the interest – is costing them \$2900 every day.

Question. When local municipalities don't receive the money they are owed by FEMA – whether it is FEMA's fault or not – the cost of recovery goes up. How can we break this logjam? What can FEMA do to speed up the flow from federal government to local recipients?

Answer. Under the Public Assistance Program, FEMA obligates funds for eligible emergency and permanent work based on estimates. Those funds are provided to the recipient (state, territory, or tribe). Subrecipients (e.g., local municipalities) request reimbursement for eligible work once the work has been completed. Funds are disbursed to subrecipients by the recipient from the funds obligated by FEMA. There are documentation requirements to validate costs claimed that must be met by Subrecipients in order to receive reimbursement for completed work.

FEMA works with its state and local partners to ensure that program requirements are understood and can be met effectively; however, delays in the disbursement of funds FEMA has already approved and obligated is a matter between the recipient and the subrecipient. As to the cause of such delays, any information provided would be, at best, speculative. FEMA's role in mitigating such delays is in continuing to build relationships with state and local partners to provide awareness of and access to available resources to improve knowledge and understanding of PA program requirements.

FEMA Contracting Requirements

Background: Another issue I have heard from municipal electric utilities and rural electric co-ops is the challenge they have with federal contracting regulations. They are told the pre-storm contracts they enter into with local municipalities to get the power turned back on after a storm don't meet federal contracting standards – even though they meet the state and local contracting standards. After the work has been done and the power turned back on, they are told by FEMA that they need to enter into new contracts that meet federal requirements, often creating new bureaucratic problems, including federal claw-back processes.

Question. What can be done to improve the regulation of federal contractual requirements during times of emergency?

Answer. The Office of Management and Budget (OMB) procurement under grant regulations found at 2 C.F.R. § 200.317-326 are applicable to all federal grant awards, including FEMA Public Assistance grants. The OMB rules require recipients and subrecipients of federal funds to follow the federal procurement under grant requirements to ensure full and open competition and reasonable costs, among other public policy goals. As such, OMB has the sole discretion to make any changes to the federal procurement under grant rules applicable to FEMA applicants. FEMA will follow the requirements prescribed by OMB.

The rules also include an exception to competitive procurement requirements when an emergency or exigency circumstance exists. Thus, non-state entities such as municipal electric utilities and rural electric co-ops currently have a reprieve from conducting competitive procurements when there is an immediate threat to life, health, public safety or property or imminent harm. This means that they can use sole-sourced (non-competitive) contracts that might have been procured pre-disaster to address emergency or exigency circumstances after a disaster. The entities must document the emergency or exigency circumstances and should refer to the [FEMA Public Assistance Fact Sheet](#) for sample documentation. Note the rules do not prescribe the length of emergency or exigency periods as each circumstance and threat is different, dictating different emergency/exigency periods based on the communities' needs. Non-state entities are only able to use sole-sourced contracts under this exception for the limited period of time the emergency or exigency circumstances are present. OMB could prescribe a baseline time period, if desired, but that period should be carefully assessed considering it would be applicable to all grants under all situations.

While full competitive procurements are not required in emergency and exigency circumstances, non-federal entities are still obligated to follow other requirements –e.g., conducting a cost or price analysis per 2 C.F.R. § 200.323 and including all required provisions in contracts in accordance with 2 C.F.R. § 200.326. This latter requirement also applies to state entities. As such, to the extent municipal electric utilities and rural electric co-ops wish to use sole-sourced pre-event contracts for emergency and exigency circumstances, they still need to ensure they meet other applicable procurement under grant requirements. It is not recommended that these requirements be waived as they protect the taxpayer dollar by requiring, for example, remedies and termination for cause or convenience clauses. Moreover, if pre-event contracts are involved, compliance with this and other requirements is less challenging as resources are available and the entities are not under the stress of a disaster.

WEDNESDAY, MARCH 13, 2019.

SECURING FEDERAL NETWORKS AND STATE ELECTION SYSTEMS

WITNESS

CHRISTOPHER KREBS, DIRECTOR, CYBERSECURITY AND INFRA-STRUCTURE SECURITY AGENCY

I am going to make my opening statements brief this afternoon in order to maximize time for questions.

Director Krebs, congratulations on being named the first director of the Department of Homeland Security's Cyber Security and Infrastructure Security Agency.

We have spoken about some of the challenges that you and CISA have faced, and I want to reaffirm my commitment to helping you address those challenges. As you know, election security has been a major focus of this subcommittee.

For the second year in a row we have supported significant increases to your budget to address the vulnerabilities to ensure that our election system is secure and reliable.

Director Krebs, thank you again for being here and I would now like to turn to the distinguished gentleman from Tennessee, Ranking Member Fleischmann for his opening remarks.

Mr. FLEISCHMANN. Thank you, Madam Chairwoman. I appreciate those remarks.

Director Krebs, thank you for being here today, and I appreciate you visiting our office and congratulations on being the very first. That is outstanding for this very important agency.

Director Krebs, the importance of our government cyber security cannot be underestimated. So much of what we do is through networks, from getting \$20 from an ATM to our military weapon systems. Our society today is dependent on safe and secure networks.

Further the principle of fair and accurate election voting is paramount to our democracy. And because of this, we need to be ever vigilant to protect our critical infrastructure from foreign nations and criminals who seek undermine our economy and government.

As you know, the Oakridge National is in my district in Oakridge, Tennessee. While Oakridge is sponsored by the Department of Energy, it partners with a number of federal agencies, including the Department of Homeland Security to conduct high level research in many of these areas.

I will have a few questions later in my rounds about CISA and how it works with Oakridge. I think the good work that you do combined with the good work at Oakridge does is a great value for the taxpayers' dollar, plus we can best bring safeguards to our nation and its critical infrastructure working together.

I look forward today to your testimony and to the questions from my colleagues as we hear from you about your initiatives. Thank you, and I yield back.

Ms. ROYBAL-ALLARD. First, for some housekeeping issues. As in other subcommittee hearings, members will be called based on their seniority and those who are present when the hearing started. I would also, would ask that every member stick to the 5-minute time they are allotted to allow everyone to have time to ask their questions.

Also, my understanding is, there is a problem with the microphones, and so, make sure that you have them on.

Please proceed.

Mr. KREBS. Thank you. Chairwoman Roybal-Allard, Ranking Member Fleischmann, members of the subcommittee, thank you for the opportunity to testify today.

This hearing is timely, as I recently announced, five operational mission priorities for the Cybersecurity and Infrastructure Security Agency over the next two years. Two of those priorities, federal network security and election security, we will discuss today.

In both Federal network security and election security, agencies whether Federal, state or local are responsible for the security of their networks. CISA's job is to make their job easier as they managed their risk. In this sense we are the nation's risk advisor. We work to understand risk, share our understanding with those that can best manage that risk, and provide targeted support to help them manage their risk.

On Federal network security our approach is three-fold. First, we define for agencies what secure is. Second, we provide tools and technical assistance to agencies to better secure themselves. And third, when needed or appropriate, we act to intervene or intervene to ensure secure and resilient systems.

In all, this is a particularly challenging undertaking, and there is room left for improvement in a number of areas, including establishing and enforcing a security baseline across the government, analyzing the data we have and collect, and accounting for new technologies like Cloud and mobile. And yet, there is no question that cyber security and federal networks is stronger than it was just four years ago.

Through our approach, our understanding of what is happening across networks is improving. IT capabilities government-wide are on a path to prioritization and standardization, and leadership awareness at the cabinet level is increasing, leading to better accountability and more consistent implementation of policy and guidance.

I would like to briefly highlight a few areas of measurable progress. Through our Continuous Diagnostics and Mitigation program, we are protecting over three million assets across the Federal civilian enterprise.

Before 2016 there was no over-the-top understanding of how many devices were even out there. Through our Intrusion Prevention System that uses classified signatures, from 2016 to July 2017 we stopped 13 campaigns launched by 16 different advanced actors.

Through a Binding Operational Directive we issued in 2015 we reduced the time agencies were taking to patch critical

vulnerabilities from an average of 219 days to today's average of around 20 days. In many cases this is better than industry.

In 2017 we issued a Binding Operational Directive to require the removal of Kaspersky antivirus products from federal networks.

And finally through a Binding Operational Directive in 2018 we have enforced stronger email and web security standards with the federal government leading all industry sectors in deploying DMARC to stop email-based phishing attacks.

We have made our directives public and available for the network defense community. Just recently, we issued an emergency directive to protect federal networks from a global campaign tampering with what is essentially the internet's phone book. We heard back from numerous stakeholders outside of the federal government, including a large metropolitan chief information security officer that they followed our guidance, but did not have to, and yet they did.

Cyber threats also pose a growing risk to our nation's critical infrastructure. Perhaps the highest profile threat we face today are attempts by nation state actors to interfere in our democratic elections. Ahead of the 2018 midterms, we surged our efforts and over 550 CISA employees throughout the agency worked with all 50 states and over 1,400 local and territorial election offices to raise awareness of the threat, provide free technical cyber security assistance, share threat mitigation information and otherwise empower state and local election officials to secure their systems.

Our efforts to Protect 2020 are already underway. Protect 2020 will focus on broadening the reach and depth of assistance to state and local election officials and their private sector partners, emphasizing the criticality of election auditability, prioritizing the need to patch election systems, and developing state and locality-specific cyber security profiles that officials can use to manage risk.

In closing, I would like to thank the Committee for its continued support of CISA and our mission. The additional \$33 million provided in Fiscal Year 2019 for election security helps ensure that election security is here to stay at CISA.

Additional resources provided over the years for our federal cyber security programs that helped raised the baseline of cyber security across the federal enterprise and have mitigated countless threats to federal networks and critical infrastructure. We at CISA are committed to working with Congress to ensure that our efforts cultivate a safer, more secure and resilient homeland.

Thank you again for the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Krebs follows:]



Testimony

Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

“Securing Federal Networks and State Election Systems”

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON HOMELAND SECURITY

Wednesday, March 13, 2019

Washington, DC

Chairwoman Roybal-Allard, Ranking Member Fleischmann, and members of the Subcommittee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to strengthen the cybersecurity of federal networks and increase the security and resilience of our Nation's critical infrastructure. Safeguarding and securing cyberspace is a core homeland security mission.

At DHS's Cybersecurity and Infrastructure Security Agency (CISA), our mission is to defend against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow – "Defend Today, Secure Tomorrow."

CISA leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. We assist agencies with the protection of civilian federal networks and coordinate with other federal agencies, state, local, tribal, and territorial (SLTT) governments, and the private sector to defend our Nation's critical infrastructure from malicious cyber activity. By bringing together all levels of government, the private sector, international partners, and the public, DHS protects against cybersecurity risks, improves our whole-of-government incident response capabilities, enhances information sharing of best practices and cyber threats, and strengthens resilience of our Nation's critical infrastructure.

Cyber Threats

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. The past several years have marked a growing awareness of the cyber domain in the public consciousness. Federal networks face large and diverse cyber threats ranging from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of their attacks. Our adversaries develop and use advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

Cybersecurity Priorities

CISA, our government partners, and the private sector are all engaging in a more strategic and unified approach towards improving our Nation's overall defensive posture against malicious cyber activity. In May 2018, DHS published the Department-wide *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. Both the Strategy and Presidential Policy Directive 21- Critical Infrastructure Security and Resilience, emphasize that we must maintain an integrated approach to managing risk.

The *National Cyber Strategy*, released in September 2018, reiterates the criticality of collaboration and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide CISA's efforts to secure federal networks and

strengthen critical infrastructure. DHS works across government and critical infrastructure industry partnerships to share timely and actionable information as well as to provide training and technical assistance. Our work enhances cyber threat information sharing between and among governments and businesses across the globe to stop cyber incidents before they occur and quickly recover when they do. By bringing together all levels of government, the private sector, international partners, and the public, we are enabling a collective defense against cybersecurity risks, while improving our whole-of-government incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

The Department of Homeland Security's Cybersecurity Responsibilities

CISA works with federal civilian departments and agencies to implement common policies and best practices that help manage risk in the face of ever-evolving threats. By protecting systems and sharing information, alerts can be issued at machine speed when events are detected to help protect networks across the government information technology enterprise and the private sector. This enterprise approach helps transform the way agencies manage cyber networks through strategically-sourced tools and services that enhance the speed and cost effectiveness of federal cybersecurity procurements and allow consistent application of best practices.

CISA is embracing our statutory responsibility to administer the implementation of federal agency cybersecurity policies and practices by leading the effort to secure the federal civilian executive branch enterprise. The overarching goal of federal cybersecurity is to ensure that every agency maintains an adequate level of cybersecurity, commensurate with its own risks and with those of the federal enterprise. The result is a mix of decentralization and centralization in governance and implementation. Agencies implement their cybersecurity programs and manage their own risk, as they are best positioned to understand how their unique mission environments need to be protected. While individual agencies ultimately must implement their own cybersecurity risk-management programs because they are best positioned to understand their unique mission environments, DHS works with the Office of Management and Budget (OMB) to ensure an adequate level of security enterprise-wide and to address systemic risks and interdependencies across and between agencies. DHS also supports agency efforts to reduce their vulnerabilities to cyber threats by providing tailored capabilities, tools, and services to protect legacy systems, as well as cloud and shared infrastructure

CISA's efforts are guided by three principles: 1.) risk-oriented, 2.) cost-effective and scalable, and 3.) leading and collaborative. DHS addresses the greatest risks first and focuses on the highest impact systems, assets, and capabilities. This means centering efforts around the most critical systems across the federal enterprise, including High Value Assets (HVA). CISA will be more engaged and focused on identifying and securing these systems. Cost-effective, scalable approaches will achieve the most risk reduction for the investment. Actions like policy changes, analysis, operational planning, and engagement can sometimes have greater cost-effectiveness than additional technical services or capabilities. CISA leads through direct action and offerings, but also through collaboration and communication with agencies and partners, such as OMB, the

General Services Administration (GSA), and the National Institute of Standards and Technology (NIST).

The *Federal Information Security Modernization Act of 2014* provided the Secretary of Homeland Security with the authority to develop and oversee implementation of Binding Operational Directives (BOD) to agencies. In 2016, the Secretary issued a BOD on securing HVAs, or those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. CISA works with interagency partners to prioritize HVAs for assessment and remediation activities across the Federal Government. For instance, CISA conducts security architecture reviews on these HVAs to help agencies assess their network architecture and configurations.

As part of the effort to secure HVAs, CISA conducts in-depth vulnerability assessments of prioritized agency HVAs to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which CISA network security operators send emails to agency personnel (with consent of the requesting agency) and test whether recipients click on potentially malicious links. CISA has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. CISA also works with the GSA to ensure that contractors can provide assessments that align with our HVA initiative to agencies.

Another BOD issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing systems that are most at risk from their exposure. The National Cybersecurity and Communications Integration Center (NCCIC) conducts Cyber Hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this BOD, CISA identified more than 360 "stale" critical vulnerabilities across federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, CISA has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified. By conducting vulnerability assessments and security architecture reviews, CISA is helping agencies find and fix vulnerabilities and secure their networks before an incident occurs.

When necessary, DHS can also issue emergency directives to federal agencies in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency. This year, CISA issued the first emergency directive after carefully considering the current and potential risk posed to federal agencies. On January 22, CISA directed federal civilian agencies to take a series of immediate actions in response to a global Domain Name System (DNS) hijacking

campaign. DNS is part of the global internet infrastructure that translates the names humans prefer, such as www.dhs.gov, to numbers computers need to access a website or send an email. The hijacking campaign by malicious actors allowed them to obtain access to accounts that controlled DNS records, allowing them to obtain decrypted data on the internet while looking normal to users. This risk necessitated quick action to ensure the security of federal networks, and we did not hesitate.

DHS's two primary federal network protection programs are the National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM). NCPS is an integrated system-of-systems that delivers intrusion detection and prevention, analytics, and information sharing capability for federal networks. NCPS primarily targets traffic flowing into and out of federal networks. One of its key technologies is the EINSTEIN sensor set. This technology provides the Federal Government with an early warning system, improves situational awareness of intrusion threats to federal networks, near real-time identification of malicious cyber activity, and prevention of malicious cyber activity. NCPS provides the technological foundation necessary to enable DHS to secure and defend federal networks.

The CDM program provides federal agencies with a risk-based and cost-effective approach to mitigating threats inside the network. The program fortifies the cybersecurity of government networks and systems by providing federal network defenders with a common set of capabilities and tools they can use to identify cybersecurity risks and threats within their network on an ongoing basis, prioritize these risks based on potential impact, and mitigate the most significant problems first. DHS works with individual agencies to assess their systems and networks, identify risk, and deploy the CDM tools and capabilities they need. By pooling requirements across the federal space, DHS is able to provide departments and agencies with flexible and cost-effective options to mitigate those risks and secure their networks.

The operational side of these programs comes together at CISA's NCCIC. The NCCIC provides entities with information, technical assistance, and guidance they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. The NCCIC operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The *Cybersecurity Information Sharing Act of 2015* (P.L. 114-113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. By focusing on rapid sharing of the technical features that permit network defenders to identify and respond to threats while minimizing the receipt of personally identifiable information, CISA's automated indicator sharing capability allows the Federal Government and private sector network defenders to share technical information at machine speed in a way that also protects privacy and civil liberties.

CISA's NCCIC provides a broad range of capabilities to assist private sector entities across all 16 sectors of critical infrastructure. In addition to information sharing and incident response, these capabilities include assessments and technical services as well as recommended remediation and mitigation techniques that improve the cybersecurity posture of our Nation's critical infrastructure. Among other services, these include vulnerability scanning and testing,

penetration testing, phishing assessments, and red teaming on operational technology that includes the industrial control systems which operate our nation's critical infrastructure.

Supply Chain Risks

There are also steps we can take to secure the actual hardware agencies use to build their networks and the software that runs them. Information and Communications Technology (ICT) is critical to every business and a government agency's ability to carry out its mission efficiently and effectively. Vulnerabilities can be exploited intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft, and insertion of malicious software or hardware. If these risks are not detected and mitigated, the impact to the ICT supply chain could be a fundamental degradation of its confidentiality, integrity, or availability and potentially create adverse impacts to essential government or critical infrastructure systems.

CISA recently launched the ICT Supply Chain Risk Management (SCRM) Task Force as a public-private partnership to mitigate emerging supply chain threats. The Task Force is the main private sector point of entry for our SCRM efforts and is jointly chaired by DHS and the chairs of ICT Sector Coordinating Councils (SCC). The Task Force is focused on supply chain threat information sharing, supply chain threat mapping and assessment, establishing criteria for qualified bidder and manufacturer lists, and incentivizing the purchase of ICT from original manufacturers and authorized resellers.

Election Security

One of the highest-profile threats we face today is attempts by nation-state actors to maliciously interfere in our democratic elections. Leading up to the 2018 midterms, DHS worked hand-in-hand with federal partners, state and local election officials, and private sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. This partnership led to successful implementation of a model that helps illustrate how CISA's cyber and critical infrastructure security missions complement each other, and the critical role CISA plays in bringing stakeholders at all levels together to address a common threat. We are now working to build upon these efforts during the 2020 election cycle.

Since 2016, CISA has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information. CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response. To ensure a coordinated approach, CISA convened stakeholders from across the Federal Government through the Election Task Force. The Department and the Election Assistance Commission (EAC) also convened Federal Government and election officials regularly through the Election Infrastructure Subsector Government Coordinating Council (GCC) to share cybersecurity risk information and to determine an effective means of assistance. DHS and the EAC also worked with election vendors to launch an industry-led SCC, a self-governed council with leadership designated by sector membership that serves as the industry's principal entity for coordinating with the Federal Government. All of these efforts enhanced

DHS's ability to identify, assess, and manage risks to election infrastructure in concert with state and local government partners and the private sector organizations that support elections.

Within the context of today's hearing, I will highlight CISA's efforts in 2018 to help enhance the security of elections administered by jurisdictions around the country, along with our election related priorities through 2020.

Assessing the Threat

The Department regularly coordinates with the intelligence community and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS engages with state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. Election infrastructure includes ICT, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

We also partnered with trusted third parties to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the National Association of Secretaries of State, and the National Association of State Election Directors. DHS field personnel deployed around the country furthered information sharing and enhanced outreach.

Enhancing Election System Security

During the 2018 midterms, CISA provided a coordinated response from DHS and its federal partners to plan, prepare, and mitigate risk to election infrastructure. CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure and ensure a more secure election.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and ongoing engagements, CISA will continue to work to provide value-added — yet voluntary — services to support their efforts to secure elections in the 2020 election cycle.

Improving Coordination with State, Local, Tribal, Territorial and Private Sector Partners

Increasingly, the Nation's election infrastructure leverages information technology for efficiency and convenience, but also exposes systems to cybersecurity risks. CISA helps stakeholders in federal departments and agencies, SLTT governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with SLTT governments, we work with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

CISA also works with the EI-ISAC to provide threat and vulnerability information to state and local officials. Through funding by CISA, the Center for Internet Security created and operates the EI-ISAC. The EI-ISAC has representatives co-located with CISA's NCCIC to enable regular collaboration and access to information and services for election officials.

Providing Technical Assistance and Sharing Information

Knowing what to do before a security incident happens, whether physical or cyber, is critical. CISA supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications is a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively when an incident unfolds. In some cases, we do this directly with SLTT jurisdictions. In others, we partner with outside organizations. We recognize that securing our nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission. CISA actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, CISA provides a report identifying vulnerabilities and mitigation recommendations to improve the security of systems connected to the Internet, such as online voter registration, election night reporting, and other election management systems.

Risk and vulnerability assessments: We have prioritized state and local election systems upon request, and increased the availability of risk and vulnerability assessments. These in-depth, on-site evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage election officials to report suspected malicious cyber activity to NCCIC. Upon request, the NCCIC can provide assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the Federal Government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information is shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Information sharing: CISA maintains numerous platforms and services to share relevant information on cyber incidents. Election officials may receive information directly from the NCCIC. The NCCIC also works with the EI-ISAC, allowing election officials to connect with the EI-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems. Best practices, cyber threat information, and technical indicators, some of which had been previously classified, have been shared with election officials in thousands of state and local jurisdictions. In all cases, the sharing and use of such cybersecurity threat indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with DHS policies protective of privacy and civil liberties.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to rapidly declassify relevant intelligence or provide as much intelligence as possible at the lowest classification level possible. While DHS prioritizes declassifying information to the extent possible, DHS also provides classified information to cleared stakeholders, as appropriate, and has been working with state chief election officials and additional election staff in each state to provide them with security clearances.

Field-based cybersecurity advisors and protective security advisors: CISA has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: CISA provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance helps train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device: www.dhs.gov/hometown-security.

Election Security Efforts Leading up to the 2018 Midterms

In the weeks leading up to the 2018 midterm elections, DHS officials supported a high degree of preparedness nationwide. DHS provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns. EI-ISAC threat alerts were shared with all 50 states, over 1,400 local and territorial election offices, 6 election associations, and 12 election vendors.

In August 2018, DHS hosted a “*Tabletop the Vote*” exercise, a three-day, first-of-its-kind event to assist federal partners, state and local election officials, and private sector vendors in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery. Through simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and election integrity. Partners for this exercise included 44 states and the District of Columbia; the EAC; the Department of Defense; Department of Justice; Federal Bureau of Investigation; Office of the Director of National Intelligence; NIST; National Security Agency; and the U.S. Cyber Command.

Through the “*Last Mile Initiative*,” DHS worked closely with state and local governments to outline critical cybersecurity actions that should be implemented at the county level. This effort partnered DHS with state governments to produce county-specific cybersecurity snapshot posters. The posters contained valuable information for auditors, staff and voters, including a checklist and timeline election officials should follow to ensure security of the elections in their county. For political campaigns, DHS disseminated a cybersecurity best practices checklist to help candidates and their teams better secure their devices and systems.

On Election Day, DHS deployed field staff across the country to maintain situational awareness and connect election officials to appropriate incident response professionals, if needed. In many cases, these field staff were co-located with election officials in their own security operations centers. DHS also hosted the National Cybersecurity Situational Awareness Room, an online portal for state and local election officials and vendors that facilitates rapid sharing of information which gave election officials virtual access to the 24/7 operational watch floor of the NCCIC. This setup allowed DHS to monitor potential threats across multiple states at once and respond in a rapid fashion.

Our goal has been for the American people to enter the voting booth with the confidence that their vote counts and is counted correctly. I am proud to say that our efforts over the past two years have resulted in the most secure election in modern history.

Election Security Efforts Moving Forward

Ensuring the security of our electoral process remains a vital national interest and one of our highest priorities at DHS. We will continue to prioritize elections by broadening the reach and depth of information sharing and assistance that we are providing to state and local election officials.

DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continued incentivizing the patching of election systems, and working with states to develop cybersecurity profiles utilizing the NIST framework. We will also continue to engage any political entity that wants our help. DHS offers these entities the same tools and resources that we offer to state and local election officials, including trainings, cyber hygiene support, information sharing, and other resources.

DHS has made tremendous strides and remains committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. In February, DHS officials provided updates to the secretaries of state, state election directors, and members of the GCC and SCC on the full package of election security resources that are available from the Federal Government, along with a roadmap on how to improve coordination across these entities. DHS also worked with our intelligence community partners to provide a classified one day read-ins for these individuals regarding the current threats facing our election infrastructure.

We will remain transparent and agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across SLTT governments, and state and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the Nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole of government approach. The President and this Administration are committed to addressing these risks.

Conclusion

In the face of increasingly sophisticated threats, DHS employees stand on the front lines of the Federal Government's efforts to defend our Nation's federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies, and is where CISA brings unique expertise and capabilities.

I appreciate this Committee's leadership in working to adequately resource CISA as we work to fulfill our mission. Your support over the past few years has helped greatly as we worked to bring federal departments and agencies into NCPS, speed deployment of CDM tools and capabilities, and build our election security efforts. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure and resilient Homeland while also being faithful stewards of the American taxpayer.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

Ms. ROYBAL-ALLARD. Thank you.

Director Krebs, in fiscal year 2018, Congress provided an additional \$26 million for election security efforts by the National Protection and Programs Directorate which is now the Cybersecurity and Infrastructure Security Agency.

Congress also provided \$380 million to the Election Assistance Commission to help secure elections through grants to states.

In the fiscal year 2019 appropriation we provided \$33 million to CISA to continue and expand its efforts. How did CISA use its fiscal year 2018 funds, and did you see a significant improvement in state election security efforts compared to the 2016 election, and to what extent is CISA able to coordinate with the Election Assistance Commission to better leverage the use of its grant funding?

Mr. KREBS. Yes, ma'am. Absolutely. I have said it before and it was an initial earlier draft of my opening statement, but I have said that 2018 was the most secure election held in the modern era here in the United States.

What we did with that \$26.2 million in 2018 was help broaden and build additional capacity in the agency. What I mean by that is additional risk and vulnerability assessment. So the actual technical services that are free, voluntary, and confidentially provided to state and local officials. So we provide those services that prior to 2016 had never happened. So let me give you a metric for example of why things were different in 2018 compared to 2016.

In 2018, we had deployed network intrusion detection sensors, and those are things that look for communication with malicious internet infrastructure. So for 2018 we had deployed sensors that covered about 90 to 92 percent of state and local networks that managed the voting process, 92 percent.

Prior to 2016 it was about 32 percent. That is a significant improvement based on Congress' recognition of our role and empowering us with part of the 26.2 million.

We were also able to conduct a number of exercises. In fact we had an exercise last August with 44 states and the District of Columbia. It was a 3-day exercise, had never been done before.

You had a hearing with FEMA yesterday. They do an exercise every year called the Great Shake-out, an earthquake-focused exercise. We are going to take the same approach every year, whether it is a presidential, a midterm or off cycle, we will do an election security exercise every single year to help support our state and local partners.

For the upcoming year of 2020, we will continue to build our capacity, continue to build the services needed to support state and local governments. In terms of the Election Assistance Commission, that \$380 million, we used some of the free services we provide through which we were able to develop an understanding of what the real weaknesses in state and local systems are, and we used that to develop with our partners in the state and local government guidance to help inform how they are spending that \$380 million.

Ms. ROYBAL-ALLARD. In May of last year the administration published a federal cybersecurity risk determination report and action plan. And the report stated that 71 of the 96 agencies or 74 percent that participated in the risk assessment process have cybersecurity

programs that are either at risk or high risk. And this strikes me to be pretty alarming.

And so the GAO noted in the December, 2018 report that they have considered Federal information security to be a government-wide, high-risk area since 1997. So we have been working on these issues for at least 22 years and yet it seems that our adversaries continue to outpace us in our efforts to secure our agencies' networks.

In fact, as you noted in your testimony just this last past January you issued the first emergency directive to Federal and civilian agencies because of another known cybersecurity threat. Can you provide more context about what the current federal cybersecurity risks are, and what kind of damage can this cause to federal government operations and to the public?

Mr. KREBS. Yes, ma'am. So my sense of things is that federal networks will always be a high-risk space because of the level of threat that we see in the cybersecurity space. The emergency directive is a great example of something that we, frankly, there was, as I mentioned in my opening, basically tampering with the internet's phone book, a simple way to put it. But it is not something that we had monitored for, that we were actually tracking because we hadn't seen it happen at scale.

As soon as we realized that it was happening, we were able to implement services and a set of recommendations to hardening infrastructure and improve monitoring.

Again, things are better than they were in 2016, so we are tracking a series of metrics of improvement. They are not measurements or metrics for success, because it is really hard to measure success in cyber security, even the highest organizations have difficulty with that. But we have demonstrable improvement in terms of the systems we are providing.

The thing we are focusing on right now is getting systems more secure by design and by deployment. And so, as I look to the work that Congress has done on IT modernization and that the administration has done on IT modernization that is an opportunity for us to make common investments to ensure that that the next iteration of what Federal networks are more secure, so we are not doing security by bolt-on.

Ms. ROYBAL-ALLARD. Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you, Madam Chairman.

Director Krebs, thank you again, sir. As I mentioned, I represent the Oakridge National Laboratory which includes a cybersecurity division. As I understand it this division does a lot of work with DHS, S&Ts, transition-to-practice program.

The core part of this mission is to bridge the gap between research and the private sector which requires a transition process that allows for technology to mature, and partnerships with the marketplace to form.

Through TTP, DHS S&T is leading the successful transition of federally funded cybersecurity technologies into broader use through commercialization and adoption by end-users. The TTP program has three main goals, identify promising technologies that address an existing or imminent cybersecurity need that impacts national security, increase utilization through partnerships, prod-

uct development efforts and commercialization, and finally, sir, to improve the long-term ability of the Federal Government research organizations to transition technology more efficiently.

My first question to you is what is the relationship between CISA and DHS S&T?

Mr. KREBS. Yes, sir, I have actually a very close working relationship with the senior official performing the duties of the Under Secretary which is the title I used to hold, Bill Bryan over at S&T, and through his revitalization process at S&T, we have shifted to a much closer alignment between what my requirements are as a network defender, a support element for network defenders and their actual research and development programs. We are seeing a much tighter alignment between what they go out and solicit for, and what my requirements are.

I have a small R&D budget, relatively speaking, along the order of, I want to say somewhere in the neighborhood of \$4.5 million. The cyber research and development budget at S&T is much, much larger. Again, we have to make sure that we are aligning and not just going off and doing good idea projects.

One of the areas of interest including working with Oakridge is the Silicon Valley Innovation Program that S&T has. I was just out in San Francisco last week and the week before and met with their folks. They have very good relationships with those innovators and the venture capital companies out in the Valley, that we can really tap into to get ahead of the next threat.

Mr. FLEISCHMANN. Yes, sir. As a follow-up to the question how is CISA working in coordination with DHS, S&T to leverage and deploy new technologies into the marketplace?

Mr. KREBS. So in part through the TTP process that you have mentioned. It is, again, it is identifying our requirements, what are the things we have identified that may be useful across federal networks, but also soliciting input from the critical infrastructure community and help sorting out what the opportunities are for research with S&T.

Mr. FLEISCHMANN. How is DHS, whether CISA or S&T or other elements, sir, leveraging the new cyber technologies coming out of our universities and national labs to protect our election cyber system, sir?

Mr. KREBS. So specific to elections, we work with NIST, but primarily the Election Assistance Commission has that core election relationship with the community, again, providing technology assistance or security assistance to those stakeholders.

One of the things that we just recently completed with one of our national labs is, as they were developing a technology we brought into our lab and worked with them on basically red-teaming or really breaking down the equipment and finding out through the design process what the vulnerabilities might be, so that when they deliver a product, it is secure by design.

Mr. FLEISCHMANN. One final question, what new technologies are being used to defend and monitor our U.S. election systems for cyber intrusions or manipulations, sir?

Mr. KREBS. So I touched briefly on the sensors that we have deployed, that DHS has deployed. But I do want to step back a little bit on election security, as we go out there and get a better sense

of what election offices and jurisdictions and the systems they have deployed look like, we are reinforcing the basics of patching, multi-factor authentication, training to spot what a phishing email looks like. It is really just focusing on the basics.

Sometimes a lot of the infrastructure even within the federal government is not mature enough to accept some of these new technologies that are coming out. So while we continue to look for new technology and security opportunities, it is really hitting the basics hard and that is going to be one of our focuses for Protecting 2020.

Mr. FLEISCHMANN. Thank you, Director Krebs.

Madam Chair, I yield back.

Ms. ROYBAL-ALLARD. Mr. Cuellar.

Mr. CUELLAR. Thank you, Madam Chair.

Director, thank you. Let me ask you about elections. I was the secretary of state for the state of Texas, so I got familiar with elections. And as you know, there are a couple of things.

One is when you look at the election infrastructure it covers so many things, whether it is ICT, capabilities, fiscal assets, technologies for the registration or the validation the casting, the transmission, the tabulation, the reporting of votes, the certification, the auditing, the verification of election. It is a series that you have to go through and there are always opportunities in the different steps.

Then on top of that you have got, for example, Texas has 254 counties. That is only the state of Texas. So how are you helping all 50 states, and then how do you go down to especially the small rural counties that say, nothing is going to happen here. How are you all doing that type of outreach? I mean is there a systematic way of doing this?

Mr. KREBS. Yes, sir, there is. So when we stepped back and looked at it there are about 8,800. I think the number changes. In some states there are up to 1,800 jurisdictions, voting jurisdictions in the states.

So we have to kind of look at this in a one-to-many approach. And so, what we do is work with secretaries of state like you used to be to reach out and down into the jurisdictions within each state.

So last year in the run-up to 2018, we developed, it was called the Last Mile Initiative. And basically it was a poster that went to each jurisdiction in participating states. And I think at this point we have 33 participating states, but we knocked out 19 states in the run-up to 2018, and that is the states that wanted to do it, we got through 19. And that is it is awareness building.

So it is here are the threats, here are the potential risks in the election process. It really is like you said, a system of systems. Here are the things you can do to address and mitigate those risks, and then here are the resources available from the federal government including signing up for the multi-state or the Election Infrastructure Information Sharing and Analysis Center to do, sign up for a cyber hygiene scan, to participate in an exercise.

So it is really, first and foremost it is increasing awareness and then bringing them into some of the free voluntary services that we provide.

Mr. CUELLAR. So do you have an idea, you said 88?

Mr. KREBS. It is about 8,800, and in the run-up to 2018 we were able to work with 1,400 of them, and our goal, our top priority for 2020 is extending and broadening that reach.

Mr. CUELLAR. So 8,800, you have covered 1,400?

Mr. KREBS. Yes, sir.

Mr. CUELLAR. So how do you reach the rest?

Mr. KREBS. Persistence, persistence, yes, sir. It is, again, we started from a common denominator pretty much of zero. In 2016 there was no relationship between the Department of Homeland Security and state or local election officials. We are starting from scratch.

Last February we, working with the election community, established the Election Infrastructure Information Sharing and Analysis Center or the ISAC. And at that point I believe it is about 1,500 local members in all 50 states. That over the period of time that that developed, that is the fastest growing ISAC of any other sector. So there is progress, there is commitment, but this does not happen overnight.

And the one thing that I have found that is most critical and you can't buy it, is trust. So we have had to put an enormous amount of boots on the ground time, out across the United States to meet, to work, to do exercises, to have a cup of coffee and just get to know these folks and let them know who we are and what we do, and that we are not here to take over elections. We are here to make sure that their elections go smoothly, go safely and go securely.

Mr. CUELLAR. Thank you so much.

Mr. KREBS. Thank you.

Ms. ROYBAL-ALLARD. Mr. Newhouse.

Mr. NEWHOUSE. Thank you, Madam Chair.

And welcome, Director Krebs, I appreciate you being here. You made the statement that 2018 was our most secure election so far, and that is a great statement to be able to make. So thank you for your efforts to make that happen.

Ms. ROYBAL-ALLARD. Excuse me, Dan. They are having trouble hearing us so we are going to have to speak up a little bit and get closer to the microphone.

Mr. NEWHOUSE. So eat the microphone. I appreciate your efforts to make our elections more secure. I think the American public really wants that and appreciates the government's effort to do that, and so, just a couple of questions surrounding that.

You have been with Mr. Cuellar's line of questioning, touching on a lot of that as some of the others too but you made the points. I think you laid out three general things that you are going to do to work on for 2020. So I wanted to give you an opportunity to expound on that, so we will be able to come back in 2 years and say that 2020 was the most secure election we have ever had.

And then also as we talked about before the meeting stated, the whole subject of security clearances, is that impeding agencies' work, your work, and is there anything that we can do to help in the whole area of making sure that clearances are provided to the right individuals for the right levels, so just a couple of enquiries there?

Mr. KREBS. Yes, sir. So on priorities for 2020 I created a new hashtag last week at a conference out in San Francisco. We are calling it Protect 2020. I mentioned it in my opening.

We have three primary areas of focus. One is increasing that reach, getting as close to 8,800 as we can possibly get by 2020.

The second one is really getting to the bottom of where is the risk in the system of systems that is elections. Part of that though is understanding that we still need to really focus on the basics, and so, that is why we are prioritizing organizations really improving patch management. You still find that systems out there are either legacy or old systems that haven't been patched recently and are still open vulnerability.

And as we increase that reach, as we increase this understanding of where the risk is, we are also going to develop and have already developed tools that we can drop on top to say I am working with you now, we understand what your risk is, I have this capability. I can scan the internet facing systems of any organization, and we require it across federal government, but I can do it with state and locals, and tell them you haven't patched that system and that is out touching the public internet. That is probably vulnerable and it might be a good way for a bad guy to get inside. So you may want to take care of that.

And the third piece is once we get our understanding of where the real risk is, informing the conversation on the Hill and state capitals, on the resources whether it is people, equipment, funding, whatever, of what it is going to take to get these systems to where they want to go. That is probably the biggest policy conversation ahead of us, is what it is going to take to get these systems where they need to be and who is going to pay for it?

On the security clearances piece, the process of security clearances has always been a bit of that albatross over the Federal Government. It takes a little too long for the highest level of clearances. I think it is in the 17-month period. Fortunately, the Department of Defense is prioritizing and focusing on that. I have all the confidence in the world that they will be able to knock down those wait times.

At the same time we can do things to make our lives easier. We can declassify and we can stop over-classifying. So I have certain authorities that I can read people in and give them short term clearances. I also have declassification authorities in certain spaces. So we need to be looking at this problem from both ends.

I do have the ability and actually the honor of sponsoring a program called the Private Sector Clearance Program, where from across the 16 critical infrastructure sectors, I can sponsor clearances for network defenders and other security officers. And that is something that we take very seriously and we are looking to streamline that process as much as possible. But again, keeping in mind that having a security clearance is not a silver bullet and there is not necessarily a treasure trove of information on the other side of that wall.

Mr. NEWHOUSE. Keeping it in mind that we don't want to compromise any systems in place.

Mr. KREBS. Absolutely, yes, sir.

Mr. NEWHOUSE. And one of the difficulties I would imagine is with the election system you have got 50 different systems out there, right?

Mr. KREBS. Well at least. Congressman Cuellar mentioned that Texas, Texas, 283, is a bottom-up state, home rule, all that. And so, you are having purchasing decisions happening at individual county levels. It further complicates it.

But back to the clearance piece really quick. A lot of what makes information classified, particularly at that much, much higher level that network defenders don't need. They don't need the sources and methods. They really want to know the tactics, the techniques and the procedures against which they can defend themselves.

Mr. NEWHOUSE. Again, thank you for being here. I appreciate it. Thank you, Madam Chair. I yield back.

Ms. ROYBAL-ALLARD. Okay.

Mr. Price.

Mr. PRICE. Thank you.

Welcome, glad to have you before us. I appreciate your testimony. I want to ask you to elaborate a bit more on your staffing successes, and I am referring here of course to the IG report last month that indicates that it has, staffing has been a hindrance. And that to secure our election infrastructure we need to pay attention to that.

I know you are paying to it, but I wonder what kind of progress you can report between department leadership changes and a prolonged management vacancy in CISA and insufficient resources.

The inspector general has reported that DHS' efforts to complete its election infrastructure planning have been delayed. The inspector general also found that CISA did not have enough dedicated election infrastructure staff and that you have not clearly delineated the roles, responsibilities and procedure that the staff should have. I am sure you are familiar with this.

As many have said, we are clearly approaching the 2020 election season. It is critical to ensure that our infrastructure for these purposes is properly supported. So a couple of questions.

What steps are you taking, have you taken to hire more dedicated election infrastructure staff and to finalize the detailed strategy in advance of the 2020 election cycle? And of course are there ways that we can or should assist you in achieving the staffing goals?

Mr. KREBS. Yes, sir, thank you. As I mentioned in my opening, in 2018 and the run-up, over the course of let us a month or so we had over 550 employees within the Cybersecurity and Infrastructure Security Agency working election issues.

Was that every single day? No, because we are not election administrators, we are not election experts. State and locals are not looking to me to help them understand how to run a better election. What they are looking to me for is cybersecurity advice and physical security advice.

And so, when I talk about dedicated election staff, when we started in 2016, when we stood up our program for election infrastructure we had zero election infrastructure specialists. We established a task force that brought in detailees from across the, in some cases the Administration but primarily the Department of

Homeland Security. And then over time as we were running up and surging into the election, I was also building institutional capacity so that I don't have to have a taskforce, I have a sustained, sustainable program.

We made a series of strategic hires. We are still making strategic hires. I actually hired someone off the Election Assistance Commission who is a renowned election security expert. We just recently brought in through a support mechanism, through a contract a local election security expert. So we are building that core that sits here in the national capital region that more than anything, they are kind of air traffic controllers for getting security resources out to state and local governments.

Again, I have got over 200 people in the field at any given moment and I can bring that number up and down based on what the threat is, but at any given point, I have got somebody out there in the field doing elections and that will only increase, that will only surge as we run up to the 2020.

Reinforcing the importance of this mission in DHS and CISA through appropriations, 59 million between 2018 and 2019 is huge, because I am building capacity that is here to stay, that is sustainable.

In addition, that is building capacity that can go shift to other threats as they emerge, whether it is the grid, whether it is another industrial control systems issue, we are building depth. The highlight for me beyond the fact that it was the most secure election in modern era, is that I used elections to better coordinate across the interagency with the Department of Defense and the intelligence community, so not just we are better for elections, we are better for every other critical infrastructure sector.

Mr. PRICE. Well, I appreciate that and it is hard for someone in our position to assess this simply because we are not certain what standard you or the IG is measuring staff adequacy against. So maybe I could just focus it as my time is running out here.

Focus a little more on your assessment on that report, I mean do you accept the implied benchmarks that the IG was using, the implied staffing levels that would be optimal, or do you differ from that and either way, what remains to be done as far as you are concerned?

Mr. KREBS. I think there may be some differences in management style and how to execute in a highly dynamic threat environment. I am not focused necessarily on building static staff, I am focused on building broader capacity, that as the threat environment shifts, I can bring to bear all the resources necessary.

So, I think we did a pretty darn good job in the 2018 election, I think the results prove it, I think our stakeholders would support that and we are only going to continue our approach as we go forward into 2020.

Ms. ROYBAL-ALLARD. Mr. Rutherford.

Mr. RUTHERFORD. Thank you, Madam Chair. Thank you very much for being here this afternoon. You know, it seems like in this cyber world, if we look at the attacks on systems, private industry and others, I am curious how much self-defense if I will call it that, how much self-defense are businesses allowed as far as responding to and attacking those who are attacking them?

Or is it always just blocking, are we never punching back and who makes that decision?

Mr. KREBS. So while I may have legal training, I am not necessarily an expert in the CFA, the Computer Fraud and Abuse Act and some of the other legal pieces.

What we focus on is network defense, the blue team side. And so, yes, in some cases it could be perceived as taking punches, but it is hardening the things we know they are going after. So——

Mr. RUTHERFORD. But do we ever respond to those sources that are attacking us?

Mr. KREBS. That is——

Mr. RUTHERFORD. By trying to take them out?

Mr. KREBS. That is the domain of the Department of Defense and I am sure in a different setting they probably would be happy to talk about those issues but we are purely on the defense side. And sometimes I kind of liken us to the geek squad or whatever. You know, we are there to help those that own the networks, that own the infrastructure be better.

Mr. RUTHERFORD. Okay. And so——

Mr. KREBS. Yes, sir. There is certainly a role for levying consequences though against foreign adversaries and that is, again, I mentioned that Department of Defense there are already a range of tools, there are sanctions, indictments, other diplomatic actions, there are a range of tools. But CISA we are purely on the——

Mr. RUTHERFORD. You are not focused on that.

Mr. KREBS. Network defense.

Mr. RUTHERFORD. So, as you have gone through a great 2018 cycle and you are looking at different election software, hardware, is there a list that CISA is saying, This stuff really works well. Hey guys, don't use this again, it doesn't work well. Is there an evaluation system that you are making available to the different states and localities?

Mr. KREBS. So under the Help America Vote Act from the last decade, the Election Assistance Commission is responsible for working with NIST and other organizations, they have a certification process and this is the equipment that EAC has certified. Each state legislature and in some cases local under Article I Section 4 of the Constitution is then responsible for administering the elections.

Each state has their own process for how they use that certification list, how they do testing, every state is a little bit different but——

Mr. RUTHERFORD. But they are there for the——

Mr. KREBS. Yes, sir. And so we do work with EAC and NIST on providing technical expertise. One of the areas that we are focusing on right now is as equipment is being developed because new equipment is always in the development process, working with vendors to help them, again, secure their equipment by design.

Mr. RUTHERFORD. I can't tell if I have any time left. In the other 16 categories, energy I guess is one I am sure. How are we doing in those fields as well? Have you seen a lot of tremendous improvement here in the last couple of years? Since CISA is kind of starting to pull everything together it seems like.

Mr. KREBS. So, I think every year there is increase awareness of the threat. Just I mentioned last week I was at a conference in San Francisco, it is the largest cybersecurity conference in the world.

The general feel, the sense is that things are a little bit better, primarily because of the decision makers, the executives, the people that own the risk, that manage the risk, the CEOs, the governors, the boards, the general counsels, they are highly attuned to what the threat is and what their risk is, and so they are focusing resources to address the risk.

But, the basics are still hard, configuring systems the right way, patch management, enabling multifactor authentication. The basics are still hard to do and we are going to keep hammering on the need to do the basics until the basics get done and then we will move on to the hard stuff.

Mr. RUTHERFORD. Two and a half, three years ago we were I think really behind the curve.

Mr. KREBS. Yes.

Mr. RUTHERFORD. How much better do you think we are now than we were three years ago?

Mr. KREBS. So I mentioned in my opening that I like using the federal networks as a good baseline because I can actually really measure that quite well.

Prior to 2015, the average time to patch a critical vulnerability was something on the order of 219 days, now it is averaging about 20 days, and I bet we can probably do better than that too. That is dramatic improvement. That is dramatic. And if you can't measure it, you can't improve it so we are continuing to look for what those indicators of improvement are.

Mr. RUTHERFORD. Well, you guys keep up the great work. I appreciate what you are doing.

Mr. KREBS. Thank you, sir.

Mr. RUTHERFORD. And I yield back, Madam Chair.

Ms. ROYBAL-ALLARD. Mr. Aguilar.

Mr. AGUILAR. Thank you, director. I know what it is like on this side of the table now, you are doing well here. I will testify to Mr. Fleischmann and Ms. Roybal-Allard. No, I am okay at my current position, thank you. Thank you, congressman, appreciate that.

Director, I wanted to drill down a little bit more, you have been talking about obviously the importance of measuring these connections and these touches, 8,800 jurisdictions total, you said you have worked with 1,400. Can you classify the nature of that? Can you tell us a little bit more and drill down, those 1,400, did they come to you and seek support? Were those ones that you proactively went to? And how would you describe those 1,400 touches? Is there any one area that jumped out more?

Mr. KREBS. You know, it is hard because every state is different. It is hard to really characterize of those 1,400 what the buckets are. But in some cases, give you an example, there is a state down south that required at the state level, all counties to sign up for the election ISAC and sign up for our cyber hygiene scan, that external internet facing scanning capability.

And right off the bat, I got a bunch of, my participation level went up. So, we focus in the run-up to 2018 on building relationships and a level of trust and comfort with the state elections be-

cause we understand they have roles of positions of authority in their states.

But, again, not every state is the same. So we look for opportunities through other one to many communities, whether it is advocacy groups or associations of election officials. But sometimes it is really just about getting out there and going to various meetings, not necessarily in the big cities, but sometimes it is getting on a commuter plane and going to county level meetings.

Mr. AGUILAR. Sorry to interrupt, but can you call the state elections officials in other states and tell them to share that exact story?

Mr. KREBS. We absolutely do. But their ability to influence, so in Texas for instance, it is more of an advice role from the state election director down. And that is just the way elections are run right now. So it is, to us it is about awareness, awareness, awareness.

Mr. AGUILAR. Okay. How do you ensure that those local jurisdictions then follow through? So let us use that as the example that one that reached out that had others sign up for hygiene, the checks? How do you ensure that they are using that appropriately and if that isn't just one person getting the training and then that person moves on or retires in two months. How do you ensure continuity?

Mr. KREBS. So on the hygiene scanning, that is a biweekly thing, right? We do it every week, it just kind of rolls through, they get a report. And then from there it is persistence, it is following through, it is following up with touch points.

And we can look at some of these things and say this one looks particularly concerning, are you taking care of it? So, again, to a certain extent it is almost risk-scoring what the results that we are getting back are.

Mr. AGUILAR. As you are doing analysis and as you are looking and saying, okay, this one looks a little risky, this jurisdiction these things jump off the page, how many would you classify in a high risk category of they should be contacting your and they should be working with you or are they should be doing things that they are doing, what would you call that category and how many do you think would fall into that?

Mr. KREBS. I don't know if I have a name for it, but what I am looking at right now and I mentioned and used auditability. So there are five/six states right now that are of particular concern, five states entirely don't have voter-verifiable paper trails. So South Carolina and Georgia, Louisiana, New Jersey, and Delaware, everybody knows this, this isn't classified, they know it.

They don't have a paper record, it is all machine-based. Pennsylvania has about 83 percent I think of their voting population, vote on machines, they don't have the paper trail. So those are areas of particular concern. And my primary focus and area of encouragement would be get them off those machines onto something that produces paper that leads to an auditability outcome.

The good news is all five of those states and Pennsylvania, Pennsylvania legislature I think passed a bill that said, Thou shall do this by the 2020, those other five, they are all on the path. They have all either demonstrate it through legislative action, through

a procurement action, or whatever, they are all moving that way. So we monitor, engage, continue to help along.

Mr. AGUILAR. And would you say those five deserve a little bit more discussion and help along the way to verify that they are getting there from an auditability perspective of paper ballots?

Mr. KREBS. So on the verification side, I am more thinking about how do we get them there? And that is going to be technical assistance, there is going to be a resource question, some states may not have budget it appropriately to get that done, particularly by 2020. So whatever we can do to help them get there is what we are focused on.

Mr. AGUILAR. Thank you. Thanks, Madam Chair.

Ms. ROYBAL-ALLARD. Ms. Meng.

Ms. MENG. Thank you for being here today and thank you to our chairman and ranking member for holding this important hearing. I wanted to ask about STEM education, I am concerned that our nation's education institutions have not been keeping up with the pace of our growing need for cyber talent.

For the past several years DHS has partnered with the National Integrated Cyber Education Research Center to provide K through 12 cyber security curricula and hands-on professional development for teachers. I know that the center has been funded through a series of DHS grants since 2012. Last year it got \$21.5 million for a period of five years. What metrics does your agency use to assess the effectiveness of this program and other similar DHS-funded programs?

Mr. KREBS. So on the CETAP program, last year I believe was \$4.3 million, we have 12,000 educators in the program across 11 states and they are able to engage 1.8 million, I think it is 1.8 million students.

That is good, that is not good enough. There is a role here for everyone, it is a whole of nation effort. So we continue to work with foundations, the private sector, large companies that are invested in ensuring that when they get into hiring actions 15, 20 years from now that they have a pipeline.

So there are a number of efforts afoot right now, there is the National Cyber Education Program I think is working with Discovery Education. We are looking at ways that we can partner with other efforts recognizing that Congress doesn't need to be footing this bill entirely that, again, this is a whole of government approach.

And I have got to say that I am as invested in this, this is probably the thing I am most passionate about across the portfolio. I have five kids that are in or will be in the public education system here in Northern Virginia and I know what the offerings are right now, and then I have to pay for after school programs. You know, that is one way to do it but I think we have to mainstream STEM education much, much better than we are. And, again, there is a role for everyone, not just government, but the private sector as well.

Ms. MENG. Thank you. And do you think the curricula of this center and this program or just programs in general, are they preparing them properly to fit the needs of what our country's actual cyber security workforce needs?

For example, we have heard random stories about the kids who are studying this curriculum, but don't necessarily match the needs of actual programs or what the workforce is in the government or whatever the needs are, that they don't necessarily match with their learning. Is that something that you have seen or?

Mr. KREBS. So, I don't believe I have done a specific audit of the curriculum against what the hiring requirements are for the federal government, recognizing that the federal government cyber security workforce demands are quite diverse.

It is more of a general STEM education-base that they can go into any technology field including cyber security. To me, I think there is some sense in making sure that sound development processes are focused on, rather than purely on cyber security because there is a certain fatalism associated with it is always going to be insecure, so we have to have cyber security expertise.

I want to put a lot more focus into secure by design, secure by design, that way we don't need to worry so much about the big apps on the cyber security side.

Ms. MENG. And my other question is about shortages of qualified cyber security professionals already in the federal workforce. Workforce recruitment and retention has been challenging, especially when competing with the private sector.

Cyber security professionals and the federal workforce are paid by the GS level system and maybe you offered a recruitment or retention incentive of up to 25 percent of their basic pay but there are still difficulties in staffing. Is CISA looking into maybe a new pay scale for cyber security professionals and are you taking steps to recruit and retain some of these professionals?

Mr. KREBS. So a couple of years ago, Congress passed a law that directed us to pull together this program and we are in the final stages of developing, that program is called the Cyber Talent Management System.

And the point behind the system is that the GS approach the government uses right now for hiring is not tailored to the unique education, certification, approaches, processes, whatever for the cyber security workforce. And kind of the point is, if I have someone that goes to a two-year college or maybe no college at all and yet has demonstrated experience where they could be incredibly technically proficient at 22, 10 years' worth of experience effectively, how do I account for that?

Are they a GS4 or a GS11? You know, by the standards that we have in place right now, I can't reward that person and pay them the way they could be paid in the private sector. So it is about balancing the way that we can bring people in.

That program, we should be making our first hires under that program this year. We will have to have a transition between the current system and the new system, but in the meantime, we are looking at what you mentioned, the 25 percent retention rates, we have a very exciting mission. So it is about making the job that much more exciting for them in the meantime.

Ms. MENG. Would that apply to returning the federal employees too, if they have gone to private and want to come back?

Mr. KREBS. Absolutely. Absolutely. You know, there is a program called Scholarship for Service where current college and graduate

students, I want to have dedicated pipelines in the Nation's colleges, universities of all sizes and stripes and be able to bring in steady drumbeat every single year.

And if they come in, they work for me for 5 or 6 years and they go out to the private sector, I am okay with that. I am okay with that because they know who I am and they know how to work with me and they will come back.

Ms. MENG. Thank you. I yield back.

Ms. ROYBAL-ALLARD. Mr. Ruppertsberger.

Mr. RUPPERSBERGER. First of all, I am glad you are here. I think you are on the right track. I know we had a meeting and I just want to make sure that you have the resources to do the job, because it is a big job and we have a long way to go. And once we get where we are, we have got to keep innovating, you know that.

I am going to get into the area of trusted internet connections. On one area I have a concern with the modernization there. The goal of this program is to consolidate department and agency connections to the internet. And the general theory is that if the federal government has less connections to the internet, then our intrusion, detection, and prevention capabilities like Einstein, which it helps us to detect and prevent common cyber attacks will be more effective. Do you agree with that?

Mr. KREBS. In the traditional on premise environment, Yes, sir.

Mr. RUPPERSBERGER. Okay. Now first, can you give us an update on the TIC modernization and how many TICs does the government have and what is your goal?

Mr. KREBS. I will have to get back—

Mr. RUPPERSBERGER. It is kind of in the weeds, I know.

Mr. KREBS. Well I—

Mr. RUPPERSBERGER. It is important to get it on the record.

Mr. KREBS. The thing that I was alluding to in my initial response is that in the traditional or historic on premise environment of having a server room and having a data center where you know where the equipment is and you can really sit on the pipes and focus them down, TIC was important.

Going forward, as particularly we shift through IT modernization to Cloud because Cloud is efficient, it is scalable, it is flexible to meet modern workforce demands, TIC won't work because TIC actually undermines the low latency and high speed and flexibility of the Cloud.

So what we are doing is shifting to a model in a series of pilots right now where instead of me putting an Einstein sensor in—

Mr. RUPPERSBERGER. Explain to the committee what Einstein is.

Mr. KREBS. Einstein is, well, one of three things, it is an intrusion detection system, so you can kind of see the bad stuff that is coming in and out and then the intrusion prevention system which filters email, which if you see the bad traffic, it actually stops it and diverts it to another space.

The problem is you have to sit on that pipe to look at the email and the net flow, and the traffic and how it is working. But if it goes to the Cloud, the whole point of the Cloud is you have this distributed environment with traffic bouncing back and forth.

So the alternative model which in the end will actually be more efficient and save the taxpayer money because we are not owning

the infrastructure, it is we are setting a set of outcomes, security outcomes and requirements for the Cloud provider, saying, this is the kind of information we need, you guys need to send it back to us and then we can analyze it.

So it is not about putting the equipment out and looking at it as it goes out, instead it is they have got it, they will tell us what they are seeing, and then we can alert on that.

Mr. RUPPERSBERGER. You know, counter to the idea of reducing the connections to the internet, the federal workforce is actually moving in the opposite direction, and with more and more employees working remotely which is the future, by the way, and off of the cellular devices and tablets.

Now, there is a large push in the government to consolidate our Cloud infrastructure as you talked about to further reduce our attack surface, would you agree to that?

Mr. KREBS. Yes, sir.

Mr. RUPPERSBERGER. Okay. All right. How is CISA adapting its network security strategy to the changing federal workforce, and do you intend to start incorporating more endpoint protection and endpoint detection in response to protect the users at the edge of the network? Did you understand what I just said?

Mr. KREBS. Yes, sir. So through the Continuous Diagnostics and Mitigation program that we rolled out a couple of years ago, we are going through a capability enhancement, basically the life cycle.

And we historically called them phase one, phase two, phase three, phase four. What we are finding now is that it is better to go through phases based on the capability of the organization. Some agencies are just more sophisticated than others.

But to your point, we are really focusing what the next couple of years look like for mobile and for Cloud. Some agencies are going to be able to take some of the Cloud and mobile capabilities sooner than others. But it is in the CDM lifecycle or the phased approach.

But as I mentioned, we are ultimately going to shift from a model where we own the infrastructure, we own the sensors and instead, we are putting out a baseline policy and a series of outcomes that we are looking to achieve. And so we have everybody playing by our rules rather than we are doing the operations and maintenance on equipment, and ultimately I think we are going to be more effective and I think we are going to be able to do it faster and I think we are going to be able to use the private sector's agility to get those better secured outcomes.

Mr. RUPPERSBERGER. And you are going to need more resources and money, so it is so important you maintain this relationship with our committee and our staff, so we know where you are going to be next year and the year out, because this is going to get more difficult and it has more needs as we move to the future.

Mr. KREBS. Yes, sir. Thank you.

Ms. ROYBAL-ALLARD. We have been joined by the chair of the full Appropriations Committee, Ms. Lowey.

The CHAIRWOMAN. Thank you. I don't have my roller skates on but there are a lot of hearings going on at the same time today.

Mr. RUPPERSBERGER. I like to see you in roller skates, you are pretty good.

The CHAIRWOMAN. I will show you pictures of me—

Mr. RUPPERSBERGER. Okay.

The CHAIRWOMAN. When I was 8. At the age of 8. Excuse me. First of all, I would like to join my colleagues in welcoming you, Director Krebs. DHS' inspector general released a report about the department's efforts to secure our nation's election infrastructure.

According to that report, state and local officials' rampant mistrust to Federal Government assistance critically harmed the DHS's ability to secure election infrastructure. I understand that some states are sensitive to what they perceive as Federal overreach into their election systems, however, integrity and trust in our election processes are fundamental to our democracy at every level. And I know you face significant challenges in threading the needle.

In 2017, election infrastructure was brought under the government facilities critical infrastructure sector within DHS. I would be interested to know, how did that move change your relationship with state and local governments?

Mr. KREBS. Ma'am, prior to that designation, that was before I came on board in March 2017, I think Johnson made that on January 7, 2017. The easy answer is relatively just prior to that designation, there really was no relationship.

So it probably got worse as a result of that designation, but there wasn't much further down to go from there. So what I have focused on since day one of March 2017 is getting us to a place where we have a trusted relationship with state and local election officials.

The CHAIRWOMAN. I would be interested in knowing how does CISA work with entities like the Multistate Information Sharing and Analysis Center, the Election Infrastructure Information Sharing and Analysis Center, the Election Taskforce, and others.

Mr. KREBS. So the multistate information sharing ISAC, it is based in Albany, New York. It is an organization that we actually fund through a grant or contract, and they provide resources to state and local governments. A lot of the tools and capabilities in some cases that we provide to federal agencies, they are able to provide out to state and locals.

The MS-ISAC as we call it, they started, founded with state and local officials the EI-SAC, the Election ISAC. So we work with them day in, day out, throughout the 2018 election in the run up, we provided technical alerts, we provided intelligence, we provided basic trend analysis of what was going on out there in the world, and they were able to send to their members.

By the election, they had 50 states, all 50 states and 1,400 election, local jurisdictions participating in the ISAC which is a historic number relative to any other sector. Now, bad news is there are 8,800 or so jurisdictions, so we still have room to go, but we started from zero and I think we have made pretty good progress and we will continue to focus there for 2020.

The CHAIRWOMAN. That is really impressive. So I just wonder how we can continue to improve these relationships and how do you address the concerns that some state and local governments have about working with CISA like federal overreach? How do you deal with it? How do you build confidence?

Mr. KREBS. You know, it doesn't happen overnight. It is investing a lot of personal time, a lot of miles out there. I spent a good deal

of last summer in the run-up and actually pretty much all of 2018 out there on the road, just meeting with secretaries of state, meeting with local officials, letting them know that we are here to help.

We are not here to take anything over, we just want to make sure that they are successful in their jobs as election administrators. But really, it is all about trust, it is all about letting them know that we are here to help, and when I get the question of how do you think you did, I sometimes get a little uncomfortable in asking that question and say particularly if I am testifying in front of an authorizers panel and I am next to a state election official and say, I don't know, ask him or her.

And generally speaking, I think the response has been pretty good across both sides of the aisle. This is not a partisan issue, I take a nonpartisan approach and I think, again, the proof is in the participation.

The CHAIRWOMAN. And what percent is left that you haven't been able to interact with?

Mr. KREBS. So on the local side, I am not a math guy, right? But we have worked with over 1,400. So we have got a big number left out there. 7,400.

So we will get there and it is just going to take time, it is going to take boots on the ground work, it is going to take advocacy. You all actually have a role as well when you go home, when you go back to your districts, if you can work with your counties, if you can work with your voting jurisdictions and say, hey, are you working with DHS? Are you working with CISA? They are here to help you, they are not taking anything over.

The CHAIRWOMAN. And I wonder about is with all the talk today, cyber security and the past election and who leaked what to who, I don't want to get into that stuff today, but I who I am not an expert in all that stuff.

Believe me, I just worry who is dreaming up the next challenge for the next election. Do you get into any of that stuff?

Mr. KREBS. Absolutely. That is what keeps me up at night. I know what they did in 2016, I know what they tried to do in 2018, what are they going to do in 2020? So we have got to make sure that we are covering down on the basics.

We have got to make sure that they can't get in through the last approach, and try to be a little creative. The one way that we are going to be able to do this is we have to engage the American public, we have to let them know that there are bad people out there that try to do bad things, but you know what, we have got a system here that works and we are doing everything we can to protect it, we have to restore faith and confidence in the American people that this is not a system that is about to tip over and fall down. That we are doing the right things and I think we are going to be successful.

The CHAIRWOMAN. I hope so. I wish you good luck.

Mr. KREBS. Thank you.

The CHAIRWOMAN. But I think those are the questions that really—

Mr. KREBS. Yes, ma'am.

The CHAIRWOMAN. Keep me up at night because so many of us were blindsided. We still don't have all the facts, although the facts

may be out there but they are not believed across the board, across parties and I just think this is so serious and we really have to work in a bipartisan way and figure it out.

Mr. KREBS. Yes, ma'am.

The CHAIRWOMAN. Thank you very much. Thank you.

Ms. ROYBAL-ALLARD. I think it keeps a lot of us up at night.

Okay. That completes the first round. So we are going to go on to the second round. And I would like to go back to the federal cybersecurity risk. You talked a little bit about the obstacles that you face in getting ahead of our adversaries.

But what I would like to ask you is, are agencies appropriately prioritizing their budget request to ensure these risk are mitigated and to the extent that funds are budgeted for this purpose, are they being used effectively, and would more funding help in this effort?

Mr. KREBS. So I do think that with more we can do more, but we—we have to get back to the question of the basics. We continue to have outdated legacy infrastructure out there, and with the turn—the changeover in the administration, one of the statistics was there is \$60 million being spent on Federal IT and about \$40 million of it was operations and maintenance, and a lot of that is keeping legacy systems up and running.

We have—we have got to get out of this model where we are just paying to patch and paying to keep the old stuff running. We have got to modernize. But that is—but that is in and of itself not going to fix. I am excited about the IT modernization efforts, because it means we have an opportunity to shift from the security bolt-on mentality where I am adding security solutions on top and instead, we can design and configure and deploy IT secure—securely.

Now, the remaining challenges that we have at least in the civilian non-DOD, non-intelligence community space, we still have decentralized model which means every agency and 99 some odd agencies, every agency is responsible for their own IT and their own security. So what we are focused on right now, working with OMB, is defining what a security baseline looks like for all agencies, centralizing services.

Some agencies just can't do the job, so I can help them do it for them, identifying and enforcing policy to ensure consistency of approach. Again, the more that we get into a centralized approach and that is not just on the federal, the executive branch side, but also on the congressional oversight, there is still decentralized oversight, decentralized budget and appropriations, if we can bring it all together, if we can bring it all together, that is going to be make it much easier to manage.

Ms. ROYBAL-ALLARD. Director Krebs, you mentioned in your testimony under the heading supply chain risk that you are taking steps to secure the actual hardware agencies use to build their networks and the software that runs them. Can you describe what these risks are and where they come from? And have you encountered issues on any federal networking resulting from this type of risk?

Mr. KREBS. So this is the emerging issue right now that I have found, it is supply chain risk management. It is really, really hard because of the lack—the lack of transparency in whether it is hard-

ware or software, firmware of the build process, who is four, five, six layers down.

We have encountered software or—or supply chain challenges and vendor management challenges over the last couple of years. Congress passed a bill last Congress on federal supply chain security that set up a federal acquisition supply chain council, so thank you for that. It is an important process that is, from our position will address some of the issues that we experienced during the Kaspersky binding operational directive process. So yes, we have experienced issues in the federal government, Kaspersky was one of them. We identified it as a threat or as a risk to information security, risk management posture, and we eliminated, we removed it, required the removal from networks and Congress subsequently mandated by statute.

So we are in the early days of figuring out what supply chain risk management looks like for the federal government and we are implementing the legislation, the statute. There will be a council stood up, DHS will be a key member, we will look at the standards, the processes. There will be adjustments to regulations and acquisition processes, but it—we have tools now that we didn't have this time last year.

Ms. ROYBAL-ALLARD. Can—can you just remind me what kind of damage was done by Kaspersky?

Mr. KREBS. So on Kaspersky, it—it wasn't that there was necessarily damage, there was the potential—potential for damage, but most importantly, it was an untenable risk position. So the way I look at the Kaspersky issue was that it was this anti-virus product which had effectively wide, broad access to equipment below a level against which you monitor, effective anti-virus products bring the information they collect back to a central collection point. It just so happens, in that case, it was in Moscow, and we know that there are a series of laws in Russia—and other laws that intelligence and law enforcement services over there can compel access to information.

So basically, if you work that chain back, FSB, GRE or whatever, the Russian services potentially had access to civilian networks. Untenable position, ripped the equipment out.

Ms. ROYBAL-ALLARD. Okay. What tools exist today to help agencies identify the hardware and software they are using that is vulnerable?

Mr. KREBS. So there—there are a range of both kind of hard tools and soft tools, more through contracting processes you can require the prime contractor to identify second, third, fourth tier subcontractors. There are open source tools that can map supply chains and identify where in those, where in the process those risks are. Those are the sorts of things that we are looking at, what those tools and capabilities are that we can pull into the supply chain council and issue guidance and issue contracting language, model contract language to departments and agencies.

Ms. ROYBAL-ALLARD. Okay. I have several other questions, but my time is up. So Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you, Madam Chairman. Director Krebs, in your testimony, you referenced initiatives CISA is taking to mitigate supply chain threats as one way of securing out net-

works and infrastructure. Do these efforts include election equipment?

Mr. KREBS. So we do work with the election community, state and local election officials, the vendor community, the Election Assistance Commission in this to provide threat awareness and security best practices. We do have a pilot program that we are in the initial stages of as I mentioned earlier where we are working with a vendor, we are taking their equipment as it is in the development process and we are basically red teaming it. Meaning, we are trying to attack that box. We are trying to hack into it. And we then provide the findings back to the vendor and say, Here are some of the things you need to work on.

Mr. FLEISCHMANN. Okay. As a follow-up to that sir, do you believe the Election Assistance Commission and their partners at NIST have developed voting system guidelines and certification processes that adequately take supply chain risk into account?

Mr. KREBS. So the—it is kind of a temporal question, but they are in the process right now of developing or receiving comments, I am sorry, on the voter—the voluntary voter systems guide, voting system's guide 2.0. They have just—the EAC that just recently got—reached a quorum where they could issue it. So that process is ongoing right now.

So I haven't reviewed the—the guidance in detail recently, but it is—it is certainly progress.

Mr. FLEISCHMANN. Thank you, sir. Help America Vote Act or HAVA was enacted in October of 2002, nearly 19 years ago when the Hanging Chad was the greatest threat to our democracy. Fast forward to today and we are looking at challenges we would never have dreamed of back then. The Election Security Act was included as a separate title of H.R. 1. How much input or communication did the department have in crafting the Election Security Act and do you feel your concerns were incorporated into the text?

Mr. KREBS. So over the course of the last Congress, we provided technical assistance on a range of election security-related legislation with the Election Security Act, with the secure act, I can't recall the specific name. So over the last Congress, we did provide technical assistance.

You know, when I look at section 3 of H.R. 1, there are a lot of things that we do already in there. You know, we will provide technical assistance to anyone that—that requests it whether it is a vendor or a state and local government.

Mr. FLEISCHMANN. The Election Security Act has a number of new requirements and about four new grant programs by our count. One question, do you find your best work with the states comes about because you have collaborative and voluntary relationships?

Mr. KREBS. I think our best work comes from, with state and locals, they come because I have a service that—that they need and they trust.

Mr. FLEISCHMANN. All right, I think that about does it. Thank you, Director Krebs. Again, I want to thank you and your department for an outstanding job. Well done, sir.

Ms. ROYBAL-ALLARD. Mr. Price.

Mr. PRICE. Thank you, Mr. Commissioner. I want to ask you about the international context of this—of this challenge. Based on press reports and other reports we hear, it is sometimes hard to distinguish what the level of involvement is. I mean there are disinformation campaigns, there is hacking into the election-related communications, the famous email cases, there is hacking into the actual voting equipment, the countries in which there has been serious interference seem to include, according to reports, Montenegro, Moldova, Ukraine, a number of European situations, I wonder how much—how much do we monitor this, how much do we know about it, how much do we learn from it?

This is partly a question about the relationships your agency has with, of course, with the intelligence community, with Defense, with State, with other—other government agencies and exactly what the division of labor is with respect to international monitoring and international cooperation. It is also a question though about how you would assess the state of play here. Do we have the kind of international agreements and understandings we need to monitor what is going on and understand what is going on, to—to devise protections in a cooperative way, to have mutual warning systems and so on.

So I am asking you for an assessment of what we—what we know and what we have yet to achieve in terms of understanding and dealing with this internationally.

Mr. KREBS. Sir, you—I think you laid out the three vectors appropriately and that is how they are characterized in the intelligence community assessment after the 2016 elections. It is—it is the technical lacking of election equipment, it is the disinformation, the—the campaign to sow discord and divisiveness across the American people and then the hacking lead campaigns and political operations and campaigns.

In terms of the level of—well, let me—so I am—my team leads the domestic efforts of protecting election equipment. The FBI is responsible for the disinformation campaigns, the discord and divisiveness and countering those efforts and then there is the hacking lead piece where we do work very—we work with political campaigns, particularly the national parties to help them secure. In fact just last week, I met with a number of folks on that that count.

Internationally, the intelligence community is all over this. They regularly track these activities. They work closely with their international—with their partners overseas. What we are doing within CISA right now is kind of collating the—our lessons learned from 2016 and 2018 and then going to our international partners particularly in Europe as they are about to face, there are national level votes coming up and then there are also the European Parliament votes that are coming up in a matter of months.

And we are just offering our experience and our findings and saying, You know, these are some of the things that we found useful. We did some kind of innovative things I think of working with the media of raising awareness and education, the things we are doing and where the risk really is.

Mr. PRICE. CISA is engaged in this directly.

Mr. KREBS. Yes, sir.

Mr. PRICE. With international counterparts.

Mr. KREBS. Just last week, again, out in San Francisco at the RSA conference, I met with probably 30 to 40, I lost count, of my international partners and the hot topic is election security. So we shared our experiences, the things we found useful. I am going to send basically a travel team more sounds like kind of a European vacation for spring break, but over to Europe to share our experience and the best practices and tips that we have.

Mr. PRICE. Do you feel, by virtue of these international contacts and your access of course to our other agencies, do you feel like you have a good fix on the full range of techniques and how advanced the different classes of actors there might be?

Mr. KREBS. I will admit that part of this experience of engaging with our international partners is there are tools being deployed and techniques being deployed in certain spaces in the Baltics for instance that we haven't seen here yet. So I want to figure out what that is going to the chairwoman's point of what are you thinking for 2020? What do you think they are going to do? I don't know yet. I haven't seen it yet, but maybe they are using it somewhere else and if I can go spot it over there, I can go—I can get ahead of it here.

Mr. PRICE. Well, that is really why I am asking, it is clearly relevant, urgently so.

Mr. KREBS. Yes, sir.

Mr. PRICE. And I would think a bellwether of what we might see here.

Mr. KREBS. Yes, sir.

Mr. PRICE. And you are confident you have those—those links out?

Mr. KREBS. Yes, I will be spending part of April over in Europe to do just this. We host delegations of international partners virtually every week, whether it is Europe or Asia-Pacific. We are working this every single day and we are working with our partners every single day.

Mr. PRICE. Thank you. Thank you, Mr. Chairman.

Ms. ROYBAL-ALLARD. Mr. Rutherford.

Mr. RUTHERFORD. Thank you, Madam Chairman. Director, I am—I am going to follow-up on this international kind of angle here as well, but let us switch it over to private industry, you know, the strength of any chain is only as strong as the weakest link. And so what is CISA's relationship with private industry abroad, particularly when we look at issues like China? You know, I am hearing some of the property theft as high as—well, I have heard a lot higher than that, I have heard a trillion, so, who knows what the number is?

But it is it is obviously significant. Can you talk a little bit about what are we doing working, what does CISA doing working with those private industries to combat these attacks on their intellectual property?

Mr. KREBS. So two kind of—two ways to address this question. One is what is happening overseas that we may not have seen here yet and that is what certain countries are maybe doing, in Ukraine or the Middle East or elsewhere. So we work with our international partners and we work with their domestic industry to, again, get ahead, try to get ahead of what the bad guys are doing, and so that

we can bring that learning back here and harden our domestic infrastructure. So that is point one.

Point two is the U.S. companies traveling overseas, engaging overseas we are working to build awareness and share strategic intelligence. And what by that, I talked about this a lot last week, but China has kind of told us what their areas of interest are. They have set out a plan for strategic sectors of where they want to grow and how they are going to get there. So what we do is we look at those strategic sectors and we engage domestic companies that play in those sectors.

And we try to make, we hope they understand that they are our target, they need to make sure they are taking care of their networks and we can help them. But the risk level is going to change. So if you play in those sectors, your risk is at this level, a five let us say. If you do business with China, a Chinese company or Chinese government, then your risk is a little bit higher, maybe a seven. If you operate in China, your risk is then, I don't know, quote Spinal Tap here, your risk is an 11.

It really does matter where you operate and what space you operate in and how you do business. Do you outsource your services?

Mr. RUTHERFORD. So do we have any guidelines for them or are there any CISA requirements?

Mr. KREBS. We have guidelines—Yes, sir. So requirements, no. We are a voluntary organization, but we are in the midst of an awareness campaign in—in December 20th last year, the Department of Justice indicted a number of Chinese hackers related to a global hacking campaign.

So what we have done is a series of webinars, outreach, engagement, working with our industry partners to help them understand what the Chinese did and some of the things that we can do collectively and individually to protect against those sorts of attacks. This is—I mentioned in my opening, I have five strategic priorities for the next 18 months to 2 years, 2 of them federal networks and elections.

Number one, China supply chain, 5G.

Mr. RUTHERFORD. Okay, thank you very much. I yield back.

Ms. ROYBAL-ALLARD. Mr. Ruppertsberger.

Mr. RUPPERSBERGER. Yes. I would like to know your thoughts on how the CISA's successes or failures can be communicated to the subcommittee, again, because of preparations, what tools and things you need. And I know you brought this up in your opening statement, I needed to be at another event, so I couldn't be there, but I have always had problems or concern, that DHS' cyber mission and not yours but just generally is that I don't know how we are doing it in this field. It is evolving and I think since you have been here your position to stabilize to an extent, but I think we have to go a long way as far as educating this committee.

And you have a good team, you have good people, though I don't think you have enough people or resources, but that is another thought and you have got your budget and we are going to deal with that. But can you expand upon your risk management, your metrics as far as determining your successes or failures as it relates to where you are so this committee can deal with that and

understand more other than just showing up for a hearing, ask staff to do the work.

Because I am really concerned, I know that—I represent NSA and I have been dealing with cyber since I have been in Congress and I am really concerned. It is such a major, other than nuclear weapon, this is probably one of the most dangerous threats that we have in the world and in this country too, and we haven't, even destructive attacks and that type of thing. So I want to find a way that you can continue to communicate, let us know where you are and not because someone from the administration says you got to do this, you got to do that.

I mean this is serious and I know you have credibility and you want to do what is right. So do you have any ideas on how we can deal with this and what metrics we can use to do it?

Mr. KREBS. So the metrics distinguish us from NSA because this is—

Mr. RUPPERSBERGER. Yes, probably different, I understand.

Mr. KREBS. It is not apples to apples. They have control authorities over the—

Mr. RUPPERSBERGER. They have got the—they have got the resources and they do it—and you have got a mission.

Mr. KREBS. And so we are a voluntary organization for the critical infrastructure community. We do have certain authorities over the federal government and that includes setting baselines, deploying tools. Congress has helped with that through some of our—what is known as Einstein Program. And we—well, where we are going to be most successful whether it is in the federal government or in the critical infrastructure community is by providing something of value.

One of the key areas of focus right now for our Continuous Diagnostics and Mitigation program, we just entered the defend phase. What this really means is we are buying at scale to provide a resource to an agency cheaper than they would be able to get otherwise, whether directly through GSA or effectively on the open market.

Einstein 1, Einstein 2, what we do is we aggregate all sources, commercial sources, open source, we bring everything together. Again, no agency would be able to do, buy every single threat feed out there and bring it all together and clean it up and package it. It just—it doesn't scale and it is not the right way to do government.

So while we have these tools, these services, these capabilities we are pushing out there, adding a value below the price point somebody would be able to do otherwise, we are also looking at where from a defense in depth perspective, we can be the most effective. And really it is things like the patch management, Binding Operational Directive 15-01, we said thou shalt patch, federal agencies patch critical vulnerabilities in 30 days.

What we found is they went from 219, 219 days to about 20. That was purely because of a policy. So I need to be looking in that stack of defense in depth and say where else can I have a high return on investment that doesn't just saddle a CISA with one more thing that they need to do on a daily basis. And that is—that is really our area of focus right now.

Mr. RUPPERSBERGER. And I think that is laudable, but here is one concern. You have different agencies. Sometimes these agencies have been given independence. They have their techs, some are not very good, some are better. Now, it seems to me you, as the oversight, need to deal with that, not only deal with it with the administration, but deal with it with us, because if you have—if you don't have that coalescing of everyone together, you are talking about the tools. You have talking about the oversight that we still have—we haven't done what we need to do in dot gov, you know that. And it is going to take more than just what you are seeing here today.

It is going to be Congress working with the administration and to make sure that if we have got a lousy department because of their boss or because they don't have the technology, then we are in trouble. And you talk about the chain, the weakness of the chain.

Mr. KREBS. Yes, sir. We are working with the Office of Management and Budget right now and Suzanne Kent the CIO, federal CIO on establishing a security baseline. And this is what every agency's profile from an outcomes perspective, in particular, should look like.

Mr. RUPPERSBERGER. And that is really important to me on where we think what we are going.

Mr. KREBS. Absolutely yes. And—

Mr. RUPPERSBERGER. Yes, are you finished?

Mr. KREBS. Yes. So—so as we, again, as we go through this IT modernization process, as Congress continues to invest in better citizen services, if we hit the baseline, then we are much better off than where we are. And if an agency can't do it, I am there as a backstop to help them get there.

Mr. RUPPERSBERGER. You work very closely with the FBI because they have the jurisdiction here too.

Mr. KREBS. Yes, sir.

Mr. RUPPERSBERGER. Because they really improved a lot I think from where they started and where they are.

Mr. KREBS. It is a whole government approach and I just—I am—I didn't think that I would necessarily see this level of cooperation across the intelligence community at the Department of Defense, the law enforcement community.

Mr. RUPPERSBERGER. And—

Mr. KREBS. So we are—we are—we are a lot better than we were certainly four or five years ago, just, again, I think it is the awareness, the sense of urgency and the desire to just jump in and take—and try to tackle the problem.

Mr. RUPPERSBERGER. Thank you.

Mr. KREBS. Yes, sir.

Ms. ROYBAL-ALLARD. Ms. Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. Thank you. Mr. Krebs, thanks for joining us. In your prepared testimony, you stated that one of the highest profile threats we face today is attempts by nation state actors to maliciously interfere in our democratic elections. You went on to describe the work that CISA did in the lead-up to 2018 mid-terms to assess federal partners, state and local election officials and private sector vendors in better defending their infrastructure from malicious actors.

In August, the heads of the National Security Agency said that Russia was still trying to influence and disrupt our 2018 midterm elections. Did Russia attempt to interfere on our elections in 2018?

Mr. KREBS. So the departments were all here is to assess whether there was a material impact. The secretary alongside the attorney general, the acting attorney general at that time issued a statement a month or so ago that said there was no material impact tied, attributed to a nation state on the 2018 election.

Ms. WASSERMAN SCHULTZ. The question is, did they attempt?

Mr. KREBS. I would—I would have to go and look back specifically at DNI Coats’—

Ms. WASSERMAN SCHULTZ. Material impact is different than an attempt.

Mr. KREBS. But Russia is an active player in this space. They continue to try, they will continue to try. I would be disappointed in them if they didn’t try again in 2020. They are here to stay.

Ms. WASSERMAN SCHULTZ. Okay. So if Vladimir Putin denied that they were attempting to interfere in our elections, would you believe him?

Mr. KREBS. My job is to help state and local election officials protect our systems.

Ms. WASSERMAN SCHULTZ. I know, given what you have just said—given what you have just said, if Vladimir Putin denied that Russia is attempting to interfere on our elections, would you believe him?

Mr. KREBS. You know, I base on what I see. We see activity. The intelligence community was very clear in their statement in the report of 2017. Russia, they tried to interfere, absolutely.

Ms. WASSERMAN SCHULTZ. So you would not believe Vladimir Putin if he denied their intentions.

Mr. KREBS. I believe in the intelligence community. They said he did it, he did it.

Ms. WASSERMAN SCHULTZ. Okay. Did any nation state beyond Russia attempt to interfere on our elections in 2018? And did any non-state foreign actors attempt to interfere on—in our elections in 2018?

Mr. KREBS. So generally the landscape is pretty active right now. I think in part Russia gave the playbook in 2016, but everybody has a different style and different objectives they want. The best—you know, I describe it this way.

Russia is trying to disrupt the system. They are trying to create havoc. They are trying to undermine the American people’s confidence in our system of democracy. China on the other hand, very, very active. I think the FBI director has said that they have active counterintelligence investigations in every—in all 50 states or every field office, whatever their metric is. But they are trying to manipulate the system to their advantage.

China is—you know, you are only successful in China if they let you be successful. They are trying to shape global politics in their favor so that they are the prime—

Ms. WASSERMAN SCHULTZ. So are they making attempts to interfere in our elections process?

Mr. KREBS. They are—they are absolutely engaging and influencing the political process.

Ms. WASSERMAN SCHULTZ. In what is China engaging in that activity?

Mr. KREBS. Well for one they—as I mentioned, they are very active in local politics. They get local politics get influence money into the process. So yes, this is—I am stepping well out of my area of expertise, but you know, I—they are active.

Ms. WASSERMAN SCHULTZ. So Ms. Yang's potential ties to China could be related to those efforts?

Mr. KREBS. I am not sure.

Ms. WASSERMAN SCHULTZ. The individual who was the owner of the massage parlor in Palm Beach County where Robert Kraft was and 40 others were caught and who contributed to President Trump's campaign in the 2016 election.

Mr. KREBS. I would have to defer to the Department of Justice on that one.

Ms. WASSERMAN SCHULTZ. Okay. To your knowledge, what methods did nation states and non-state actors deploy in an attempt to interfere in our mid-term elections and were they preventable?

Mr. KREBS. So in terms—

Ms. WASSERMAN SCHULTZ. Just as you describe with China I know, I can see the difference between Russia's efforts and China's, but are—are the non-mechanical attempts to interfere preventable?

Mr. KREBS. Non-mechanical, you mean like social media, are you talking about manipulating the press?

Ms. WASSERMAN SCHULTZ. Things that are not related to influencing the outcome of our elections in our systems and voting processes and the like.

Mr. KREBS. So we are very focused on the technical tactical on network hacking of state and local elections especially and increasingly, particularly as we are in the midst of a presidential cycle, working with political campaigns.

Ms. WASSERMAN SCHULTZ. And just—just one more question because I don't know how much—I can't see how much time I have left.

Okay, given President Trump's insistence that Russia did not interfere in the 2016 election, how can we have confidence that this administration is taking the threat seriously and that you have the authority and independence needed to fulfill your responsibilities?

Mr. KREBS. I have been in meetings with the president when he said he believes the intelligence community report, he has assessed them. He said it publicly, I will take him at his word. That is what I go on. I operate with the state and local officials, below the headlines. That is my job.

Ms. WASSERMAN SCHULTZ. And you are given the authority and independence needed to fulfill your responsibilities.

Mr. KREBS. Absolutely. And again I think the proof is in the pudding. You go ask any state or local election official that has worked with us whether we are of value to them and have we been helpful or we have been in any way restrained. Again, I think—I think the proof is in our performance.

Ms. WASSERMAN SCHULTZ. Good to know. Thank you. I yield back, Madam Chair.

Ms. ROYBAL-ALLARD. Could you have—sure, absolutely.

Mr. RUTHERFORD. I want to follow-up on Mr. Ruppensberger's question about what kind of matrices can you provide to us, this committee so that we—so that we see the value and the—and the progression of what you are doing. And I was thinking about these binding operational directives that—that you guys have the capacity to put out. At agencies, they are binding on these agencies.

I think one measurement could be how many of these BODs do you put out and then how well, following up on how well those agencies are responding the way you are asking them to respond? And I would be very interested in that kind of measurement going forward.

So I appreciate Dutch bringing that up.

Mr. KREBS. So all of the binding operational directives at this point have been publicly posted. I think also the compliance metrics and we across the board, we have had the kind of—the compliance that we would want.

Mr. RUTHERFORD. And—

Mr. KREBS. Right. You know when we find—let me give you an example, the recent emergency directive which is the first emergency directive which is based on an emerging threat and something we are greatly concerned about in January that we ask—we asked agencies to do four things.

One of those things was enable multifactor authentication, which means harden the security access and authentication measures on the systems that manage the domain system—domain name system of records. What we found was that some agencies had outsourced the DNS records management to a third party, to a contractor, and when they asked the contractor to enable multifactor authentication, the contractor said, We can't. We just—we technically can't do it.

Aha, so this is one of the challenges of contracting and outsourcing processes, there is push and a pull. So what we then do is work with that agency on road mapping how to get to a provider or maybe this is something that the Department of Homeland Security can do down the road. We can build that infrastructure to provide a DNS management system for the interagency. So these are the sorts of things that we are working towards.

Mr. RUTHERFORD. But that is the kind of thing that I think—that I think Dutch was talking about and I would like to see because it shows me the bang for our buck going forward.

Mr. KREBS. Yes, sir.

Mr. RUPPERSBERGER. And we are really in a new phase now and we are pioneers. Ten years from now it is going to be a lot different. We have got to stay ahead of the curve and educate, workforce, everything.

Mr. KREBS. Yes, sir.

Mr. RUTHERFORD. Thank you.

Mr. RUPPERSBERGER. Is that the end of the hearing?

Ms. ROYBAL-ALLARD. Yes, unless—

Mr. RUPPERSBERGER. Well I do have something that is kind of a joke, but all the matters are over with, semi, when Chris and I gave—when Chris and I gave a cyber-speech in Baltimore, so I had my staff as his staff. Is there anything that, a joke, and we were

all apprehensive and didn't want to say hey, you know. Don't say it came from us.

Mr. KREBS. I came prepared, don't worry.

Mr. RUPPERSBERGER. But he loves colored socks. What are they today?

Mr. KREBS. They are a little camo.

Mr. RUPPERSBERGER. Oh yes, they are—they are conservative.

Mr. KREBS. You know, I was prepared.

Mr. RUPPERSBERGER. Okay, you got it.

Ms. ROYBAL-ALLARD. And the hearing is adjourned.

[Material submitted for inclusion in the record follows:]

Questions for the Record
Securing Federal Networks and State Elections Systems
Christopher Krebs, Director Department of Homeland Security
Senate Committee on Appropriations Subcommittee on Homeland Security
March 13, 2019

Qfr No. 1

Question: What steps is CISA taking to hire more dedicated election infrastructure staff and to finalize a detailed strategy in advance of the 2020 election cycle?

Are there ways for Congress to assist you in achieving your staffing goals?

Answer: Throughout the 2018 election cycle and as we work to protect 2020, the Cybersecurity and Infrastructure Security Agency (CISA) has been building the processes of securing election infrastructure into our systems and procedures. CISA continues to incorporate lessons learned from the 2018 midterms into our 2020 strategy. As we move into 2020, CISA continues the prioritization of support to election administrators and vendors; continues building relationships to support and advise partisan organizations; enhances awareness and participation by the public and interested third parties; and improve rapid bi-directional information sharing between key stakeholders in the private sector, the federal government, and the state, local, tribal, and territorial community.

In addition to the core team dedicated to coordinating Federal Government efforts that support election officials with securing election infrastructure, there are hundreds of employees working on election security across the Nation on any given day. This includes our field-based staff, our technical experts who assess election infrastructure for vulnerabilities, and our incident responders. CISA's field personnel will continue to be critical to building relationships and awareness within the election community regarding the support and services CISA offers.

CISA is resourced to reach state and local officials around the country, and assist them with managing risk. We are achieving this objective in the near term with the resources already appropriated by Congress and would continue to do so with those identified within the President's Fiscal Year (FY) 2020 Budget. In 2018, DHS was able to meet all requests from election stakeholders for support and services prior to the 2018 general election. Moving forward, thanks to the additional funding provided by Congress, CISA will establish additional teams to support election officials including risk and vulnerability assessments, and hunt and incident responses. In addition, based on feedback from the election community, CISA was able to develop a scalable, remote penetration testing service that is now available for all critical infrastructure partners.

CISA is currently recruiting multiple personnel and bringing in additional expertise through contracts that will support the Election Security Initiative and our 2020 priorities. We are hiring additional staff to provide election administration expertise, coordinate with DHS field staff, coordinate with the intelligence community, develop educational materials, and manage CISA's financial and operational support to the Elections Infrastructure Information Sharing and Analysis Center.

TUESDAY, MARCH 26, 2019.

UNITED STATES COAST GUARD

WITNESS

ADMIRAL KARL SCHULTZ, COMMANDANT, UNITED STATES COAST GUARD

Ms. ROYBAL-ALLARD. The subcommittee on Homeland Security will come to order.

Admiral Schultz, I want to welcome you to your first hearing before the subcommittee, and we are pleased to have you testifying before us today.

I would also like to thank you and the thousands of Coasties you have the privilege of leading for your service to the Coast Guard and our country.

Nearly a year into your tenure as commandant, we look forward to a good discussion of your observations and visions for the future.

As the fiscal year 2019 bill, I was pleased we were able to provide the Coast Guard with over \$10 billion in discretionary funding. We funded important investments to recapitalize the Coast Guard's air and marine assets, including for the Coast Guard's first polar security cutter to replace the current aging family of ice-breakers.

I want to acknowledge that the government shutdown was difficult for the Coast Guard families. The Coast Guard was the only armed service that worked without pay for those 5 weeks. But I was pleased that in our enacted bill we were able to support those men and women with resources for more staff, increased pay and increased subsidies for childcare.

Unfortunately, the President's fiscal year 2020 request for the Coast Guard was less promising. It proposes an overall reduction to the Coast Guard budget of over \$700 million, including a reduction of more than \$1 billion to the procurement account. We look forward to hearing from you today about your fiscal year 2020 request and whether it would provide the resources that you need to support your important and varied missions.

I personally want to add that I look forward to seeing some of the assets and capabilities of the Coast Guard in my home state next month, when a number of my colleagues and I come to observe DHS operations in San Diego and Long Beach. Thank you again for joining us, and I look forward to our discussion.

I would now like to turn to the distinguished gentleman from Tennessee, Ranking Member Fleischmann, for his opening comments.

Mr. FLEISCHMANN. Thank you, Madam Chairwoman.

Admiral, I just want to take a personal note of thanks to you, to the government shutdown. You represented the Coast Guard

and the men and women who serve you in exemplary fashion. I want to thank you for sending Admiral Ray to Chattanooga for Coast Guard Week, and to all of the men and women who serve us in our great United States Coast Guard, a heartfelt thanks. This is a very special subcommittee, but I—I can assure you, there's tremendous bipartisan support for what you do, and I thank you, sir.

I can see that the priority in this budget is to support the men and women of the Coast Guard. Reading through your written statement, it is apparent that your goal is making sure the people on your command are taken care of, and that they have the resources they need because they give so much to our country each and every day. I will have some questions about some specific investments later.

However, I also see the procurement account where OMB is proposing to short-fund some of the programs that are a priority of the Congress, which we have seen before across the committee. I have some questions about those investments, as well.

I look forward to working with you and the chairwoman as she puts together the bill to address the needs across the department, sir. Thank you again for your testimony today, and for your service every day, sir, and I yield back.

Ms. ROYBAL-ALLARD. Before your testimony, I would like to take care of some housekeeping items. The order in which members will be called for questions will be based on the seniority of those present when the hearing was called to order, alternating between majority and minority members. And to ensure that everyone has ample opportunity to ask questions, I would ask each member to keep to the five minutes that they are allotted.

So, again, Admiral Schultz, thank you again for joining us this morning. Please provide a brief summary of your testimony, and we will enter the full text of your testimony for the record.

Admiral SCHULTZ. Good afternoon, Madam Chairwoman Roybal-Allard, Ranking Member Fleischmann, members of the committee. I appreciate the opportunity to testify today and ask that my written statement be entered into the record as you noted, Madam Chairwoman.

First, on behalf of the men and women of the United States Coast Guard, please accept my profound gratitude for your unwavering support, including the recently enacted fiscal year 2019 appropriation and the 2018 hurricane payment supplemental funding. These were meaningful steps towards delivering a Coast Guard that's ready, relevant and responsive to meet the American needs and expectations, what the American public deserves.

Yet our work is not done. If you take away just one thing from this hearing today, please remember this: Readiness. We must be ready: ready to push our maritime border 1,500 miles from our shores; ready to preserve the \$5.4 trillion in economic activity that flows through our Maritime Marine Transportation System annually; ready to support the geographic combatant commander needs around the globe; ready for the next hurricane season, which is just around the corner; and ready to put our cyber-authorities to use as we adapt to 21st century threats.

Without question, building and sustaining readiness is my top priority. And we are at a critical juncture, a tipping point of sorts.

Almost a decade of near-flatline operations and support funding, Coast Guard readiness is eroding, just like the other armed services.

Yet unlike the Department of Defense, the Coast Guard funding is categorized as nondiscretionary or non-defense discretionary, which means we are excluded from the effort to rebuild our military, and continue to find ourselves outside looking in when it comes to material operations and support plus-ups. In 2017, Department of Defense received a 12 percent boost in operations and support funding, while the Coast Guard received a 4 percent increase.

Yet the Coast Guard military contributions are innumerable. Every year, we profoundly—excuse me—we proudly expend over \$1 billion on defense-related activities in direct support of the combatant commanders. But the \$340 million of defense readiness dollars that we receive for this work has not changed in 18 years.

As an example of our growing defense portfolio, the National Security Cutter *Bertholf* is supporting the Indo-Pacific commander operating in the South China Sea right now, enforcing U.N. sanctions against North Korea and protecting and advancing U.S. interests throughout the Western Pacific.

Though we strive for relentless resilience to execute Homeland Security and Defense operations, our purchasing power has, in fact, declined. If we continue to neglect our growing backlog of deferred repairs on our capital assets, including shore infrastructure, we will lose ground in the fight to defend our homeland from the evolving threats challenging our nation.

Despite these challenges, I am extremely proud of the Coast Guard's contributions. In 2018, as part of the Department of Homeland Security's layered security strategy, and in support of Joint Interagency Task Force South, our surface and aviation assets interdicted 209 metric tonnes—that's 460,000 pounds—of cocaine, more than all other federal agencies combined, and apprehended more than 600 suspected smugglers.

Disrupting transnational criminal organizations at sea where they are most vulnerable helps reduce what we call the push factors that are responsible for driving human migration to our southwest land border. As I speak today, National Security Cutter *Waesche* is patrolling in the Eastern Pacific.

Our national security cutters have exceeded performance expectations by every metric, and now we must focus on a transition from outdated and costly medium-endurance cutters—our 210s and 270-foot ships—to a planned fleet of 25 highly capable offshore patrol cutters, which will be the backbone of the Coast Guard's offshore presence for decades to come.

In the polar regions, your Coast Guard's the sole surface presence to protect our rights and project sovereignty. As access to the region expands and interest from China and Russia grows, it's in our national interest to be there to enhance maritime domain awareness and build governance in this economically and geostrategically competitive area. In the high latitudes presence equals influence.

Two weeks ago, our sole operational heavy icebreaker, the *Polar Star*, 43 years young, returned from a 105-day patrol to Antarctica,

where it's conducting the annual McMurdo Station breakout, enabling resupply of this vital national interest. These missions take a toll, and *Polar Star's* crew worked miracles to keep their cutter mission-viable, battling a ship-board fire, numerous electrical outages, and combating engine room—just off the ice edge, we put embarked Coast Guard and Navy divers into the frigid Antarctic Ocean to effect repairs to the shaft seal. I am proud of their efforts, and I remain concerned, however, that we are only one casualty away from being a nation without any heavy ice-breaking capability. New icebreakers cannot come fast enough.

And thank you for the \$675 million in the fiscal year 2019 appropriation. Coupled with the \$300 million in prior years' appropriations, I am pleased to report we are on track to award the detail, design and construction contract in 2019 to keep this vital program on schedule.

Finally, I appreciate the administration's support for a number of initiatives that invest in our greatest strength, and that is our people. While modest, they represent tangible investments towards what I call the mission-ready total workforce; for instance, critical investments in our marine inspections workforce and to our cybersecurity operations. That builds upon the capabilities that facilitate the \$5.4 trillion of annual economic activity on our nation's waterways, while protecting maritime critical infrastructure from attacks, accidents and disasters.

A dollar invested in your Coast Guard is a dollar well spent, and with your continued support, the Coast Guard will live up to our motto, *Semper Paratus*—always ready.

Madam Chairwoman, I would just like to add thank you for your gracious remarks this morning on behalf of our Coast Guard. It was very gracious of you, ma'am and Ranking Member Fleischmann.

I stand ready to answer any questions, and appreciate the opportunity to testify today.

[The prepared statement of Admiral Schultz follows:]

U. S. Department of
Homeland Security

United States
Coast Guard



Commandant
United States Coast Guard

2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7000
Staff Symbol: CCG
Phone: (202) 372-4411
FAX: (202) 372-8302

**TESTIMONY OF
ADMIRAL KARL L. SCHULTZ
COMMANDANT, U.S. COAST GUARD**

**ON
“THE COAST GUARD’S FISCAL YEAR 2020 BUDGET REQUEST”**

**BEFORE THE
HOUSE APPROPRIATIONS
SUBCOMMITTEE ON HOMELAND SECURITY**

MARCH 26, 2019

Introduction

Madam Chairwoman and distinguished members of the Committee, I appreciate the opportunity to testify today. Thank you for your enduring support of the United States Coast Guard, particularly the significant investments provided in the Fiscal Year (FY) 2019 Consolidated Appropriations Act.

Your Coast Guard is on the front lines of our Nation’s effort to protect the American people, our homeland, and our way of life. As threats and challenges to our national security and global influence grow more complex, the need for a *Ready, Relevant, and Responsive* Coast Guard has never been greater.

Appropriately positioned within the U.S. Department of Homeland Security (DHS), the Coast Guard is a federal law enforcement agency, a regulatory body, a first responder, a member of the U.S. Intelligence Community, and a military service and a branch of the Armed Forces of the United States at all times¹– The Coast Guard offers specialized and unique capabilities across the full spectrum of maritime activities, from security cooperation up to armed conflict.

The Coast Guard has matured and evolved over the course of our 228-year history, adapting our people, assets, and capabilities in response to emerging national demands and international challenges. We are locally based, nationally responsive, and globally impactful.

To outline my vision for the Service, I recently released the U.S. Coast Guard Strategic Plan 2018-2022. To that end, my highest priority is to “Maximize Readiness Today and Tomorrow,” and readiness starts with our people, who are our greatest strength. In the competitive marketplace the Armed Forces find ourselves, now is a critical time to invest in our mission-ready total workforce.

My second top priority is continuing to “Address the Nation’s Complex Maritime Challenges” through international and domestic leadership in the maritime domain. A unique instrument of national power, the Coast Guard offers the ability to secure the maritime border, combat Transnational Criminal Organizations (TCOs), and facilitate \$4.6 trillion of annual economic activity on our Nation’s waterways.

¹ 14 U.S.C. § 1; 10 U.S.C. § 101

Finally, in a competitive budget environment, your Coast Guard is acutely focused on my third priority, “Delivering Mission Excellence Anytime, Anywhere,” by continuously challenging ourselves to innovate and drive increased efficiency for better organizational performance in response to both manmade crises and natural disasters.

Strategic Effects

The Coast Guard plays a critical role in a comprehensive approach to securing our borders – from disrupting drug trafficking and illegal immigration in the southern transit zones, to projecting sovereignty across the globe. Our Nation’s maritime borders are vast, and include one of the largest systems of ports, waterways, and critical maritime infrastructure in the world, including 95,000 miles of coastline.

As part of the DHS layered security strategy, the Coast Guard pushes out our Nation’s border, and serves as the “offense” in a comprehensive approach to layered border security strategy. Through the interdiction of illicit drugs and the detention of suspected drug smugglers, the Coast Guard disrupts TCO networks at sea, over a thousand miles from our shore, where they are most vulnerable. Coast Guard maritime interdictions weaken the TCOs who destabilize our immediate neighbor Mexico, the Central American land corridor, and South American countries. Our interdiction efforts minimize corruption and create space for effective governance to exist. Coast Guard interdiction efforts reduce the “push factors” that are responsible for driving migration to our Southwest land border.

Working with interagency partners, the Coast Guard seized 209 metric tons of cocaine and detained over 600 suspected smugglers in FY 2018, which is more than all other federal agencies combined. Highlighting the capabilities of one of our modern assets, in November 2018, the National Security Cutter (NSC) CGC JAMES, in support of Joint Interagency Task Force South (JIATF-S), seized nearly nine tons of cocaine and detained over 40 suspected drug smugglers from various drug conveyances, including low-profile go-fast vessels and fishing vessels. In addition to stopping these drugs from getting to our streets, the information we gather and share with our partners in the Intelligence Community facilitates deeper understanding of TCOs and ultimately helps our unified efforts to dismantle them.

As an important part of the modern military’s Joint Force², we currently have forces assigned to each of the six geographic Combatant Commanders (COCOMs), as well as Cyber Command, Transportation Command, and Special Operations Command. The Coast Guard deploys worldwide to execute our statutory Defense Operations mission in support of national security priorities. Typically, on any given day, 11 cutters, 2 maritime patrol aircraft, 5 helicopters, 2 specialized boarding teams, and an entire Port Security Unit are supporting Department of Defense (DoD) COCOMs on all seven continents. In the Middle East, our squadron of six patrol boats continues to conduct maritime security operations on the waters of the Arabian Gulf in close cooperation with the U.S. Navy, promoting regional peace and stability.

Likewise, as one of the principal federal agencies performing Detection and Monitoring (D&M) in the southern maritime transit zone, the Coast Guard provides more than 4,000 hours of maritime

² In addition to the Coast Guard’s status as an Armed Force (10 U.S.C. § 101), see also Memorandum of Agreement Between DoD and DHS on the Use of Coast Guard Capabilities and Resources in Support of the National Military Strategy, 02 May 2008, as amended 18 May 2010.

patrol aircraft support and 2,000 major cutter days to DoD's Southern Command (SOUTHCOM) each year.

Coast Guard authorities and capabilities bridge national security needs between DoD war fighters abroad and DHS agencies protecting our homeland. In addition to COCOM support, the Coast Guard partners with federal, state, local, territorial, tribal, private, and international stakeholders to address problems across an increasingly complex maritime domain. Our leadership on global maritime governing bodies and our collaborative approach to operationalize international agreements drives stability, legitimacy, and order. We shape how countries conduct maritime law enforcement and establish governance.

Looking forward, the performance capabilities and expected capacity of our future Offshore Patrol Cutter (OPC) fleet will provide the tools to more effectively enforce federal laws, secure our maritime borders, disrupt TCOs, and respond to 21st century threats. Continued progress on this acquisition is vital to recapitalizing our aging fleet of Medium Endurance Cutters (MECs), some of which will be over 55 years old when the first OPC is delivered in 2021. In concert with the extended range and capability of the NSC and the enhanced coastal patrol capability of the Fast Response Cutter (FRC), our planned program of record for 25 OPCs will be the backbone of the Coast Guard's strategy to project and maintain offshore presence.

In the Arctic region, the Coast Guard remains steadfastly committed to our role as the lead federal agency for homeland security, safety, and environmental stewardship. There, we enhance maritime domain awareness, facilitate governance and promote partnerships to meet security and safety needs in this geo-strategically and economically vital area. As access to the region continues to expand, strategic competition drives more nations to look to the Arctic for economic and geopolitical advantages, and the Coast Guard stands ready to provide the leadership and sustained surface presence necessary to protect our rights and sovereignty as an Arctic Nation.

Looking to the Antarctic, the 43-year old CGC POLAR STAR, the Nation's only operational heavy icebreaker, just returned home after successfully completing Operation DEEP FREEZE (DF-19), the annual McMurdo Station breakout, though not without overcoming several high-risk casualties to the ship's engineering systems. The ship's crew had to battle a fire that left lasting damage to electrical systems; ship-wide power outages occurred during ice breaking operations. And in the same transit, divers were sent into the icy waters to investigate and repair a propeller shaft seal leak. Events like these reinforce the reality that we are only one major casualty away from leaving the Nation without any heavy icebreaking capability.

With increased activity in the maritime reaches and growing competition for resources, we cannot wait any longer for increased access and a more persistent presence in the Polar Regions. Our sustained presence there is imperative to ensuring our Nation's security, asserting our sovereign rights, and protecting our long-term economic interests.

Last year, we released a request for proposal (RFP) and later this spring we plan to award a detail design and construction (DD&C) contract for the construction of three heavy Polar Security Cutters (PSCs). I am thankful for your support for the \$675 million in the FY 2019 appropriation. This funding, coupled with the \$300 million in Shipbuilding and Conversion, Navy (SCN) funding in FY 2017 and 2018, is sufficient to fund construction of the first PSC as well as initial long lead time material for a second PSC.

Our value to the Nation is observed on the farthest shores around the globe as well as closer to home where we continue to be “Always Ready” to answer the call for help. The 2018 hurricane season led to yet another historic Coast Guard response effort. The Coast Guard mobilized over 8,600 active duty members, reservists, and civilians for hurricane response across the United States for hurricanes Florence and Michael in the mid-Atlantic states and Gulf Coast respectively, as well as typhoon Mangkhut in Guam.

In support of, and in coordination with the Federal Emergency Management Agency (FEMA) and other federal, state, local, and territorial agencies, the Coast Guard saved nearly 1,000 lives using helicopters and shallow water craft, provided logistical support to first responders, and oversaw the safe and effective resumption of commerce at over 20 impacted sea ports.

While such a level of professionalism and distinction is what the American people have come to expect from your Coast Guard, that response comes at a cost. We continue to do our very best to stand ready to respond to all maritime disasters, both natural and manmade; however, these efforts consume future readiness. Our aging assets and infrastructure require increased maintenance and repairs, all of which is compounded by the on-going recovery and restoration operations of the historic hurricane season of 2017.

In 2017 alone, the Coast Guard lost the equivalent of two major cutters (e.g., over 300 operational days) due to unplanned repairs. Expanding that to the last two years, we have lost three years’ worth of major cutter patrol days. In 2017 and again in 2018, shortages in parts and supplies cost the Coast Guard over 4,500 flight hours each year, or the equivalent of programmed operating hours for seven MH-65 helicopters. Each hour lost in the transit zones keeps us further from reaching our interdiction targets and helps the TCOs deliver their illicit cargoes.

Service readiness starts with our most valuable asset – our people. We must continue to recruit, train, support, and retain a mission ready total workforce that not only positions the Service to excel across the full spectrum of Coast Guard missions, but is representative of the diverse Nation we serve. Our workforce end strength was reduced by over 1,250 personnel during a three-year period from FY 2012 to FY 2015. And compared to the workforce of FY 2012, the Coast Guard has nearly 1,000 fewer personnel to accomplish an ever increasing mission set. Adequate increases to depot maintenance funding, coupled with strategic human capital investments, are critical to addressing these readiness challenges.

Conclusion

The Coast Guard offers a capability unmatched in the federal government. Whether combating TCOs to help stabilize to the Western Hemisphere, responding to mariners in distress in the Bering Sea, or supporting U.S. Central Command (CENTCOM) on the Arabian Gulf, the Coast Guard stands ready to execute a suite of law enforcement, military, and regulatory authorities and capabilities to achieve mission success anytime, anywhere. We cannot do this on the backs of our people –now is the time to address the erosion of readiness experienced in our Service over the past decade due to near flat line funding for operations and support..

While the demand for Coast Guard services has never been higher, we must address our lost purchasing power, the growing backlogs of deferred maintenance on our capital assets, and the degraded habitability of our infrastructure. Our 48,000 active duty and reserve members, 8,500 civilians, and over 25,000 volunteer members of the Coast Guard Auxiliary need your support to maintain a *Ready, Relevant, and Responsive* Coast Guard.

With the continued support of the Administration and Congress, your Coast Guard will live up to our motto – *Semper Paratus* – Always Ready. Thank you for your support of the men and women of the Coast Guard.

FY 2020 BUDGET REQUEST

The Coast Guard’s FY 2020 Budget request is focused on three main priorities:

1. Maximize Readiness Today and Tomorrow
2. Address the Nation’s Complex Maritime Challenges
3. Deliver Mission Excellence Anytime, Anywhere

Maximize Readiness Today and Tomorrow

The Coast Guard’s top priority is Service readiness. The FY 2020 President’s Budget request begins to address the erosion of readiness that resulted from years under the Budget Control Act. Critical investments in the workforce as well as depot maintenance for the fleet will put the Service on the path to recovery to sustain critical frontline operations.

Additionally, investments in asset modernization sustain recapitalization momentum while advancing other critical programs. The FY 2020 Budget request supports the Service’s highest priority acquisition, the OPC, and continues recapitalization efforts for cutters, boats, aircraft, IT systems, and infrastructure.

Address the Nation’s Complex Maritime Challenges

As one of the Nation’s most unique instruments of national authority across the full spectrum of maritime operations, the Coast Guard cooperates and builds capacity to detect, deter, and counter maritime threats.

While nefarious activities destabilize and threaten vulnerable regions, the Coast Guard offers capabilities, authorities, and established partnerships that lead to a more secure maritime border. The FY 2020 Budget invests in a holistic approach to combat TCOs through targeted detection and interdiction of suspected drug smugglers, at-sea biometrics, and increased partnerships with allied law enforcement nations in Central and South America, to quell illegal migration.

As the Marine Transportation System (MTS) grows increasingly complex, the Coast Guard’s marine safety workforce must adapt to continue to facilitate commerce. The FY 2020 Budget increases the marine inspection workforce while addressing key findings from the report on the tragic sinking of the freight vessel EL FARO and the loss of 33 crewmembers.

Deliver Mission Excellence Anytime, Anywhere

The Coast Guard is an agile and adaptive force whose greatest value to the Nation is an ability to rapidly shift among its many missions to meet national priorities during steady state and crisis operations.

As new threats in the cyber domain emerge, the Coast Guard's cyber workforce serves as the critical link between DoD, DHS, and the Intelligence Community. The FY 2020 Budget increases the cyber workforce to promote cyber risk management and protect maritime critical infrastructure from attacks, accidents, and disasters.

The Coast Guard seeks to continually improve organizational effectiveness and the FY 2020 Budget eliminates redundant and outdated IT services to reinforce the culture of continuous innovation and enhance information-sharing across the Service.

FY 2020 BUDGET HIGHLIGHTS

Procurement, Construction, & Improvements (PC&I)

Surface Assets: The budget provides \$792 million for the following surface asset recapitalization and sustainment initiatives:

- National Security Cutter (NSC) – Provides funding for post-delivery activities for the seventh through eleventh NSCs, and other program-wide activities. The acquisition of the NSC is vital to performing DHS missions in the far offshore regions around the world. The NSC also provides a robust command and control platform for homeland security and contingency operations.
- Offshore Patrol Cutter (OPC) – Provides funding for construction of the third ship and long lead time materials (LLTM) for the fourth and fifth OPC. The OPC will replace the Medium Endurance Cutters, now well beyond their service lives, which conduct multi-mission operations on the high seas and coastal approaches.
- Fast Response Cutter (FRC) – Funds procurement of two FRCs, totaling 54 of the 58 vessels needed for the domestic program of record. These assets provide coastal capability to conduct Search and Rescue operations, enforce border security, interdict drugs, uphold immigration laws, prevent terrorism, and enhance resiliency to disasters.
- Polar Security Cutter (PSC) – Provides funding to support detail design and construction activities of the joint Coast Guard-Navy Integrated Program Office (IPO) and program management associated with construction of the lead PSC. PSCs will provide the Nation with assured surface access to the Polar Regions for decades to come.
- Polar Sustainment – Supports a multi-year Service Life Extension Project (SLEP) for CGC POLAR STAR, including program management activities, materials purchases, and production work.
- Waterways Commerce Cutter (WCC) – Provides funding for acquisition planning activities, including continued evaluation of options to replace the capabilities provided by the current fleet of inland tenders and barges commissioned between 1944 and 1990. These multi-mission platforms are integral to the protection of maritime commerce on the inland rivers.
- Cutter Boats – Continues funding for the production of multi-mission cutter boats fielded on the Coast Guard's major cutter fleet, including the NSC, OPC, and PSC.
- In-Service Vessel Sustainment – Continues funding for sustainment projects on 270-foot Medium Endurance Cutters, 225-foot seagoing Buoy Tenders, and 47-foot Motor Lifeboats.
- Survey and Design – Continues funding for multi-year engineering and design work for multiple cutter classes in support of future sustainment projects. Funds are included to plan Mid-Life Maintenance Availabilities (MMA) on the CGC HEALY, CGC MACKINAW, and the fleet of 175-foot Coastal Buoy Tenders.

Air Assets: The budget provides **\$200 million** for the following air asset recapitalization or enhancement initiatives:

- HC-144 – Continues Minotaur mission system retrofits and provides high-definition electro-optical infrared cameras to meet DHS Joint Operational Requirements.
- HC-27 – Continues missionization activities, including funding for spare parts, logistics, training, and mission system development.
- HH-65 – Continues modernization and sustainment of the Coast Guard’s fleet of H-65 short range recovery helicopters, converting them to MH-65E variants. The modernization effort includes reliability and sustainability improvements, where obsolete components are replaced with modernized sub-systems, including an integrated cockpit and sensor suite. Funding is also included to extend aircraft service life for an additional 10,000 hours.
- MH-60 – Includes funding to support a service life extension for the fleet of medium range recovery helicopters to better align recapitalization with DOD’s future vertical lift program.
- sUAS – Continues program funding to deploy sUAS onboard the NSC allowing increased interdiction through greater Intelligence, Surveillance, and Reconnaissance (ISR).

Shore Units and Aids to Navigation (ATON): The budget provides **\$174 million** to recapitalize shore infrastructure that supports Coast Guard assets and personnel, as well as construction and improvements to ensure public safety on waterways. Examples include:

- Replacement of covered boat moorings at Station Siuslaw River, Oregon; recapitalization of failed aviation pavement at Sector Columbia River, Oregon; construction in Boston, Massachusetts to support arriving FRCs; and construction in Sitka, Alaska to support arriving FRCs.

Other (Asset Recapitalization): The budget provides **\$69 million** for other initiatives funded under the Procurement, Construction, and Improvements account, including the following equipment and services:

- Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) – Provides design, development, upgrades, and assistance on C4ISR hardware and software for new and in-service assets.
- Program Oversight and Management – Funds administrative and technical support for acquisition programs and personnel.
- CG-Logistics Information Management System – Continues development and deployment of this system to Coast Guard operational assets.
- Cyber and Enterprise Mission Platform – Provides funding for emerging Command and Control, Communications, Computer, Cyber, and Intelligence (C5I) capabilities.
- Other Equipment and Systems – Funds end-use items costing more than \$250,000 used to support Coast Guard missions, including equipment to support operation and maintenance of vessels, aircraft, and infrastructure.

Operations and Support (O&S)

Operation and Maintenance of New Assets: The budget provides **\$59 million and 297 FTE** to operate and maintain shore facilities and sustain new cutters, boats, aircraft, and associated C4ISR subsystems delivered through acquisition efforts:

- Shore Facilities – Funds operation and maintenance of shore facility projects scheduled for completion prior to FY 2020. Projects include: Coast Guard Yard dry dock facilities in Baltimore, Maryland; FRC Homeport Facilities in Galveston, Texas; Electrical Utilities for Air Station Barbers Point, Hawaii; and Housing for Station Jonesport, Maine.
- FRC – Funds operation and maintenance and personnel for five FRCs and shore-side support for FRCs in Galveston, Texas; Key West, Florida; and Apra Harbor, Guam.
- NSC – Funds crew of NSC #9, as well as personnel for sensitive compartmented information facility (SCIF) crews and analytical support, and shore-side support personnel in Charleston, South Carolina.
- OPC – Funds a portion of the crew for OPC #1, as well as shore-side personnel to develop operational doctrine for the new class of cutter to be homeported in Los Angeles/Long Beach, California.
- HC-130J Aircraft – Funds operations, maintenance, air crews, and pilots for HC-130J airframe #12.

Pay & Allowances: The budget provides **\$118 million** to maintain parity with DoD for military pay, allowances, and health care, and for civilian benefits and retirement contributions, including a 3.1 percent military pay raise in 2020. As a branch of the Armed Forces of the United States, the Coast Guard is subject to the provisions of the National Defense Authorization Act, which include pay and personnel benefits for the military workforce.

Asset Decommissionings: The budget saves **\$12 million and 119 FTE** associated with the planned decommissioning of one High Endurance Cutter (WHEC) and three 110-foot Patrol Boats (WPBs). As the Coast Guard recapitalizes its cutter and aircraft fleets and brings new assets into service, the older assets that are being replaced will be decommissioned:

- High Endurance Cutter (WHEC) – The budget decommissions one WHEC. These assets are being replaced with modernized and more capable NSCs.
- 110-foot Patrol Boats (WPBs) – The budget decommissions three WPBs. These assets are being replaced with modernized and more capable FRCs.

Operational Adjustments: In FY 2020, the Coast Guard will make investments that begin to address the erosion of readiness of the Service while investing in new workforce initiatives:

- Aircraft Federal Aviation Administration (FAA) Compliance – The budget provides **\$22 million** to replace obsolete aircraft equipment and systems necessary to comply with FAA 2020 airspace requirements.
- Cyber and IT Infrastructure – The budget provides **\$16 million and 38 FTE** to mature the cybersecurity defense program. The budget also provides funding for an information technology framework and platform to establish a consolidated user interface primarily for Command Centers.
- Restoring Depot Readiness – The budget provides **\$10 million** to begin to restore eroded vessel and aircraft readiness and address critical information technology maintenance and inventory backlogs.
- Human Capital and Support Infrastructure – The budget provides **\$17 million and 22 FTE** to improve enterprise-wide support for the workforce, including the transition to electronic health records and training and support for the Coast Guard Reserve.
- Counter Transnational Criminal Organizations (TCO) – The budget provides **\$7 million and 26 FTE** to expand the Coast Guard's capacity to execute a multi-layered approach in the

Western Hemisphere maritime transit zone, dismantle TCOs, and secure our Nation's borders from illicit smuggling of all kinds.

- Maritime Safety, Security, and Commerce – The budget provides **\$6 million and 20 FTE** to strengthen the Coast Guard's marine safety program through improved marine inspector training, establishment of a third party oversight and auditing program, expansion of the marine inspector workforce, and improved accession opportunities for marine inspectors.

Ms. ROYBAL-ALLARD. Thank you, Admiral.

Admiral Schultz, during the partial government shutdown, the press rightfully focused on how it affected the Coast Guard families. I want to personally express my appreciation for the men and women of the Coast Guard who continued to protect our country despite the difficulties that it caused for them and their families.

However, I would also like to point out something that I don't think is getting enough attention: the lasting and persistent effects of that shutdown.

Could you spend a few minutes sharing with the subcommittee some of the effects of the shutdown—some of the effects that the shutdown had on the Coast Guard beyond the obvious effect of morale?

Admiral SCHULTZ. Yes, Madam Chairwoman.

Let me start by saying, as we head into a critical calendar event, which is, you know, the 1 June start of the annual hurricane season—we have come off three busy hurricane seasons—you will have a ready, full-up Coast Guard ready to do the Nation's business here.

The lingering effects of the shutdown, I think we are 75 percent reconstituted. Some things that we never get back, we had to defer boat maintenance periods. Those are our fleets of hundreds of small boats. Cutter maintenance periods, some of that just got pushed to the right.

We had furloughed contracting officers, so you just can't do that kind of work. That is not recoverable. My oral testimony really accentuated, as did my written testimony, readiness being my top priority. So for an organization that is struggling with readiness, the shutdown does not help that. It sort of exacerbates that.

But that said, ma'am, I think we are about 75 percent, 80 percent there. In the next month or so, I think we are going to be back to a good place. Things like parts on the shelves, our big parts warehouses out in Baltimore, mostly staffed by civilians, and that is in Mr. Ruppertsberger's district there, they are what we call the surface forces, logistics center, the warehouse. There is some catch-up ball. But if we have been able to pay our bills, restock our shelves, and we are on the road to recovery.

The one thing we just can't get back is some of that deferred maintained. But we will get after that. The Coast Guard is a pretty darn resilient and adaptable force, ma'am.

Ms. ROYBAL-ALLARD. Well, I am sure that it is frustrating to be faced with these inefficiencies and wasteful byproducts of the shutdown when you have limited resources and that you have worked so hard to attain.

Admiral SCHULTZ. Yes, ma'am.

Ms. ROYBAL-ALLARD. But I appreciate the fact that as always the Coast Guard does a lot with little.

Admiral SCHULTZ. We are trying to change. I mean, we are trying to do more with more, but—

Ms. ROYBAL-ALLARD. And I am trying to help you change that.

Admiral SCHULTZ. Thank you.

Ms. ROYBAL-ALLARD. Admiral, as I mentioned in my opening statement, we were pleased to be able to support the procurement of the new Coast Guard assets in our fiscal year 2019 bill, includ-

ing for of the first Polar Security Cutter to replace the aging *Polar Star*, and to begin to fulfill the needs of the Coast Guard in the Arctic and Antarctic. And I know you have prioritized expanding activities in the Arctic during your tenure. Could you highlight for us the importance of the missions the Polar Security Cutter will undertake?

Admiral SCHULTZ. Absolutely, Madam Chairwoman. And we are very appreciative. The \$650 million on top of the previous year's appropriations will allow us to do this contractor work here in hopefully the next 4 to 6 weeks.

The Arctic is no longer an emerging area. The Arctic is a national priority. And today the Coast Guard is really the only surface presence up there. And we are not in the Arctic much. We were up there with our ice ship, the medium endurance breaker, medium breaker *Healey*, in the fall for serving three customers, National Science Foundation, Office of Naval Research, and the NOAA, National Oceanic and Atmospheric Administration.

But that ship really—medium breaker, providing important science work that supports the Nation's interests there, or one heavy icebreaker is really limited to its annual trip down to McMurdo, the trip I talked about. We go down and we break in to the McMurdo ice station. This year, we broke through about 18 miles of heavy ice. Last year, it was more than 70 miles.

The U.S. Antarctic program is undergoing their major recapitalization. For the next 5 years, 4 or 5 years, they have got about a \$450 million there. They are absolutely critically relying on the *Polar Star* and relying on the *Polar Star's* ability to make a path for the *Ocean Giant*, the replenishment ship. So we are at a critical juncture there.

The first Polar Security Cutter, ma'am, absolutely just gives us some ability to replace *Polar Star*, and that is predominantly going to be focused on going to Antarctica. It is really when we get into Polar Security holes number two or three when we have some capacity to increase our presence. And I testified by noting presence equals influence in the Arctic. We won't really push into that until we are into those subsequent Polar Security holes, ma'am.

Ms. ROYBAL-ALLARD. Okay. I was surprised to see that the president's request proposes just \$35 million to continue the Polar Security Cutter program, which I understand would simply continue, as you said, support for the program office. And I remain concerned that the administration's budget isn't aligned with the funding projections in your 5-year capital investment plan as well as the program of record for certain assets.

Do you feel confident that the fiscal year 2019 appropriation is sufficient for procuring the first PSC? And are you comfortable not having additional procurement funding in fiscal year 2020 for the long lead time material for the second PSC, for instance?

Admiral SCHULTZ. Madam Chairwoman, I appreciate the question. First and foremost, the \$675 million did include \$20 million towards long lead materials for the second Polar Security, as you and the committee know, and for that we are very appreciative. Third-five million does allow us to maintain the program. We have yet to award the detailed design construction contract, and that is imminent, as we talked about.

There are clearly, if you go to our CIP, there was, you know, a bigger number there. There are clearly potential advantages in buying additional long lead materials earlier, such as azimuth pod propulsors and things like that. There are some, you know, economic benefit of buying those early and buying them in quantity. But we can absolutely press forward with the \$35 million on the Polar Security Cutter, anticipating a larger number in the 2021 budget, as we start marching towards the second Polar Security Cutter acquisition.

Ms. ROYBAL-ALLARD. OK. Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you, Madam Chairman. Again, Admiral, thank you for being here and for all that you do for our great nation.

Admiral, in fiscal year 2019, in the omnibus, the conferees provided \$340 million, sir, for six new fast response cutters. On increase over the 2019 budget request, there are still cutters outstanding under the program of record. The 2020 budget request only provides \$140 million for two new cutters. Admiral, why is the Coast Guard proposing a reduction to this program? And my question would be, are the cutters no longer needed, sir?

Admiral SCHULTZ. Let me start in reverse order, if I could, Congressman Fleischmann. The cutters are absolutely needed. We would love to continue momentum towards our domestic program of record of 58 fast response cutters with the support of the Congress. We have four of six that are overseas deployed in support of the naval central Fifth Fleet commander working for CENTCOM that you also funded, and I think that is a great story.

Ideally, 58 fast response cutters domestically, six fast response cutter to support our contributions to the CENTCOM theater, that would be the desired end state. The two fast response cutters in the 2020 budget are really a reflection of the reality, and we are one of 22 agencies that resides within the Department of Homeland Security. As a service chief, as component head, I am tasked to manage to a top line.

We talked about the readiness challenges, a little bit of flat funding for the good part of the last decade here under the BCA levels. And, sir, bottom line it comes down to making trade space in the budget to support the OPC and other ongoing acquisitions programs.

Mr. FLEISCHMANN. Yes, sir. Thank you. The building contract stipulates that orders are to be made in increments of four, six or eight cutters. Will the contractor accept an offer to build only two cutters?

Admiral SCHULTZ. Sir, we will have to go back to the contract, if the enacted budget reflects the two. We will have to see what the maneuver space there, how we can work on the shoulder appropriations here, sir.

Ideally, we have seen tremendous support from the Congress here on our—what we now call PC&I, our former AC&I acquisition budgets. Just frankly, I think on average, the committee and the Congress has plussed us up about \$600 million, and the FRC program has been, I don't want to say a favored program, but a program that the Congress has very much embraced. So there is a lit-

tle bit of, I guess, aspirational strategy as we had to play to a top line here, too, sir.

So we will work and see what is in the realm of contractual flexibility and maybe hold out a little bit of hope that this might be a program that Congress remains keenly interested in supporting.

Mr. FLEISCHMANN. Thank you, sir. Is the \$140 million an estimate on OMB's part for the cost of two cutters? Or is the price stipulated in the contract?

Admiral SCHULTZ. Sir, I have to go back and give you an answer. The \$140 million is the two hulls and some other program, I think, costs in there. But, sir, I would like to take that one for the record and circle back with your staff, if that is amenable to you.

Mr. FLEISCHMANN. That is fine, sir. Yes, sir. After the funding in 2019, how many cutters remain outstanding on the program of record, out of how many total, sir?

Admiral SCHULTZ. Sir, I have got to get you back on the numbers. We are starting the crew, an additional four in the 2020 budget, so we just took acceptance of the 33 hull down in Key West last week here. I had the privilege of commissioning the 31st.

I believe at the end of the day, sir, with the proposed number, that it gets us to 54. But I would like to bring that back to you on that other question. I will just pair those two together, if that is adequate.

Mr. FLEISCHMANN. Yes, sir. I see also that once again the budget proposes to skip a year of funding and acquisition for the HC-130J project. I know the HC-130 is important. To quote the budget request, HC-130J is a major contributor to performance of the Coast Guard's statutory missions with specific contributions to DHS and the Coast Guard program of maritime law enforcement, maritime response, defense operations, and maritime transportation system management.

Admiral, I am probably not the only member of this subcommittee with this question. But what is the rationale for eliminating the funding in the 2020 budget request, sir?

Admiral SCHULTZ. So, Congressman, on the HC-130J program, the HC-130J are absolutely great aircraft. C-130s writ large are great aircrafts. The Js are going to get us a leap forward in technology. We fielded the first two Js of the fleet we have to date up in Alaska, and by the end of this fiscal year, we will have five C-130J operating from Kodiak. Then we will roll into our second air station next year out in Barbers Point.

The 2019 omnibus included funding for a 16th C-130J. We are absolutely appreciative of that. Not a surprise to the committee, but we have not included the C-130Js in our budget ask in previous years. That is, as we make top-line decisions, that is one that just has not been able to fight into the mix. But the Congress has seen fit that that aircraft is absolutely essential to our maritime patrol, long-range force laydown, sir, and I think I will constrain my answer to that.

Mr. FLEISCHMANN. Yes, sir. Thank you, Admiral. Madam Chairwoman, I yield back.

Ms. ROYBAL-ALLARD. Mr. Cuellar.

Mr. CUELLAR. Thank you, Madam Chair. And, Admiral, it is good seeing you.

Admiral SCHULTZ. Good to see you, sir.

Mr. CUELLAR. We spent a couple days this weekend in my lower part of my district, in the McAllen area, with Senator Jon Tester. Let me go over a topic that we talked about yesterday, and that was—as you know, the Coast Guard has probably the best re-enlistment rate of any military branch. Around 92 percent of the first year Coast Guard re-enlisted last year, and more than 40 percent of the Coast Guard enlisted recruits are still active after 20 years, and I believe 60 percent of your officers stay active after 20 years or more.

But there seems to be a problem with females, in one particular category. Coast Guard is losing nearly 50 percent of the year group between 10 and 12 years of service among your female officers, and so my question again is, what are we—you know, why is that happening? And what are you all doing to make sure we keep them—

Admiral SCHULTZ. Yes, sir. Well, thank you for the question. And thank you for the privilege of traveling with you throughout lower Texas there. That was very insightful I hope for Senator Tester. It is always a pleasure for me to get down there and see what our DHS team is doing, sir.

You know, on women's retention, we are taking the final results of a women's retention study I believe next week, if not the following week. This has been a yearlong effort. We are very excited to better understand decisions women make. If you look at our ranks, across our ranks, officer, enlisted, combined, we are less than 15 percent women Coast Guard employees in the workforce. That is approximately 50 percent. So we are not competing to maximum advantage that we need to.

What we found in that study in the initial results are, you know, the first 0 to 4, 0 to 5 years of enlisted member, woman's career, or female woman officer's career, the pace is pretty steady. From about 5 years to when you get out here to the—you know, about the next 12 years of their career, you start to see a delta. That delta is somewhere between 12 percent and 13 percent. It is pretty consistent in both the officer and enlisted ranks. So it is not the 50 percent delta, but it is about a 12 percent difference.

And what we are trying to do is really understand, what do we have to do in there? And what adjustments can we make to make sure the Coast Guard is, you know, an employer choice for all men and women? We do have some challenges there, and I think the study has helped us understand that.

We went out and did focus groups in more than a dozen locations in the Coast Guard. We spoke to more than 1,000 women. And this was from Alaska to Hawaii, East and West Coast, the Great Lakes, Gulf of Mexico. We had a great dialogue. We had some men sitting at the table to understand the impacts that are not just specific to women's retention, so we could segregate out the facts.

And, sir, I think we have an action plan. I have stood up when I came onboard here and we have actually got the bodies in place, a seven-person team, what we call the personal readiness task force. Sometimes in the past, we have done studies, but we have not done a good job of actioning studies. This task force has been poring through the early reads of the plan. They are waiting for the

final results. And we are going to get off to the races and do some things that make us an employer choice. Equally so, hopefully we can drive up that women's retention.

And some of that, sir, is more flexible policies, flexible policies for family members, for child givers, you know, caregivers. We bumped up—it is 41 days, just shy of 6 weeks, for child birth, for a new mother, a new parent. And then there is an additional 41 days, gets you a total of 12 weeks, secondary caregiver is upwards of 3 weeks. So that is about the max we can go. I don't think any other service is quite as forward leaning as that.

We are looking at focusing on areas like child development centers. That is obviously an issue as we look at this early results that affects people's lives. We are a geographically disperse workforce along the coast in many high cost areas. Childcare ranges from \$1,000 a child on the low end to \$2,500 on the high end. And the committee was wonderful in giving us \$2 million last year for childcare subsidy. I have got about 1,060 children enrolled in that. And I would say more than 50 percent are in those high-cost areas. So that is is very helpful. And, sir, we are just leaning in to make a difference here.

Mr. CUELLAR. All right. Well, thank you for that. And just to finish this, I also appreciate the partnerships that you have with the minority serving institutions.

Admiral SCHULTZ. Absolutely.

Mr. CUELLAR. And if you don't mind, maybe one of your staffers can give us a list as to who you are working with, we would appreciate it.

Admiral SCHULTZ. Absolutely.

Mr. CUELLAR. Because that is good for pools of applicants, but also in the STEM areas and other areas it will be helpful, too.

Admiral SCHULTZ. Absolutely.

Mr. CUELLAR. Not only to you, but to your country.

Admiral SCHULTZ. Yes, sir. We have a lot of good news stories going on, and we will get you a list of that, and would welcome your interest in participating with any of those institutions, sir.

Mr. CUELLAR. Thank you so much.

Admiral SCHULTZ. Yes, sir.

Mr. CUELLAR. Thank you. Thank you, Madam Chair.

Ms. ROYBAL-ALLARD. Mr. Newhouse.

Mr. NEWHOUSE. Thank you, Chair Roybal-Allard.

Admiral, welcome to the committee.

Admiral SCHULTZ. Thank you, congressman.

Mr. NEWHOUSE. Thank you for your leadership and the work you do with the men and women of the Coast Guard as they carry out their mission. We appreciate it very much. Thanks for the update today on how things are going.

I am interested in your—I guess your unmanned systems. I understand that you have had some experience recently with those. The Stratton, I believe, is the ship that—

Admiral SCHULTZ. Stratton is a national security cutter, absolutely, sir. We have deployed what we call a small UAS—and I don't want to get ahead of your question, sir.

Mr. NEWHOUSE. No, that is—I just wanted to give you an opportunity to talk a little bit about that, educate us somewhat on how

that complements the NSC's operations, and how could you—or how could we together expedite that?

Admiral SCHULTZ. So with the support of the committee, sir, we are now fielding a recent contract award in December to Insitu. They make the ScanEagle. It is a small UAS, about 8-foot wing-span.

Mr. NEWHOUSE. Just happens to be in Washington State. That is a coincidence, I am sure.

Admiral SCHULTZ. Sir, you can launch that ScanEagle off the back of a flight deck on a national security cutter. It is got about a 12-hour endurance profile. The cutters that have sailed with that, on some of the prototype work we did, the sailors don't want to go out without it again. It is that much of a game-changer. It is terrific.

The National Security Cutter *Stratton* that you spoke about, I think, had the ScanEagle involved in about 28 interdictions tied into the removal of 40,000 pounds of illicit cocaine at sea.

Mr. NEWHOUSE. Oh, my.

Admiral SCHULTZ. So there is a lot of potential. We are the—there is a \$9.2 million ask in the 2020 budget here that is before you. That will allow us to put small UAS capability on two NSCs a year. One of the things I said in my state of the Coast Guard, I would love to see if there is a means to possibly accelerate that, because it is truly game-changing capability.

We are actually doing with a little bit of money we had in prior years' appropriation. We have done a land-based test in Puerto Rico back last spring, and here in early April we are going to do another land-based test down out of Corpus Christi, TX, as well, so fantastic capability at sea. We are trying to see what this might do as a land-based opportunity, as well, sir.

Mr. NEWHOUSE. As well as at sea.

Admiral SCHULTZ. As well as at sea.

Mr. NEWHOUSE. It certainly seems like it extends the reach of the Coast Guard and it extends your capabilities, so it is exciting to be able to watch this technology be put in place.

Admiral SCHULTZ. Congressman, we have a national security cutter in the Eastern Pacific where 85 percent of the drugs transit at sea. That area is—if you took the United States and sort of turned it about 30, 40 degrees its axis, that would sit in the Eastern Pacific. We have the equivalent of about six to seven ships there on a given day, Coast Guard cutters. That would be like patrolling North America with six or seven police cars.

Mr. NEWHOUSE. Wow.

Admiral SCHULTZ. The key enablers there are over the rise in boats. Our national security cutters can deploy three boats. It is really maritime patrol, aircraft responding to intelligence. It is far reaches. These ships are going out west of the Galapagos. So a maritime patrol airplane comes out there in response to intelligence, has an hour or 2 on-scene, finds the target. That national security cutter is still hours away. The plane runs out of gas. You can use all your planes just staying on top.

The UAS allows us to bridge that gap. We can get that UAS 50, 70 miles away from the ship. That is 3 or 4 hours of time you buy where the UAS sits on top, whether it is electrical, optical, infra-

red. The smugglers do not see it. The ship can see what is going on. When they get there and launch their boats, it is a much safer situation.

So truly game-changing impactful capability, and we are very appreciative of the committee's support for the capability.

Mr. NEWHOUSE. Good, good. Well, we look forward to continuing working with you on that.

Admiral SCHULTZ. Sure, thank you for the question.

Mr. NEWHOUSE. Yeah, thank you for your answer. Thank you, Madam Chair. I will yield back.

Ms. ROYBAL-ALLARD. Mr. Ruppertsberger.

Mr. RUPPERSBERGER. Yeah, first, Admiral, I have a lot of respect for the Coast Guard. I really didn't work with the Coast Guard until I came here. You always seem—you seem to be there for our Americans whenever you need to be. You don't have a lot of money. I think it was a good move for you to come into the umbrella of Homeland Security, and I think you are probably the most competent operation that we have there.

And I hope we can help the others bring up to where you are. And you have been underfunded. And people on this committee are going to try to help you any way we can. And I know the chairman and ranking member feel that way, too.

As you said, I represent a portion of the Coast Guard yard in Curtis Bay. We were able to secure about \$25 million in the recently passed omnibus to address your need for a new travel lift. And it is essential infrastructure which will allow those stationed there to performed dry dock maintenance on their 500-ton, 150-foot fast response cutters.

Now, this was listed as one of the top three major acquisition systems, infrastructure projects on the Coast Guard's unfunded priorities list. My question—does the \$25 million cover the full cost of the project? And could you provide a tentative timeline for its completion?

Admiral SCHULTZ. Absolutely, Mr. Ruppertsberger. So, first off, appreciate the committee's—I think it was \$22.5 million towards that project. We have a program, what we call the RDAP, recurring depot availability program. We have been doing that with the 87-foot coastal patrol boats at the yard. It has been a very great program, great results. We are modeling that for these new fast response cutters we are fielding.

The \$22.5 million buys us the infrastructure for the pier work, some building work. There is a paint booth component of that. There is actually about another \$5 million piece for the actual travel lift, but we are going to be able to support that through the capital working fund the yard has. So that is the appropriate way to fund that.

So I think, sir, at the end of the day, we should be in good shape. And I think it is 2021 and 2022—2021 I think will be—we will have some of that infrastructure work, 2022 we should have that facility up and running, sir.

Mr. RUPPERSBERGER. All right, the other question I have is the icebreaker. I know our chairwoman cares very much about this. The Russians consider the Arctic to be the next frontier, with environmental changes, ice and permafrost is retreating, exposing valu-

able land and navigable waterways. New opportunities are rising for oil and gas drilling, as well as access to untouched fisheries.

Now, we have both Russia and China have recognized this development and are scrambling to establish a foothold in the region. In this regard, America is coming up short. Russia currently has 44 working icebreakers, seven of which are nuclear-powered, while the United States has two in operation. You just said maybe even one. And I know putting new breakers in the water is just as high a priority for you as it is for all of us I think on this committee.

Now, my question is, what impact would an unchecked Russian-China presence in the Arctic region have on our national security and sovereignty? Also, there is a moratorium on fishing and unexplored, untapped oil reserves in the Arctic outside of our exclusive economic zones. Do you feel that without American assets in the region, we will be able to enforce international law and stake our claim to the natural resources?

And lastly, I have heard in the past that the Coast Guard needs three heavy and three medium icebreakers to counter Russia and China's influence in the Arctic. Is this number still accurate, so we can focus our goals to help you?

Admiral SCHULTZ. Yes, sir. Well, let me start in reverse order. So my strategy—I have talked about consistent with the high latitude studies has been a minimum of six icebreakers. I frame that conversation as three that are Polar Security or heavy breakers, like the one we are talking about awarding here in the coming weeks, and then three potential medium or less capable breakers.

There is probably a conversation that is some hybrid of that, but that is consistent with the high latitude study. Russia does have upwards of four dozen icebreakers, and your numbers are correct, seven nuclear, building more breakers.

I would say the Russian Arctic, you know, when you look at Russia's border in the Arctic, they do have a long Arctic region. We are not sensing Arctic presence here off of the U.S. Alaska Arctic. But Russia is deriving 20 percent of their GDP from the Arctic. They are re-establishing themselves in bases. They are looking at taxing northern sea routes, shipping.

So they are going to derive a lot of economic benefit, which makes Russia a more difficult global partner here, I think, when their economy gets stronger. Right now, they are meddlesome. With more resources, they are more meddlesome, more globally reaching.

Up in the Arctic here off Alaska, where we are really looking to project more presence. You know, presence does equal influence. China has been up there, you know, 4 of the last 6 or 7 years with the Xue Long, their research ship. They have just launched the second icebreaker, the Xue Long 2, last summer. I anticipate that being operational in the not-too-distant future. They are talking about building a heavy breaker.

They are not an Arctic nation. They are a near Arctic self-declared state. And they are up there. They are doing—you know, obviously, they have interest. They are paying attention to us fielding fifth-generation fighters to places like Elmendorf. They are paying attention what we are doing with undersea cabling.

As you mentioned, Arctic is rich in natural resource. About 13 percent of the untapped petroleum are in fairly shallow water depths up there for potential deriving here for our energy needs, 30 percent of the untapped LNG, trillion dollars of rich minerals that we care about. So the Arctic is a geostrategically important place, sir. And we do need to pay attention what China is doing.

China is also in the high latitudes of Antarctica. They are building additional science stations down there. And I think the Coast Guard, as the face of the U.S. surface capability in the high latitudes, you know, we can't get there fast enough. My strategy was six, three, one. The one was now. And with the help of this committee, we are going to get after that one here. So that is a great—this is 12 years in the making, and we are very appreciative of the committee's support.

Mr. RUPPERSBERGER. Well, I know the chairwoman feels that way, too, so this committee is going to try to help you any way we can because it is national security.

Admiral SCHULTZ. Thank you.

Ms. ROYBAL-ALLARD. Because I call on Mr. Palazzo—I apologize for that discussion that was back here—but we are being told that votes are going to be in just a few minutes. So it will be an additional 15 minutes that we will have. So if everybody can ask their questions the first round, and because otherwise you may have to be here for a half hour to 45 minutes.

Admiral SCHULTZ. Yes, ma'am. I will try to shorten my answers, too, ma'am. I apologize.

Ms. ROYBAL-ALLARD. Okay. So, Mr. Palazzo.

Mr. PALAZZO. Thank you, Madam Chairman. Commandant—

Admiral SCHULTZ. Good to see you, sir.

Mr. PALAZZO. Great to see you, too. Really appreciate what your coasties are doing. I know the shutdown was tough on them and their families, and hopefully moving forward legislatively we can find a way that that doesn't happen again. But we appreciate their service and especially their sacrifice. Please pass that message along on behalf of this whole committee. I think one—you are going to find some bipartisanship when it comes to our Coast Guard here.

My remarks pretty much aren't new to your predecessor. I think I have asked some of these same questions. And there has been a lot of talk about the southern border, but there is also a maritime border. And I think coast states and eastern and pacific, as well, it is a border that we take very seriously.

And I know just from news reports in February of 2019, I believe you all, the Coast Guard sees 17 tons of cocaine, that is almost 35,000 pounds of street value of almost \$500 million. And I think the more that we squeeze the southern border to secure it, to protect Americans, we may be seeing some increased activity on our seas and in our maritime domains.

Can you tell me a little bit about what the Coast Guard is doing on the war on drugs? Again, last year, you seized—more than half of all cocaine seizures came from the United States Coast Guard, which, by the way, thank you for keeping those deadly drugs out of our communities and out of our states. I think it is extremely important. But I will give you a moment to talk about it.

Admiral SCHULTZ. Sure. Well, Congressman, I would say this. Thank you for the support. I mentioned earlier we interdicted about 209 metric tons last year. If you look at the last 3 years, 1.4 million pounds of illicit, uncut cocaine. We rolled up about 1,600 smugglers at sea. Our Coast Guard strategy is to push the border far from U.S. shores. So we push the border about 1,500 miles off the coast of southern California, off the Gulf Coast.

We interdict large loads of cocaine at sea when most vulnerable. Those drugs—their destination isn't California by sea. Their destination is Mexico. Their destination is Guatemala, El Salvador, the Central American corridor, where it gets broken down into smaller loads, associated violence, corruption. It creates instability in governments. So those are the push factors that have people, families like ourselves with children that live in Honduras, El Salvador, Guatemala, the northern triangle country, that make the difficult decision, because there is no future for their children in their home countries, to send them up through Mexico to try to get to the southwest land border in Texas and California.

So our work, I think, is absolutely seminal. It is apolitical work. I think there is bipartisan agreement that stopping those drugs at sea do help the push factors. And we are very proud of the work we do down there. We partner with—CBP provides, you know, almost 40 percent, 50 percent of the maritime patrol aircraft.

We partner with international—with U.S. Southern Command. So I am a force provider of the Coast Guard to SOUTHCOM. We commit to four ships around the calendar year. We strive to be somewhere six to eight ships. We are about 6.7, 7 plus the last couple years, and we remain committed. It is consistent with our Western Hemisphere strategy, sir, and we remain committed to the fight.

Mr. PALAZZO. And we are glad you are committed to that fight, and we want to give you the continued resources.

Admiral SCHULTZ. Yes, sir.

Mr. PALAZZO. Whether it is ships or technology or the UAS's that Congressman Newhouse mentioned, to expand your ability to—I want my colleagues to have time to answer, but I can't pass this question up. The Jones Act, why is it important to our economic and national security?

Admiral SCHULTZ. Sir, the Jones Act—my predecessors have stood for the Jones Act. The Jones Act is important to the security of the nation. The merchant fleet here, our ability to move military supplies in a military outload to support—let's say we had a large theater war in the Pacific and that part of the world. That is important.

You know, I think economically, you know, folks have invested in that. The Jones Act gets attacked that there are cheaper ways to do business. I would say, I think there is a lot. The Jones Act has been in place here for about 100 years here, and it serves a very important—continually important service.

I think before there is any meddling with the Jones Act, people should really step back and have an informed conversation about all the puts and takes and the impacts to national security.

Mr. PALAZZO. Thank you, Commandant. I yield back.

Admiral SCHULTZ. Yes, sir.

Ms. ROYBAL-ALLARD. Mr. Price.

Mr. PRICE. Thank you, Admiral. Good to have you here with us. I will shorten my comments here and ask a question very quickly. I think it is an important question.

I don't want to pass by the opportunity to thank you for the good work your people did in North Carolina and the Carolinas generally with Hurricane Florence last summer. They saved many lives in my state, and we once again—the Coast Guard distinguished itself in these disaster—

Admiral SCHULTZ. Sir, we are pleased to partner with your very capable emergency response folks in the state of North Carolina. It is a good team effort down there.

Mr. PRICE. Yes, sir. We know that is true, but you are the best, and we are very grateful. I want to move directly to your operations and support budget, which has been basically flat-lined for the last 8 years. In your state of the Coast Guard 2019 message, you mentioned that this has resulted—and I am quoting you now—this has resulted in deferred maintenance, a strained and under-sized workforce, and antiquated information systems.

Let me, if I might, stress the workforce piece of that and ask you to comment on it. You are an extraordinary organization. You have always done more with less. But that shouldn't preclude you from getting the funding increases you need. It doesn't make sense that you are providing—we are funding new vessels. We are funding new functions. But without an increase in maintenance funding, support for your personnel and their families, it just doesn't fit. All need to go together.

So we want to know how we can best help you achieve your workforce goals. Where do you see the most urgent, unmet needs? And what is the overall challenge you have with respect to recruiting and retaining personnel? Are your benefits competitive? Are your salary increases competitive? I mean, what would be your prescription? More money, yes, but more—but maybe spending that money in some strategic ways. What would you suggest for addressing these needs?

Admiral SCHULTZ. Yes, sir, thank you for that question. Consistent with my comment to the chairwoman about, you know, retention of women, we need to recruit in different places. We need to retain more—recruit and retain more underrepresented minorities, more women. There are some resource components, you know, recruiting, more recruiting officers.

We cut back our recruiting officers years back to make space for capital assets. I would say when you look across the DOD services, tuition assistance is a benefit they give their folks, so you can do some college work and derive a benefit. We have capped our tuition assistance for active-duty members at 50 percent. We were doing this every year, and it was very frustrating folks. We just said we can't get above 50 percent. That is a competitive tool.

With the support of the—with the 2020 budget includes \$2.7 million to do tuition assistance for reservists. We have not offered a reservist tuition assistance in more than a decade. So if you are a young member in the Coast Guard and you have served your nation 4 years, 8 years, but there are other life callings you want to do, family situations don't always serve, I would like a reservist to

look—or Coast Guard active duty member look and say, boy, I really love the culture, I love the work, but I have other things in my life. I have to take care of ailing parents. It is not, you know, my spouse's career.

Offering tuition assistance to reservists is an attractive thing to keep them in. Right now they are jumping ship and going to go join the National Guard, drill in their local armory. We require them to drive 300 miles to drill because we don't have reserve people everywhere, but that ability to offer the reservists some tuition assistance is game-changing.

I talked about child development centers. We really—you know, we don't live on big bases. If you go over here to JBAB, Joint Base Anacostia-Bolling, they have a state-of-the-art facility. They feed the kids. They are investing. They are hearing the noise about housing across the nation. There is a clarion call on DOD with all the defense leaders when they come up here about, what are you doing with housing? Less than 10 percent of my workforce is in housing. Some of that housing is old. We have had very little money to invest in that housing.

We have got a \$1.7 billion backlog, so we are fixing broken roofs on buildings. But those things all, you know, factor into people's willingness to stay. It is the best workforce, brightest workforce we have ever seen. One of the big assets that will be coming forward in the 2020 budget has \$14 million in the PC&I line item is for IT, or what we call C5I infrastructure, command, control, communications, computers, cyber, and intelligence. That used to be C2 when I was a young guy, command and control. But now our mission platform that supports all our technology is very old, congressman, and we have got to make some investments.

So I think all these things factor into a Coast Guard that is attractive to the best and brightest in America. We have no trouble recruiting people. I want those people to stay in. And Congressman Cuellar talked about, you know, almost 40 percent are enlisted people go to 20, 58 percent of our officers go to 20. Blended retirements start on the 1st of January, so at 12 years now, you do a thrift savings plan, you derive a 2 percent benefit a year, so you get 40 percent plus your TSB, it is going to be hard to get folks to 20 unless they see the Coast Guard really committed.

It is electronic health records. There is money in the 2020 budget for that. We are appreciative. It is a sufficient number of docs and things like that, sir. So a lot of those things speak to that attractiveness and being an employer of choice.

Mr. PRICE. Good, thank you.

Ms. MENG. Thank you, Admiral, and thank you, Chairwoman. I will try to speed up my phrasing of the questions. Thank you for your service. Wanted to talk a little bit more about the workforce diversity in terms of if the Coast Guard is planning to allocate any funds, any steps you will be taking.

And I know that the Coast Guard is releasing a study on the retention of women. And is there anything like that in the works in relation to diversity and recruitment?

Admiral SCHULTZ. Yes, ma'am. So working backwards, based on this study, it was through the HOSAC, working with Rand, our homeland security advisory group, we intend to launch a study I

think as soon as this summer, an underrepresented minority study, about retention, attracting and retaining underrepresented minorities. We are using this women's retention study trying to get that perfected. I thought we would have these results maybe before the end of the last calendar year. With the shutdown, we lost a little time, but now we are kind of doing the puts and takes. We will get the final results.

That will help us get out the door more effectively. So that is coming. This personal readiness task force is an action body. So you are going to see some—I made some announcements last week about where we have women, moms, new parents that step out of the workforce. In the past, if you are a small geographically remote unit, small number of people, and you are a woman and you are pregnant and you step out to go take care of your new child or adjust to your new family situation, there is a certain pressure on you, because your colleagues kind of feel like you are jumping ship.

And now we are going to take reserve surge capacity, send a body to that chair—the work goes on, you can step out, we are trying to create a space where family and work are not mutually exclusive. You can find the balance. We are supportive. We are working on more permeability for the workforce, more flexibility.

Ms. MENG. Thank you, sir.

Admiral SCHULTZ. Yes, ma'am.

Ms. ROYBAL-ALLARD. Mr. Aguilar.

Mr. AGUILAR. Just real briefly, Admiral, specific to the kind of SOUTHCOM, you know, AOR in the Pacific, it is my understanding that our ability to identify drug smuggling in the Pacific, building off of what Mr. Palazzo was talking about, is far greater than our capacity to interdict.

Admiral SCHULTZ. Yes, sir.

Mr. AGUILAR. And so a good day on the water is equivalent to—from a value and a tonnage perspective, probably a year at a port of entry. And so what more can we do to assist in these efforts? We know you partner with other countries, and that is amazing, but what can we do? And is this an issue of we need more ships? Would adding a naval LCS to these efforts help, as well?

Admiral SCHULTZ. Well, I would say this, Congressman. Thanks for your question. Absolutely, that is part of the conversation here. The ships that we are building, continuing to focus on recapitalizing our offshore patrol cutters, replacing those 52-year-old, soon to be 60-year 210 cutters, the 30-plus-year-old 270s, the OPC program, if we can maintain momentum on that, that is essential. Things like the small UAS that Congressman Newhouse, asked about, potentially some longer-range MQ-9-type capabilities. We are interested in that. Maritime patrol aircraft, the C-130s are absolute contributors to that. CBP, continued support for CB pier and marine.

I think those are the key enablers. You know, we can always use more ships. I am not going to sit here and say, you know, a Navy combatant—I understand the demands on the CNO. He has got an increasingly difficult—Russia, we talked about that earlier. He has got a lot of challenge and problem sets in the South China Sea. The Navy lost a couple missile shooters here, you know, the *Fitzgerald* and the *McCain*.

So I would say maintaining momentum on what we are doing and some of the people things I think would make us the most ready Coast Guard we could be.

Mr. AGUILAR. We would love to talk about future resources. Thank you.

Admiral SCHULTZ. Yes, sir, thank you.

Ms. ROYBAL-ALLARD. Admiral, I apologize for us all having to leave.

Admiral SCHULTZ. Madam Chairwoman, I understand.

Ms. ROYBAL-ALLARD. We will submit others for the record.

Admiral SCHULTZ. Yes, ma'am.

Ms. ROYBAL-ALLARD. And thank you very much.

Admiral SCHULTZ. And thank you for the privilege of being here. Thank you.

[Material submitted for inclusion in the record follows:]

QUESTIONS FOR THE RECORD (QFR)**From March 26, 2019 Hearing:****“Review of the Coast Guard’s FY 2020 Budget Request”****Before the House Committee on Appropriations Subcommittee on Homeland Security
(HAC-HLS)****Witness: Admiral Karl Schultz, Commandant, U.S. Coast Guard****QFRs Submitted by Congressman Price****QFR #1****CONGRESSIONAL ASSISTANCE TOWARD WORKFORCE INITIATIVES**

BACKGROUND: Per Congressman Price, ““The Coast Guard’s O&S budget has been basically flat-lined for 8 years, resulting in deferred maintenance, a strained and undersized workforce, and antiquated information systems.”

QUESTION PART-1: How can Congress best help the Coast Guard achieve the Service’s workforce goals?

ANSWER PART-1: The Coast Guard is responsible for an extraordinary breadth of missions with a workforce that is one-fifth the size of the next smallest Armed Force (the Marine Corps’ active and reserve component end-strength is ~220,000). We accomplish our missions by ensuring we have the right people, with the right skills, in the right place, at the right time. However, our purchasing power continues to erode under the Budget Control Act caps. These reductions continue to challenge our ability to match force strength with mission demands and stresses the training system necessary to ensure we meet today and tomorrow’s mission challenges. For this reason, we do not seek to grow the workforce for the sake of growth—this simply drains precious resources. Instead, the Coast Guard identifies specific missions that we know are under-manned and explore creative ways to address the shortfall. We are thankful for Congressional support during each year’s budget cycle as we convey our workforce requirements through our budget requests. Furthermore, we appreciate Congressional assistance supporting the myriad workforce and family programs that make the Service more resilient (e.g. child care subsidies, military pay raises, etc.).

QUESTION PART-2: Where does the Coast Guard most see an unmet need in the workforce: competitive benefits and incentives? Issues with recruiting or retaining? Where?

ANSWER PART-2: The Coast Guard has a high retention rate within its workforce—both military and civilian. In fact, our military workforce has the highest retention rate of all five military services. That said, the Coast Guard does compete for the same pool of military applicants as the Department of Defense, and we are challenged to provide similar financial recruiting incentives. The Service inherently has fewer recruiting offices, a smaller recruiting footprint throughout the country, and limited incentive programs for accessions.

That said, the Service maximizes the recruiting resources as necessary to target the most critical subsets of the workforce.

QUESTION PART-3: Please tell me more about any needed improvements to the Coast Guard's tuition assistance program.

ANSWER PART-3: The Coast Guard sets Tuition Assistance (TA) limits to optimize the program's benefits and ensure maximum use by service-members. The Coast Guard's use of TA has gradually increased over the years; however, due to the growing cost of advanced education, it is becoming more and more difficult to maintain similar levels of funding disbursement each year.

QUESTION PART-4: What specifically does the Coast Guard need to enhance the Service's "Child Development Centers?"

ANSWER PART-4: The Coast Guard appreciates the continued support of Congress to help ease the childcare burdens of our members. Since many Coast Guard personnel—unlike a majority of DoD members—do not reside on or near major military bases, the child care subsidy program is the most efficient and versatile means to support our members. While Child Development Centers (CDC) represent the best option to meet childcare needs, they are simply not practical at myriad locations (e.g. small unit bases, along with limited numbers of personnel). Instead, the childcare subsidy programs allows the Service to target each individual where they reside. A program that leverages the benefits of CDCs (large populations areas) with subsidies in areas without CDCs has the ability to assist a greater percentage of Coast Guard members.

QFR #2

EFFECTS OF GOVERNMENT SHUTDOWN ON COAST GUARD & AVIATION LOGISTICS CENTER (ALC)

BACKGROUND: Per Congressman Price, "Unfortunately, the Coast Guard was caught up in a 35-day government shutdown over the demand for \$5.7 billion for border fencing. The Coast Guard was the only branch of the military that was directly affected by this shutdown. One reported effect was on the Aviation Logistic Center (ALC) in Elizabeth City, North Carolina. It was reported that to make up for production lost during the shutdown, roughly 600 ALC employees would have to work over time for five to seven months."

QUESTION PART-1: Can you please comment broadly on the effects of the government shutdown on the Coast Guard?

ANSWER PART-1:

The loss of a paycheck for the Coast Guard's active duty and reservists, and the loss of two paychecks for the Coast Guard's civilians broke faith with the Service's workforce and placed undue financial stress on our members and their families, particularly those most junior.

Asset readiness, including the surface and aviation fleet as well as IT and shore infrastructure, eroded during the shutdown. Planned maintenance was deferred and critical spare parts inventories were drawn down or completely exhausted without adequate replenishment. Payments were not made to vendors/contractors for critical supplies and services, increasing the risk/likelihood that providers would stop work. This resulted in over 300 late payment interest penalties totaling almost \$300,000.00.

QUESTION PART-2: Please comment specifically on the effects of the government shutdown on the Aviation Logistics Center (ALC)?

ANSWER PART-2: The shutdown disrupted ALC's ability to purchase parts and conduct depot level maintenance. In order to minimize disruptions to fleet operations, overtime was increased by 85% (94% increase in hours) after the shutdown.

TUESDAY, APRIL 2, 2019.

TRANSPORTATION SECURITY ADMINISTRATION

WITNESS

HON. DAVID PEKOSKE, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Ms. ROYBAL-ALLARD. The Subcommittee on Homeland Security will come to order.

Administrator Pecoske, I want to welcome you to your first hearing before this subcommittee.

We are pleased to have you testifying before us today.

Members of the public likely interact with the TSA and its employees more than any other component of the Department of Homeland Security.

While air travelers do not always express their gratitude during the process, we do appreciate what the TSA and its employees do to protect our nation.

During the partial government shutdown earlier this year, TSA personnel worked without pay. This was a burden for transportation security officers, in particular, because they earn much less than other civil servants. TSA workers overcame great personal hardship to continue carrying out their duties. There were even reports of personnel sleeping in their cars because they could not afford the costs of continuing to come work.

I hope you will convey our continued support and appreciation for your workforce. I know that you share our concerns and have been an advocate for them.

After making significant new investments in your workforce and to equip it with advanced security technologies in the bill for the fiscal year 2019, I was disappointed to see that the president's fiscal year 2020 budget proposes a cut to TSA's funding.

Many of the cuts are repeats from the past 2 years based on the elimination of activities that the Congress has repeatedly voted to continue—the Visible Intermodal Prevention and Response teams, known as VIPR; the law enforcement officer reimbursement program; and TSA staffing at exit lanes.

There is also a disconcerting mismatch between the budget and the expected growth in travelers, and once again, the budget relies on a proposal to increase the passenger security fee, which is outside of the jurisdiction of this committee and is unlikely to be enacted.

Mr. Administrator, I know the budget request reflects the funding limitations you are forced to live under, but it will be difficult to fill in the funding holes that the budget creates. We look forward to hearing more about the budget request for fiscal year 2020 and

whether it would provide the resources that you need to support your critical missions.

Thank you again for joining us, and I look forward to our discussion. I would now like to turn it over to the distinguished gentleman from Tennessee, Ranking Member Fleischmann.

Mr. FLEISCHMANN. Madam Chair, thank you, and, Mr. Administrator, thank you. I apologize for the delay. We have been voting on the floor. It has been extremely busy today.

Mr. Administrator, I echo the chairwoman's thanks for coming to testify before the subcommittee today on the Transportation Security Administration's fiscal year 2020 budget request. Thank you, sir, for reaching out last week to meet with me and my staff in your budget priorities. I really appreciated that. Put a lot of things in perspective.

I know we talked about this when we met, but I just wanted to reiterate on the record what an outstanding job the TSA team does in Chattanooga at the Chattanooga Airport. I actually told them that I met with you and I appreciate that.

With all the traveling we do between our districts and DC, you can have a great experience or a lousy experience, and often that experience can start with the TSA screening process. For many Americans, TSA might be the only face-to-face interaction they have with a homeland security employee. You have a great group in Chattanooga, sir.

I will have some questions as we move into that part of the hearing. I look forward to your testimony, sir, and I thank you for your time today. Madam Chairman, I yield back.

Ms. ROYBAL-ALLARD. Thank you. Before your testimony, just a few—I look forward to your testimony. And we will put the full statement into the record.

Mr. PEKOSKE. Chairman Roybal-Allard, Ranking Member Fleischmann, distinguished members of the subcommittee, thank you very much for the opportunity to appear before you this afternoon concerning the president's fiscal year 2020 budget request for TSA. I value your oversight and support and thank you for your critical contribution to our mission's success.

It is an honor and privilege to lead the men and women of TSA, and I very much appreciate both of your comments on the TSA workforce this afternoon. In my view, they embody our core values of integrity, respect, and commitment, and as both of you have mentioned, that commitment was so plainly evident during the recent 35-day lapse in appropriations.

I am immensely proud of this team of professionals who include screeners, explosive experts, canine handlers, intelligence and vetting personnel, domestic and international inspectors, federal air marshals, providers of critical support services, and a highly skilled headquarters staff. It is our mission to ensure that our transportation systems used by hundreds of millions of people per year and a lifeblood of our economy remain secure. We are hard at work, and with your help, to provide better security faster.

This includes the CT, or CAT scan X-ray technology you funded in fiscal year 2018 and fiscal year 2019 for carryon bags at our screening checkpoints, and its continuation in the president's budget request for fiscal 2020. It also includes the credential authentica-

tion technology, or commonly referred to as CAT by its acronym, that you similarly supported to strengthen our performance at the very first position in our screening checkpoints, the increase in the numbers of screeners to reflect the strong and sustained growth in passenger air travel, and increases in our canine capability for both passenger and air cargo screening.

The fiscal year 2020 request seeks \$7.2 billion, partially offset by \$4.2 billion from the aviation passenger security fee. It has two overarching priorities. The first is continued investment in checkpoint technology, in particular the CT, or CAT scan technology, and the credential authentication technology. And I will talk about each one separately for just a few moments.

First, with respect to the CT, or CAT scan X-ray technology, 5 days ago, we were awarded our first major contract for 300 X-ray systems. Your demonstration of support for this long-term acquisition was key to our success in obtaining a price that was substantially less than our budget estimates. Not only will this technology provide vastly superior security, but it will also be more convenient for passengers, eventually eliminating the requirement for passengers to take laptops, liquids, aerosols, and gels out of their carryon bags. The fiscal year 2020 request contains \$221 million for approximately 320 more of these X-ray machines and the associated baggage handling systems.

The second piece of the technology is the credential authentication technology. And the fiscal 2020 budget continues the large-scale investment in this technology, deploying approximately 500 additional CAT units that will improve identity and travel verification, improve risk management, and also result in more convenience for passengers who will no longer need to present their boarding pass in most situations at the screening checkpoint.

The second key priority, first being technology, the second is right-sizing our workforce. As you have noted, commercial air travel continues to grow at 5 percent per year. This requires an increase in the size of our screener workforce and the staff who support them. This budget seeks over 1,000 additional screener positions that will allow us to maintain our screening throughput standards.

Additionally, we have been hard at work in raising the global bar of aviation security. This effort is focused on security measures at the 280-plus last point of departure, or LPD, airports around the world. An increase in our international footprint is needed and is requested in this budget.

Finally, to respond to a changing threat, we revised our concept of operations for the federal air marshal service that allows us to make a modest downward adjustment to the size of this very important component of TSA, while enhancing operational effectiveness.

I would also note that we have identified efficiencies in certain aspects of TSA operations that results in approximately \$160 million of program reductions to partially offset the need for growth in other areas.

In closing, I appreciate the opportunity to discuss TSA's resource needs at today's hearing. I hope you and your staffs have found us very responsive to your requests for information. I am committed

to being as open and transparent as possible and am always available to discuss any aspect of TSA's operations with you.

I look forward to responding to your questions this afternoon. Thank you, Madam Chair.

[The prepared statement of Mr. Pekoske follows:]

Statement of

David P. Pekoske

Administrator

Transportation Security Administration

U.S. Department of Homeland Security

before the

U.S. House of Representatives

Committee on Appropriations

Subcommittee on Homeland Security

“Examining the President’s FY 2020 Budget Request for the

Transportation Security Administration”

April 2, 2019

Good afternoon Chairwoman Roybal-Allard, Ranking Member Fleischmann, and distinguished members of the subcommittee. Thank you for inviting me to testify on the President’s Fiscal Year (FY) 2020 Budget, which includes a \$7.79 billion request for the Transportation Security Administration (TSA). This is my first time appearing before this subcommittee since becoming the TSA Administrator in August 2017. I am honored to be here and welcome the opportunity to update you on the progress the agency has made during FY 2018 and thus far this year. My testimony will highlight the accomplishments of our exceptional workforce and explain how we have improved our mission execution.

The U.S. transportation system accommodates approximately 965 million domestic and international aviation passengers annually – this equates to the screening of 2.2 million

passengers, 1.4 million checked bags, and 5.1 million carry-on bags each day. There are also over 5.3 billion passengers traveling on transit and over-the-road buses each year, more than 10.1 billion passenger trips on mass transit per year, and nearly 900,000 chemical shipments on trucks every day. Beyond those usage numbers associated with a relatively open network of transportation modes, the physical scope of the system encompasses approximately 126,000 miles of railroad tracks, 4.2 million miles of highway, 615,000 highway bridges, 473 road tunnels, and nearly 2.5 million miles of pipeline.

Aviation and transportation hubs remain highly-valued targets for terrorists, and terrorist modes and methods of attack are more decentralized and opportunistic than ever before. Every day, TSA is challenged by a persistent, pervasive and constantly evolving threat environment, both in the physical and cyber realms.

We face ambitious adversaries on a daily basis who watch us, study our vulnerabilities, and work diligently to develop new attack strategies to replace those that have failed. To stay ahead of these adversaries, we have to innovate, deploy new solutions rapidly and effectively, and make the most of our resources – goals that are reflected in TSA’s three strategic priorities: Improving Security and Safeguarding the Transportation System; Accelerating Action; and Committing to Our People. In short, we must strive to deliver *Better Security Faster*.

TSA’s workforce has made significant progress implementing those priorities. In FY 2018, we -

- Screened more than 804 million aviation passengers, representing a 5 percent checkpoint volume increase from FY 2017;

- Established and rapidly implemented a Computed Tomography (CT) carry-on baggage screening program through procurement of 49 CT units and deployment of 30 of them to airports and laboratories;
- Expanded the training of explosives detection canine teams in support of maintaining 1,047 TSA Passenger Screening Canine and Law Enforcement Officer teams; and
- Conducted 1,967 air carrier inspections at foreign airports, 145 foreign airport assessments, 62 pipeline critical facility security reviews, 92 assessments of mass transit operator security enhancements, and 124 assessments of security enhancements by motor carriers.

Additionally, TSA's workforce consistently demonstrated extraordinary diligence and commitment to duty throughout FY 2018 and continues to do so today. Of particular note, Transportation Security Officers (TSOs), vetting personnel, Transportation Security Inspectors, canine handlers, and Federal Air Marshals worked for 35 days under extraordinarily challenging circumstances during the lapse in appropriations. Many of those individuals, and in particular our TSOs who are in junior pay bands, continued to report to work despite suffering financial hardships. TSA leveraged the flexibility provided by our appropriations to use prior year funding to mitigate the adverse financial impact on our workforce. Moving forward, I continue to look at various options under the broad scope of TSA's authorities to demonstrate our commitment to the workforce, reward high performers, reduce turnover, and improve employee morale.

Another important element of TSA's ability to deliver *Better Security Faster* relies upon our legal authority to execute our mission. To that end, I want to thank Congress for the passage

and ultimate enactment last October of the *FAA Reauthorization Act of 2018*, which includes the *TSA Modernization Act*.

The *TSA Modernization Act* represents the agency's first reauthorization since its inception in 2001. Among many things, the *TSA Modernization Act* authorizes appropriations for FY 2019, 2020, and 2021, modernizes TSA's structure and operations, and expands the Agency's ability to innovate, engage domestic and international stakeholders, and execute our critical mission to protect passengers and cargo traveling across all modes of transportation. In addition to directing an agency-wide efficiency review, we believe the *TSA Modernization Act* requirement for TSA to formally apply risk-based budgeting to surface transportation and to develop and submit a Capital Investment Plan (CIP) will better position us to strategically plan and apply our resources more effectively. We anticipate the CIP will be submitted next month and the surface transportation security assessment, which is a precursor for associated risk based budget and resource allocation efforts, will be completed by its October 2019 deadline. These documents will be used in the development of future budget requests.

As part of the budget development process, we identified cost-savings and efficiencies in order to pursue top funding priorities in FY 2020. These include reduction to the Federal Air Marshal Service based on our new Concept of Operations; contract and travel costs savings of \$40.2 million; and anticipated staff attrition of 11.5 percent resulting from the consolidation of TSA buildings into our new headquarters. In total, TSA reductions include 166 positions from headquarters and \$181.5 million in expenditures that will be redirected to other higher priority items, including support of the frontline workforce.

Fully funding TSA's FY 2020 Budget Request will enable the agency to build upon the progress we have made to improve frontline operations, accelerate the deployment of new

technologies, and gain efficiencies through organizational restructuring and optimizing the use of limited resources. For instance, this Budget Request continues ongoing capital investment efforts to purchase and deploy new technologies.

In FY 2020, TSA will buy 320 CT units using requested resource funding and prior year resources available in the Aviation Security Capital Fund. Building upon the FY 2018 efforts noted earlier, and the anticipated procurement of approximately 202 additional CT units in FY 2019, funding the FY 2020 request will enable us to continue to accelerate the deployment of CT technology to the field to equip our workforce and more effectively enable mission execution. CT systems provide TSOs with a 3-dimensional view of baggage, the ability to remove unwanted clutter, and a greater capacity to detect explosives and prohibited items. We are also requesting a \$12.6 million increase to further develop CT detection technology to identify a broader range of homemade explosives, reduce false alarms, enable detection of greatly reduced threat mass, and potentially provide the ability for passengers to leave liquids and laptops in their carry-on bags.

In addition, TSA will continue purchasing 294 Credentialing Authentication Technology (CAT) units using \$14.8 million from base resources. The ongoing purchases of CAT units will improve the detection of fraudulent documents and allow us to screen passengers more effectively on a risk basis.

This Budget also requests an additional \$58.6 million, including associated costs, for additional TSOs (1028 positions/700 FTE) to bolster our screening workforce. As passenger enplanements increase, so does TSA's operational workload. We constantly explore ways to improve screening efficiencies while maintaining or improving security effectiveness and consider various factors including space constraints, passenger/baggage screening demand,

equipment, and risks at airports to right size the workforce. For FY 2020, this investment in TSO staffing is necessary for us to continue to meet passenger expectations, maintain acceptable wait times, and avoid crowding at the checkpoints, which is itself a security concern. The FY 2020 Budget Request also includes \$8.8 million to implement improved training requirements for the agency's TSO Career Progression Plan. We expect this investment in the professional growth of our workforce to enhance screener proficiency, performance, and morale.

Recognizing that aviation transportation security requires global cooperation, the Budget requests \$10.2 million for increased international outreach. This reflects TSA's commitment to raising the global transportation security baseline by increasing our international footprint in Asia, the Middle East, and at CBP preclearance locations. This approach is designed to deter, detect, and deny potential adversaries access or the ability to insert a threat into the global transportation system.

Finally, in conjunction with the FY 2020 Budget Request, the Administration proposes raising the Aviation Passenger Security Fee, also known as the September 11th Security Fee, in order to fully cover the costs of aviation security by FY 2028. The fee was created to cover the costs of aviation security, but currently it covers only 40 percent. This proposal would increase the fee by one dollar, from \$5.60 to \$6.60 per one-way trip, in FY 2020 and then from \$6.60 to \$8.25 in FY 2021. This measure would generate \$599 million in new revenue in FY 2020 and close to \$23 billion over the next ten years.

Last year, I announced a one-word revision to TSA's motto - changing "*Not on My Watch*" to "*Not on Our Watch*." This simple but significant adjustment reflects the fact that securing our transportation systems is a communal effort and that our greatest assets are – and will always be – our people, our partners, and the traveling public.

TSA's FY 2020 Budget Request is consistent with that approach. To achieve the priorities reflected within it, TSA will engage industry and our stakeholders to partner with us to develop and deploy new technology. We will also invest resources in our employees, who reflect TSA's core values of integrity, respect, and commitment, and ask them to serve as leaders regardless of their titles or level in the agency, and as ambassadors for TSA. We will continue to encourage the public to be part of the solution. Finally, through constructive oversight and dialogue, we seek to partner with Congress as we work to provide *Better Security Faster*.

Chairwoman Roybal-Allard, Ranking Member Fleischmann, and members of the subcommittee, thank you for the opportunity to appear before you today. I look forward to your questions.

Ms. ROYBAL-ALLARD. Thank you, Administrator, as I mentioned during my opening statement, TSOs and other TSA personnel diligently worked without pay during the recent partial government shutdown. Can you tell us how TSA managed this and kept its workforce on the job and whether the shutdown has had an impact on recruitment or retention?

Mr. PEKOSKE. Yes, ma'am. The way we managed it is multifold. First and foremost, one of the things that I saw when I first came into this position over a year-and-a-half ago, as I traveled around the airports around the country, was the deep commitment of the men and women of TSA to the mission. This is a mission that compels performance on the part of men and women in this agency.

As I said in my opening statement, I saw that commitment up close and personal during the 35-day lapse in appropriation. I think that was a significant driver for people to continue when it was very hard to report for work and do a very difficult job, but they all recognize how critical it is to the safety and security of passengers going through our systems.

Additionally, thanks to the authority that you provided in law, we have a 2-year appropriation for our operations accounts. And so that allowed me to use unobligated fiscal 2018 funds, and we were able to do a number of novel things as a result. We were able to, for example, provide bonuses to our frontline screening workforce, with the idea to get as much cash into their checking accounts as we possibly could. And so that was one aspect that we were able to exercise because of the unique authorities that TSA has.

Additionally, we were hugely rewarded, I think, by our airline and airport partners for the dedication of that workforce. Across the entire system, we had expressions of generosity and donations of food and other support to our frontline workforce that really was very meaningful to them.

Additionally, passengers as they were going through the screening checkpoints, recognized the fact that the screeners that they encountered, if they are a regular traveler on a very routine basis, were now working, going on at the very end of the shutdown for almost 5 weeks without receiving pay. And just the expressions of appreciation, gratitude, and the fact that passengers expressed that they valued the work that the TSA workforce was performing meant an awful lot to the workforce.

Finally, I would say that from my perspective my focus is always going to be on the frontline of the organization. And I have asked all of the leaders within TSA to similarly focus on the frontline, to walk around, have a conversation, understand what challenges our employees might be dealing with, and do whatever they can to remedy them. And so we have essentially used the authorities the Congress has provided to the fullest extent of the law, and I think that has paid us big dividends.

And the shutdown impact, with respect to attrition, has been so far actually less attrition, but I am fully mindful of the fact that, you know, individuals sometimes make a decision to stay or leave employment with an employer, but don't exercise that action for several months afterwards. And so we are going to keep a very close eye on our attrition rates. But so far, immediately after the shutdown, they are lower than what we have had in the past.

Ms. ROYBAL-ALLARD. Okay. And what lessons did you learn during this period that would be relevant in the future if we have another shutdown or some similar type of situation?

Mr. PEKOSKE. A couple of key lessons. One is, first and foremost, to continue to have that appropriations flexibility, so that we can look at 2 years' worth of appropriations versus just one. The second is to take a look at potentially—and I know there are a number of bills up here on the hill—to look at potentially making the aviation passenger security fee available to TSA either on a regular basis or during a lapse in appropriations. And that would give us a funding base to be able to pay the men and women within the agency.

The other thing that is really important to emphasize here is that the screening workforce comprises the vast majority of TSA, roughly 50,000 of 63,000 employees. But there are an awful lot of employees that were also similarly working that weren't visible to passengers. And they were also impacted by the shutdown. This includes all of our personnel that do vetting operations, that basically look at passenger information before passengers board flights to be able to assess risk by passenger.

All of our Federal air marshals that provide in-flight security. All of our inspectors at airports around the country that ensure airports and airlines are complying with the regulations we have put in place. And then finally, all of our international staff that—we have a number of measures in place at those last point of departure airports that I mentioned, that has been a significant work driver. Two hundred and eighty airports and we have four series of different requirements at those airports.

And so the entire organization really pulled together. But I think it really—at the end of the day—boils down to continued, sustained leadership involvement and leadership action with respect to our employees and then the leaders having the flexibility to be able to ensure that the frontlines are able to deliver the services that are so important to the public.

Ms. ROYBAL-ALLARD. Thank you. Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you, Madam Chairman. Mr. Administrator, hello again. Mr. Administrator, I have a question. I am concerned about the threat posed by the largely unmonitored movement of high-ranking hazardous materials on our nation's highway network and about TSA's difficulty to address this vulnerability as directed by Congress and as required by law.

Section 1554 of the 9/11 Act of 2007, Motor Carrier Security Sensitive Material Tracking, requires the TSA, sir, to develop a program to facilitate the tracking of highway security sensitive materials, HSSMs. Currently, I understand that the TSA has no visibility in the movement of these dangerous materials on the nation's highways.

Compounding this, I understand that TSA lacks the basic programmatic data on the shipments, the number of shipments, quantities shipped, and the original destination and routing of the shipments. Mr. Administrator, I was pleased with the commitment you actually made, sir, during your confirmation hearing to revisit the surface security provisions of the 9/11 Act and to implement those that TSA has yet to address. However, TSA has not prioritized this

R&D program and worked stopped about a year-and-a-half ago with the Fedtrak R&D project about half completed.

I understand that there has been some preliminary discussion around an approach to implement a tracking center in an industry-funded public-private partnership at no cost to the taxpayer. My question, can you tell me what, if any, plans TSA has to restart and complete the work on Fedtrak R&D?

Mr. PEKOSKE. Yes, sir. Thank you for your question. And also thank you for your comments about the Chattanooga workforce.

And I did talk to the federal security director for that airport and personal relay the comments that you made, and he was very appreciative of your comments and your involvement and your support of TSA.

With respect to your question, I said at my confirmation hearing that I am very concerned about the level of effort that TSA is able to put forth with surface transportation security writ large, whether it is trucking, freight rail, mass transit, pipelines, over the road buses.

And one of the things that we have done to address that is we are in the midst of a restructuring which will put under the direct control of an assistant administrator for surface transportation security operations, so we elevated the position up a notch that oversees surface. And then we are also in the process of giving that assistant administrator direct control over a lot more resources than she previously had direct control over. And this includes all of our surface inspectors that are basically collocated with our inspectors at airports around the country and also a regional staff to be able to work closely with FEMA for contingency planning and response and also for surface transportation security.

Additionally, I know from looking at my own budget that we are underinvested in research and development. And that is something that is not reflected in the fiscal 2020 budget, because we are not ready yet to put specific initiatives forward to do that, but we will be in our fiscal 2021 budget. And this applies both at the screening checkpoint and also at our surface transportation efforts.

And so I pledge to you that I will keep a very close eye on this, and you will see as we complete our restructuring a significant increase in the resources directly attributable to the surface training security.

Mr. FLEISCHMANN. Yes, sir, thank you. And as a follow-up, can you speak to the potential return to the taxpayer in terms of preventing a serious incident, sir?

Mr. PEKOSKE. Yes, sir, and that is something we are always very mindful of is the—you know, the ROI is enormous on almost every aspect of what TSA performs. And we do have, in my view, a very robust risk assessment and risk management process that kind of looks across the spectrum of what we are asked to secure and makes decisions as to where we need to spend that next available dollar so we do get the highest return on investment for the taxpayer.

But that is the constant part of our process. And I just recently amended the risk assessment and management process to the point where annually it is briefed to me and my senior staff as to what risks we think we are facing and how we are going to manage and

mitigate those risks, and then quarterly updates after that, so it is constantly on our plate as we look at our own resource allocations, our own policy decisions, that we keep that in clear focus.

Mr. FLEISCHMANN. Mr. Administrator, thank you. I believe my time is up. Madam Chairman, I will reserve for round two.

Ms. ROYBAL-ALLARD. Mr. Ruppertsberger.

Mr. RUPPERSBERGER. Sure. First, thanks for being here.

When TSA first started, there were a lot of problems. I think that there wasn't really adequate training, and I think also there needed to be a theme with the people who worked really on the frontline that they were in the service business, they were representing homeland security, and that there is a way to deal with your job and working with people, and that has changed. I think TSA, whether under your leadership or before, but I see that you have better training. I think the people—I fly out of BWI airport a lot in Baltimore, but the people are really friendly, they do the job the best they can, and they are professional. And that is what you want, because they are still representing the government.

So whatever you are doing there, keep it up. And I want to acknowledge the employees of—and again, I am sorry that unfortunately for different reasons—I am not going to get into any politics here—but that you couldn't be paid while you were working. And that can't—should not happen again.

I want to get into the issue of—I think you have expedited the recurring process for fielding computed tomography, CT technology, known as a gold standard in the aviation security. You know, I was a former ranking member of the Intelligence Committee and done a lot with terrorism, and to this day, I still think that one of the key areas for terrorists is the airplane. And so you have that burden with you, and you have got to keep up that on a regular basis. And I hope you are communicating with intelligence agencies and other groups, too.

I am also pleased that you have just bought over 300 technology screening with Smiths Detection. Why I am pleased about that, they are in my district. So I want to make sure that it was a competitive bid and all that, okay, just to cover. But they—tell us why you picked them and why their technology is so good.

Mr. PEKOSKE. Yes, sir. Well, CT—

Mr. RUPPERSBERGER. And I have one other question, so try to make it quick.

Mr. PEKOSKE. Yes, sir. CT is a game-changer for us and the screening checkpoints. It provides an image that is much clearer for the operators to see and you can move that image around 360 degrees, so you can see bag and look at it in the opposite direction, see underneath. That is why laptops don't need to come out of carryon bags.

Mr. RUPPERSBERGER. That is good.

Mr. PEKOSKE. It is huge. And not only that, but the ability to detect explosive levels that we are concerned about is night and day compared to the current technology that is out there. So the current contract award, very pleased with the way that process went. We did it within a year, which is unheard of in federal procurement. We were able to do that because we had a great staff to be able to execute on it. We had great support from the Department

of Homeland Security. And also our private-sector vendors and our private-sector partners, airlines and airports, were all in on this, very, very competitive process. And you saw the results.

Mr. RUPPERSBERGER. Yeah, I have my next—whole back and neck—I have two artificial shoulders, two new knees, and five screws in each foot. That is an orthopedic surgeon's dream. But, you know, I always got nailed every time. And with that new—when you put up, it seems that you passed through that without all of the checking and that type of thing.

Mr. PEKOSKE. Yes, sir—

Mr. RUPPERSBERGER. I would give that as an example. You don't need to talk about that, my body—

[Laughter.]

Mr. PEKOSKE. Well, we have a solution we are looking at for that, too.

Mr. RUPPERSBERGER. Good, well, that is great. The other thing I want to get into is—and this is a little bit more controversial—local airports employ able and component security guards, but the level of training at TSA is so superior to—second-to-none right now in this agency. And I believe your agency should be staffing exit lanes. That is a controversial issue, because the president's budget cut that, and they did the same last year.

And the—last year, I think Congress was able to put in \$77 million back in the budget. And again, we are dealing with it again. And, you know, hopefully our colleagues come together and push for full funding. And this is not a cost that the regional airports can really afford and a lot of the other things that they have to deal with.

Customs and Border Protection is using the same mechanism to our seaports. I represent the Port of Baltimore, too, to pass the buck to local governments. And there are certain responsibilities we have and so we are going to attempt to do what we can to protect our country, but my opinion, now, I don't want to put you in a bad situation, especially with the boss you have. You never know where he is going to be sometimes, and so you don't have to comment on this.

I just want to say that we really feel that this should be your responsibility. We have got money in the budget last year, and we are going to try to do it again this year. I am saving you, son. I don't want you to have to comment on this.

Yield back.

Ms. ROYBAL-ALLARD. Mr. Newhouse.

Mr. NEWHOUSE. Welcome, Administrator Pecoske. I am sure I am going to say that wrong. Well, thank you for being here. You have a unique position, I guess, at least at TSA of being kind of the face of the federal government to a lot of people in this country. And it is an opportunity, and I just want to compliment your staff being as professional and efficient as they are when I go through airports, and also for providing that positive face of the federal government to the general public. So thank you for the hard work that you have in front of you, but also for the professional way you carry it about.

So I wanted to follow up a little bit on the chair's question, even though I wasn't in the room. I understand the question of retention

was part of what you were thinking. One of the concerns are that some airports continue to face the difficulty of retaining TSOs, particularly on a dynamic hot economy, competing.

In the Seattle region, in particular, of course, whenever I fly in and out of twice a week, I know you have been able to do temporary bonuses and some retention incentives for tight labor markets like that. But I am curious how this budget proposal will allow you to tackle some maybe larger reforms of less temporary things to change how you might address this issue, perhaps increased compensation could really lead to better retention of TSOs.

So in light of that, can you tell me what maybe some of the long-term goals are at the TSA to recruit and retain, and also certainly how we can help implement and expedite that plan?

Mr. PEKOSKE. Yes, sir. Thank you very much for your comments. And Seattle Tacoma Airport is a very, very busy airport, and we place a lot of emphasis on making sure we have the proper staff there, because of the volumes that are going through that airport, and also the proper number of canine teams to help us with security.

There are several things, though, that we are doing with respect to the workforce. I think you are right that our attrition rates are too high. And Chairwoman Roybal-Allard had the same observation. And that is due to a number of factors, including the pay levels and including some of the things that we do within TSA that are totally within our control to be able to adjust.

When TSA was formed in 2001, the law that is the baseline for TSA was signed by President Bush on November 19, 2001, so a very short period of time from 9/11 until the establishment of the agency. That Aviation and Transportation Security Act provided an awful lot of authorities to the TSA administrator to be able to manage the screening workforce. And what I am looking to do is to be able to exercise the full extent of those authorities to be able to improve job satisfaction within the workforce, to be able to look at overall pay and compensation issues, so that we begin to address them in a systematic way.

To get at that, we have already put out a TSO, transportation security officer, career progression plan. Because when I came into the agency, there was really no career mapped out for somebody who came in and wanted to be a member of the screening workforce. And so we mapped that out. We published it. We came to this subcommittee and asked for some reprogrammings to be able to execute it.

Mr. NEWHOUSE. So illustrating where a person could be in 5 or 10 or 15 years?

Mr. PEKOSKE. Yes, sir. As a member of the screening workforce and also what training we would provide them, what pay raises would come along with that, and also within TSA—you know, I mentioned in my opening statement all of the different aspects of performance in TSA, you know, vetting, federal air marshals, international inspectors. We are doing a much better job now of laying out those opportunities to the workforce so that they know that, hey, if I aspire to be an inspector, for example, that I do have a career path that allows me to do that.

The other thing that we are doing that is very significant is, I have convened a blue ribbon panel to look at our delivery of human capital services within the agency. That panel is due to report back out to me within the next 30 to 60 days. And I asked them just to take an independent look at how we manage our human capital and come back with some recommendations. That will be the basis for how we proceed with respect to resource issues going forward, but I will give you a very good example of that.

I have all the authority in the world under law to provide longevity increases for my employees. By and large, we don't do that, however, because we were constrained by categorizations of funding in the budget. But I can provide longevity increases every 52 weeks, which is much better than the general schedule can. It is every 2 or 3 years.

And so I want to step back and take a look at, hey, what makes sense for longevity? Where do we reach the point where people we know are making decisions as to whether they stay or they go? And ensure that we recognize experience at those key critical points. And I would be happy to come back to this subcommittee once I have that blue ribbon panel report and just lay out for you what they said, independent group of folks not employed by TSA who are experts in human capital management.

Final thing is that my focus is on leadership and on properly taking care of the entire workforce. And that is where I ask all my leaders to focus their time, as well, so that we are keenly aware of what the needs of the workforce are.

Mr. NEWHOUSE. Good, good. Well, I would be certainly interested in seeing that if it comes available, and also looking for ways that we can work with you as you meet the growing needs of travelers in the country and the growth at airports that we are seeing, as well. So thank you very much for your questions. I yield back, Madam Chairman.

Ms. ROYBAL-ALLARD. Mr. Price.

Mr. PRICE. Thank you, Madam Chairman. Welcome, Administrator. We are happy to have you, and appreciate your testimony.

Let me turn to the area of general aviation and ask about your work in that area, and in cooperation with general aviation stakeholders. The recently enacted FAA reauthorization act included provisions which encouraged more focus on TSA's efforts with general aviation airports and operators, and specifically encourages a dedicated general aviation representative. And part of the rationale for such a dedicated staff person is the desire to support general aviation's efforts to encourage and improve secure operations.

This includes efforts to modernize existing security programs, particularly in specialized areas, like the DCA access standard security program and gateway airports, which are used to provide access during temporary flight restrictions for special events and so on. A number of these efforts underway.

I think it is fair to say that the progress in most of them has been limited so far. So that leads to my question. What steps are being taken by TSA to encourage modernization and use of these programs in a responsive and timely manner for stakeholders? How are you prioritizing programs such as DASSP, gateway, and other

security programs used by general aviation aircraft to increase operational flexibility?

Mr. PEKOSKE. Yes, sir. We spend a lot of time making sure that any interest group having to do with aviation security or surface transportation security has a clear entry point into the TSA organization and somebody that can champion their issues so that would be an expert and be able to reflect on a short notice question generally what that segment of the industry would desire.

Additionally, we have the Aviation Security Advisory Committee that is a group of volunteers who has provided invaluable advice to me as the administrator. And I use them extensively. And I know general aviation interests are well represented there.

I have met with individuals from the general aviation industry over the course of my time as the administrator. I am very familiar with the concerns that they have. We did, in fact, look very specifically at the DC special access area and the regulations attendant there, too, and determined that what we had in place made sense given the threat that we still see. But we said that we would be willing to look at ways that we could provide an equivalent level of security by potentially doing something a little bit differently.

And that is generally an approach that we have taken with industry, is to say, hey, here is the security outcome that we need to achieve. This is our mission. This is the outcomes that we need to achieve. And then how would you propose that we achieve those outcomes? Because I want to hear from the industry as to what specific ways and measures—these are folks that are all running businesses—that they have a certain perspective that I think is incredibly valuable to our decision process. And that is the process we use is, hey, here is the threat, here is the outcome, tell us how you would achieve that outcome. And then we work together to then determine what specific measures we put in place.

Mr. PRICE. And can you give us some estimation of the state of play with respect to these efforts? How successful have they been? How far along are they? What would be maybe an example of the progress you hope to make?

Mr. PEKOSKE. Yes, sir, I will give you an example with commercial non-general aviation. I think that is the best example. We were facing a threat that had to do with powders being introduced into a cabin of an aircraft. We were able to bring representatives of the major carriers into TSA headquarters, all had security clearances. We revealed with them at a certain level what that threat entailed and told them what security outcome we wanted to achieve.

We went back and forth in this process for about 2 months and then came up with a series of measures that the true success of it is that we significantly raised security at our domestic airports and our international last point of departure airports, and most passengers never even noticed that something had happened. And the nuanced change was that we asked passengers to take large volumes of powders out of their carryon bag.

And then we put certain protocols in place. We had to decide what volume and then how we were going to resolve what those powders were. But that was a very successful process that actually has been adopted by other countries as a result.

So my point is, as open as we can be, a lot of collaboration, and then a clear explanation as to why we go down a certain path.

Mr. PRICE. Thank you. Thank you, Madam Chairman.

Ms. ROYBAL-ALLARD. Ms. Meng.

Ms. MENG. Thank you, Madam Chairwoman, and thank you, Mr. Administrator, for being here today. I want to, as a frequent flier through LaGuardia Airport in Queens, New York, very grateful to you and the TSA agents who work there who I see at least twice a week. So thank you for your commitment.

I wanted to ask about reports from the House Committee on Oversight from the fall 2018, revelations about the hostile work environment, history of sexual harassment and retaliation. Wanted to know if—what has been done to address this issue from an institutional perspective? Has anyone been terminated? Have there been new trainings? And how can we ensure that employees are able to report malfeasance without any sort of retribution?

Mr. PEKOSKE. Yes, thank you for the question. And I have been very, very strong on this issue. I think that job satisfaction, workplace environment are things we control largely. And we need to make sure, one, we comply with the law and, secondly, that we create an environment where every person who is an employee of TSA can succeed.

And so what we have done—specifically to respond to your question—is, yes, we have provided a lot more training. But I think what is important is what the leadership emphasis is. And I published in a couple of documents—first one was the new strategy for TSA that I published about a year ago. And one of the core values that we put into the TSA strategy was respect, because that was not a core value of the agency.

And to me, that means respect for each other in the workplace and also respect for passengers as they receive the services that we provide. First core value is integrity, second, respect, the third is commitment.

The other thing that we did was when we published the administrator's intent, which is a document that basically says, hey, while I am the administrator of this agency, here is what I am going to do to execute on that strategy. In the administrator's intent, I put a whole series of leadership principles. The very first leadership principle is caring for your people, because I want to create a leadership culture that gets at these longstanding inside TSA job satisfaction, work environment issues.

I am happy to report a couple things. One is that our FEV scores, the federal employee viewpoint survey, that survey that is done every year of every single federal agency, shows noticeable progress across all dimensions. We didn't go down or stay the same in any dimension. We went up in every single one.

Additionally, if you look at the complaints that we receive, those complaint rates are way down from this year over last. And so I just look at those trends to say, hey, are we on the right track here? And what else do we need to do?

Finally, I have asked every leader to be open and accessible to the people that they work with. And the only way you are going to do that, if you are a federal security director at LaGuardia airport, the only way you are going to have a feeling for how well your

people feel about the job that they perform and the people that they work with is to walk around and to talk to them. You can get them one on one and just ask them questions, give them the opportunity to get to know you and you them.

And then you will get some direct feedback. And as I travel around, I get a lot of direct feedback. And I can tell almost instantly how an airport operates, you know, after about 3 or 4 minutes on the ground, just in a couple of interactions with people.

Ms. MENG. Great. But had—from the revelations from that hearing, had anyone been terminated or what were the results?

Mr. PEKOSKE. From the hearing, the incidents that were referenced in that hearing go back several years. And what I said at the hearing was, I am not going to go back and readjudicate things that happened several years ago, because as long as I am told that the process was not fundamentally flawed and decision-makers made decisions with the facts that were available to them, that I wasn't going to go reverse those actions.

But that we would take very quick action on any future incidents that have occurred, and that is what we have done. And so, you know, I—in many cases, the actions that were the subject of that hearing had already been taken and involved agreements between the employees affected and the agency. So I really couldn't undo those from my perspective.

Ms. MENG. Okay. So, I have a second quick question about religious and racial profiling. Since 2012, over 700 complaints have been filed against the TSA using the FlyRights app, addressing mistreatment and discrimination. In contradiction to TSA protocol, Sikh Americans have been required to remove their turbans, Muslim Americans have been interrogated about which mosques they attend, for example.

To ensure that this type of profiling does not occur at airports across the country, what types of accountability systems are currently in place?

Mr. PEKOSKE. A number of things. First, we screen on average 2.4, 2.5 million passengers a day. And that number 700 goes back to 2012. So if you look at the volume of passengers to put that number 700 in context, but there are still 700 people who had a complaint. I am very mindful of that.

And we have a process that we have that allows people to register a complaint and then us to get back to the individuals, do whatever investigation is deemed necessary at that point in time, and try to resolve these as expeditiously as we can.

Additionally, I have made it a point as I am traveling around the country to visit different groups around the country, just to be able to establish that connection from the top leadership of TSA with different communities in this nation. So we are trying to make sure that we have a very good dialogue.

And, you know, we have a multicultural day every year in TSA. It is widely attended. And the attendance is growing year after year. So I think our levels of communication are very good.

Final point I would make is that when we see a passenger who has a complaint, first thing we do is we, one, ensure that our officers were following our standard operating procedures. And I will

tell you that in almost every case that is the case. So then we back up our officers. Our officers were following our procedures.

But then the second question is, are our procedures still the appropriate procedures? Because every case we use to kind of re-review our procedures to make sure they are appropriate, given the security concerns that we have.

Ms. MENG. Okay, thank you. I yield back.

Ms. ROYBAL-ALLARD. Mr. Aguilar.

Mr. AGUILAR. Thank you, Chairwoman. Thanks, Administrator, for being here. And I know I missed your answer to questions related to the shutdown and working without pay. But your folks do an amazing job each and every day.

But I did want to ask, specific to those issues and morale, how is morale among TSA employees? And if you could benchmark that against things from years past. You know, where are we at today?

Mr. PEKOSKE. I think the best indicator of morale is that federal employee viewpoint survey, because it is every year. It is the same questions. And last year, for example, that was what is called a census year, which means that every single employee was issued an e-mail invitation to participate in the survey.

Our performance on that FEV survey is constantly improving. We went up in every single category across the board. And I think our average increase was 3 percentage points, which is pretty good, given the size of the agency.

Mr. AGUILAR. What is the response rate? How many people? What is the percentage?

Mr. PEKOSKE. I will have to get back to you on the record with that, but I want to say it is something around 19 percent or so, which is actually not a bad response rate. But one of the things that we are going to do this year, is because most of our employees are doing shift work at a screening checkpoint and they only have a limited number of computers to access, is to continue to make a push—because I want to see as high a level of participation as we can, because that will give me more confidence in the results.

[Mr. Pekoske responded for the record:]

In 2018, 22,888 TSA employees completed the Federal Employee Viewpoint Survey (FEVS). This represents 38.9 percent of the eligible workforce at the time of the survey, as determined by OPM. Although TSA hopes to improve on this number in the 2019 survey, it is comparable to other government benchmarks. For example, the 2018 government wide response rate was 40.6 percent, and the response rate for DHS was 41.3 percent. In Headquarters, TSA had a response rate of 57.2 percent, well above the government average. And while response rates are much lower in the airports (37.5 percent). TSA is encouraged that many airports do participate in FEVS at high levels. For example, Detroit Metropolitan-Wayne County Airport (DTW), a Category X airport, had 61 percent participation. TSA's largest workforce, Los Angeles International Airport (LAX), had 52 percent participation. These participation rates are due to local leadership, support, and planning.

The timing of the survey, which is administered by OPM, occurs in the midst of the busy summer travel season. The vast majority of the TSA workforce serves on the frontlines and has limited access to computers during shifts. However, TSA is committed to encouraging every employee to participate in the survey. TSA believes that employee participation in the FEVS is driven by two factors: ease of access to the survey and a belief that TSA takes action on survey results.

Regarding ease of access, TSA encourages local leaders to break down barriers to taking the survey. For example, many airports set aside time when employees are scheduled to attend training, and have access to computers, for FEVS participation. This year TSA will also be piloting tablets at Los Angeles International Airport

(LAX) checkpoints to determine whether improved mobile access will boost response rates.

To help employees understand why FEVS Matters, TSA is directly engaging employees across all internal communications platforms to improve employee understanding of how survey results are used. TSA solicited local success stories, describing how the 2018 results were used at the local level to drive improvements, and stories are being shared with the larger agency each week, leading up to and during the 2019 FEVS administration period. Each success story is shared via the National Shift Brief, iShare homepage, TSO Advisor blog, and multiple TSAnews app channels. TSA is also highlighting how leadership values employee input in making TSA a great place to work by highlighting the leadership team's ongoing efforts to include every level of employee in the agency's decision making process.

As OPM is again deploying the survey as a full census, TSA intends to make the most of this opportunity to hear from the full TSA workforce.

Mr. AGUILAR. Appreciate it. News reports have mentioned that a team of TSA agents made a trip to Saudi Arabia with the goal of helping Saudi Arabia with aviation security and technical assistance. Can you expand on that, that government-to-government relationship? And how long is it scheduled to continue?

Mr. PEKOSKE. That government-to-government relationship actually started out with a technical cooperation agreement back in 2008. And really the process from 2008 to today has been a series of visits to really understand what the Saudi government was seeking in terms of our expertise and where we could best help them out.

And so there have been a series of visits back-and-forth over the intervening years. We signed an MOU—we being the Department of State and TSA—in September of 2017 as to how we were going to operationalize the requests that the Saudi government had made. But to date, where we sit right now is we are still going back and forth on scheduling and figuring out exactly what we are going to provide, but we haven't actually provided any training at this point.

Mr. AGUILAR. Does the MOU talk about timeframe?

Mr. PEKOSKE. The MOU goes out, I think, until 2023, if my memory serves me correctly.

Mr. AGUILAR. Okay. I appreciate it. Thank you. I yield back, Madam Chair.

Ms. ROYBAL-ALLARD. Ms. Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. Thank you, Madam Chair. I want to follow quickly on the heels of my colleague from California with a question, or really a statement, about our TSOs.

These are folks who are abused and ridiculed for just doing their jobs. Abuse and ridicule is not in their job description, but one would think it was, given how I have witnessed—and I know so many of us have witnessed them being treated. And then on top of that, they went through a government shutdown and did those same jobs without pay.

So have we now fully paid all of the TSOs that did not receive pay during the shutdown?

Mr. PEKOSKE. Yes, ma'am. And in any large organization, you are always going to have a very small percentage of people unrelated to the shutdown or just—that have pay issues that we work very quickly to resolve. But a lot of the pay issues that we had immediately following the resumption of full operations and appropriation were mostly related to system issues with the pay system

itself. It wasn't the actions that we were taking; it was actually executing through the pay system.

Ms. WASSERMAN SCHULTZ. Okay, thank you. I know you are aware on January 6, 2017, a man walked into the baggage claim area of Fort Lauderdale-Hollywood International Airport, collected his luggage, removed a firearm from that bag, opened fire on his fellow passengers, and murdered five people and injured six others.

The aftermath of that shooting rampage was nothing short of chaos, mostly due to a lack of coordination. The takedown of the suspect was immediate. Since that date, I know I have been working closely with TSA and with our airports and our airlines to ensure that we have a more effective model for ensuring coordination between federal, state and local law enforcement at airports so that the response to similar incidents, because we had one at LAX, we had one at JFK, can be swift and coordinated.

And so after researching and talking with many airport professionals, I am convinced that this can most effectively be accomplished by establishing unified operations centers in airports, which I had the good fortune to talk to you about in my office the other day, that would serve as a centralized hub for coordination during a security incident, like what we had at our airport.

So can you share with us whether you agree that a unified command-and-control center at airports, particularly the Cat X airports, would improve the response to security incidents?

Mr. PEKOSKE. I completely agree that having a unified operations center at any large airport—actually, any airport—is very beneficial to the day-to-day operation of the airport and certainly to the operation of an airport when there is an emergency like what happened at Fort Lauderdale airport, unfortunately.

And I also believe that the best model is to have them up on a day-to-day basis and not start them when you have an emergency, because that loss of time and just the coordination that needs to occur, precious seconds are lost and that really counts, as we saw in Fort Lauderdale.

There are provisions in the TSA Modernization Act that have us set some guidelines for airport operation centers, and we are on pace to do that, because I want to see that in writing and publish that as an agency. And then we have scheduled in the Mod Act a brief to members on this very topic. So I am looking forward to both those opportunities.

Ms. WASSERMAN SCHULTZ. Great. And I look forward to working with you as we discussed on my legislation so that we can further actualize that concept. And lastly, I wanted to just touch on the advanced imaging technology that since 2015 has been approved and utilized by our international partners at some of the world's busiest airports.

The newer, next-generation AIT technology used in Europe and internationally has been at the Transportation Security Lab since 2014. Data from TSL assessments clearly indicate that this new technology performs better than TSA's current technology. It is less intrusive. It makes it a little bit less—quite a bit less confrontational for our TSOs where there is an alarm.

Can the TSA leverage the performance data of our international partners to reduce the time and TSA resources needed to accelerate

the validation of the new AIT technology and make it available more quickly for airports to equip new terminals?

Mr. PEKOSKE. Yes, ma'am, absolutely. In fact, we have already certified that technology, which means that we have tested it in our labs and we have said it meets the performance specifications that are required for use in our screening checkpoints. So we are already doing that.

And to your larger point, we worked very, very closely with all of our international partners on their technology advancements so that we don't repeat each other's good work and that we benefit from the lessons that each other learns.

Ms. WASSERMAN SCHULTZ. Thank you. Thank you, Madam Chair. I yield back.

Ms. ROYBAL-ALLARD. Mr. Administrator, the administration's budget request for transportation security officer staffing would accommodate a passenger growth rate of 2.5 percent. But it estimates that the actual passenger growth rate is expected to be 4.5 percent. Why is there a mismatch? And wouldn't that result in an expansion of wait times at checkpoints?

Mr. PEKOSKE. Yes, ma'am, you are correct. The resources we are requesting will basically accommodate a 2.5 percent increase. We know it is 4.5 percent or 5 percent. But we also know that in certain airports around the country, we really can't add any more people, because we are maxed out in terms of the number of screening lanes that we have. And so that is a factor, is the fact that in some airports you just can't add any more lanes, even if you knew you needed to. And we essentially wait with the airports with infrastructure improvement projects to give us that additional capacity.

Also, we were looking for ways to become ever more efficient in the screening operations that we conduct. And I will give you two really good examples. For the CT, the CAT scan X-ray technology that we are looking at, that will eventually make us much better to be able to specifically isolate in a carryon bag, if the bag alarms through the X-ray, what specifically we need to look at. And that should speed the process along.

Congresswoman Wasserman Schultz mentioned the AIT technology, and she is right. With the current technology, our false alarm rate is higher than what we would all like it to be. The new technology that we are looking at brings that false alarm rate down. And so what that means is that we have—when we need to do a pat-down of a passenger, it is more likely than not that there is an anomaly, something on that person's body that alarmed the machine.

And so the technology advancements should improve our efficiency overall. But we are just in a position that with the top-line resources that the department has and the TSA has, we really can't get up to the full 4.5 percent. I don't think we really need to. And settling it at 2.5 percent is I think a very reasonable place to be at this point in time.

Ms. ROYBAL-ALLARD. The budget request recommends the elimination of three programs that Congress has repeatedly endorsed—the visible intermodal prevention and response teams, the LEO reimbursement program, and TSA staffing of exit lanes at certain airports. Are the elimination of these programs based on assess-

ments that they are poor investments of tax dollars? Or are there other reasons that you can talk about?

Mr. PEKOSKE. Yes, ma'am. All three programs are very valuable programs. And they are appropriate investments. The VIPR teams are appropriate investments. They provide security in surface transportation and airport centers. The law enforcement reimbursement reimburses our law enforcement partners who provide a presence at our screening checkpoints. And I think both of those are very valuable programs.

It really is an issue of when you look at, you know, a top-line budget number, not just for TSA, but for the entire department, what kinds of tradeoffs do we have to make to stay within that top-line budget number? And there are some difficult choices that are made in any process like that.

But what I would say, without question, that those are important programs. We are just fiscally not able to support them in this budget.

Ms. ROYBAL-ALLARD. Okay. Now, if we were able to find additional resources, what would you recommend in terms of these three programs? I mean, that we could fund all three or if we have budget constraints, could you tell us the order in which you would prioritize these?

Mr. PEKOSKE. Yes, ma'am. I would prioritize them VIPR first, because the VIPR program also provides ground-based assignments for federal air marshals. It gives them a chance to rotate from being in an aircraft on a regular basis to being in a ground-based assignment. It is good for the physical well-being of our federal air marshals, and it is also good for their family and just kind of stabilizes these schedules much more so than being in the air. So I would put VIPR first.

I would put law enforcement officer reimbursement second. And then the third—and only third because I think we might be able to get some technology solutions for this—is exit lane staffing, because when you think about it, we ought to be able to put a technology in place that prevents somebody from coming in the reverse direction in an exit lane.

And so I would rather push on the technology solution for that rather than the people solution.

Ms. ROYBAL-ALLARD. Okay. Mr. Fleischmann.

Mr. FLEISCHMANN. Thank you, again, Madam Chair. And Mr. Administrator, thank you for this very thorough hearing.

Sir, I understand that the TSA is in the process of updating key screening technology at our airports in order to keep passengers safe from threats that continue to evolve. I think using contractors in certain airports and registered known traveler programs, like TSA Pre and Clear, are areas where we have tried to make screening process faster and more efficient not only for the TSA, but also for the traveling public.

How is TSA using commercial technology to improve efficiency of operations at the checkpoint?

Mr. PEKOSKE. Sir, almost everything at our checkpoints is either commercial off-the-shelf or an adaptation of commercial off-the-shelf technology. And that is where we are proceeding for most of

the technology infusion for the next several years in our screening checkpoints.

But in answer to your first question, about research and development, there are some aspects of what we need to do at our screening checkpoints that there really is not a commercial solution available and we just need to get into some basic research and development on those items.

And I also think it is really important to be able to apply the security processes that we do based on the risk that passengers present. And that is where that credential authentication technology comes in so importantly, because just think from a technology perspective, we are going from taking somebody's driver's license or passport and visually examining it, putting an ultraviolet light on it or looking at it through a magnifying glass, and then trying to compare what is on the credential with the passenger in front of the officer to the point where those credentials get inserted into a machine and the machine comes back and says, yes, this is a valid Florida or a valid California or a valid Tennessee driver's license.

And then the really good part about it is that it automatically pulls the information from the credential, so it will pull the name, gender, and date of birth from the credential, and in real time, while the passenger is standing there, send that information back to our Secure Flight database, which will return a result that will say, yes, this is a bona fide pre-check passenger. This is a standard lane passenger. This is someone who needs additional screening.

And the other part is, it will also say, and this passenger has this flight today. So we will see the travel information. We will validate the credential. The image will come up on a screen. And so what ends up happening for the officer is, rather than being heads down, trying to match some very small printed info with the passenger in front of them, the machine takes care of a lot of that automatically, and then all of the information comes up on a screen. So you are looking more at the passenger, which I think is very beneficial from a security perspective. And it gives you the opportunity to have a conversation with the passenger, as well.

So I think the technology part of this is going to be critically important for not just passenger convenience, but really for security effectiveness, because this is also from an identity perspective very significant improvement.

Mr. FLEISCHMANN. Yes, sir. How has TSA fostered relationships with the private sector, specifically, when it comes to new technologies?

Mr. PEKOSKE. Sir, the reason we were able to move the computed tomography acquisition so quickly is because of our relationships with the private sector and because of the authorities that you have provided in law. We can accept gifts of technology from the private sector, as long as it is certified for operation in our screening checkpoints.

And so what we were able to do is do a lot of operational test and evaluation with equipment that was gifted to us from the private sector, which sped along that acquisition process.

Mr. FLEISCHMANN. Yes, sir. As you move forward with rolling out new systems, sir, are you collaborating with your partners to continue best practices to keep the security lines moving?

Mr. PEKOSKE. Yes, sir. We collaborate on everything, and I am always interested if there are better ways that we can collaborate that we will do them, because I want to make sure we have good, robust dialogue with our partners.

Mr. FLEISCHMANN. Good. Very briefly, the fiscal year 2020 budget request proposes to draw down funds from the aviation security capital fund to finance additional CT screening machines. I wholeheartedly endorse increasing the number of CT scanners in our airports, and I agree that purchasing the scanners using the aviation security capital fund meets the eligibility criteria for the fund.

However, I have concerns that the dollars in the fund have already been spoken for and have been allocated to very worthwhile security projects already on the drawing board for airports around the country. Can you say with certainty, sir, that this purchase will not have an unintended effect on delaying security projects already on the books?

Mr. PEKOSKE. Sir, the reason why we chose to go that route was because we felt that it would not have an effect on projects that were already on the books, but we also viewed this as a one-time event.

Mr. FLEISCHMANN. Yes, sir. One final question. Is the proposal one-time deal for fiscal 2020? Or do you anticipate using this accounting practice again?

Mr. PEKOSKE. Sir, we will evaluate it every year. But at this point, one time on 2020.

Mr. FLEISCHMANN. Thank you, sir. Madam Chair, I yield back.

Ms. ROYBAL-ALLARD. Ms. Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. Thank you, Madam Chair. I just had one additional question. And I know we already touched on the FAMS program, as well as the VIPR program. But having been involved in safety issues in my legislative agenda for many, many years, I really have sympathy for the difficulty associated with directly correlating the tangible benefits of programs that are intended to prevent harm, like the FAMS program, and I know the DHS IG expressed concern over the contribution that—to aviation security that the FAMS has, FAMS being the air marshals, for those that don't speak acronym.

So having said that, and knowing that we have safety programs that we utilize to make sure that we can put obstacles in the path of someone who might try to do someone else harm, and there is not really a way to measure, per se, what we prevented from occurring, can you explain how you are modernizing the FAMS program to address threats faced today? And then also just in terms of—you alluded to it on a previous answer, but I mean, I don't think people really realize how debilitating it can be on the human body for an individual to fly and go up and down and up and down. I mean, I know how debilitating it is just to be a commuter, but to fly, you know, three or so times a day.

Can you address whether you believe there is some value in giving the air marshals some ground-based assignments, like the VIPR teams, which certainly also provide a valuable service so that

they have a visible deterrence at airports, which would obviously help us expand our reach in terms of protecting people, and also address the impact—the physical impact on our air marshals?

Mr. PEKOSKE. Yes, ma'am. We just changed the concept of operations for how we deploy the federal air marshals. And I can't really go into a lot of detail on that new CONOPS in this setting, but suffice it to say that the new CONOPS results in much more effective employment of a very, very valuable and limited resource.

I would also say that, you know, I have great admiration for our federal air marshals. They perform a difficult job. It is not easy sitting in a plane for hours on end. If you are on a domestic deployment, sometimes three flights in a given day, just three takeoffs and landings, that is fatiguing. And they have got to be alert all the time.

And so we changed the concept of operations to be much more risk-based. And I think it has an awful lot more fidelity to it. And we also changed the way we place the air marshals in aircraft to be able to execute on that concept of operations.

Once we put that in place, we agreed with the inspector general in that we did not have good measures. And like you said, it is very hard to measure prevention, right? But nonetheless, we can measure certain things that will give us sort of a surrogate for how we are doing. And as we published this new CONOPS will be a set of measures that we will put in place to be able to assess the importance of this important and really this last layer of security. That is what I think about all the time is, you know, we spend a lot of money in all the vetting operations, very, very important for us to do a lot of money in our screening checkpoints, a lot of money in checked baggage screening.

We do really want to have that last line of defense with the Federal Air Marshal service. And as you have correctly stated, it is hard to be a flying federal air marshal for 6, 7, 8, 9, 10 years on end. And so one of the things that we are looking at is, how do we better manage that very important force of individuals for us? And part of that analysis is, can we identify more ground-based assignments to give them a bit of a break, and also importantly, to use their significant expertise?

I mean, these folks are experts in law enforcement. They are experts in aviation security. We can really get a lot more value, I think, by doing it that way.

Ms. WASSERMAN SCHULTZ. Absolutely. And, Madam Chair, I think it is important to just remind people, as we got a very unfortunate reminder at FLL, that our transportation security officers are part of the layers of protection. Safety, to be successful, requires layers of protection, because you need one there, and when that fails, then you have another. And, you know, you can't have infinite layers, but the air marshals are one of those layers and, like you said, the last line of defense.

And what we were reminded about—and I think many people weren't even consciously aware—that our TSOs actually are there to protect the airplane. And so we do have some work to do to educate the traveling public about what the role of the various security and safety responsibilities are at the airport, law enforcement, TSOs, the VIPRs, the air marshals, and make sure that we con-

tinue to move forward on the discussion that has been sparked from FLL and other airports on the run, hide, fight concept, and who is responsible for actually making sure that we can support the airport and protect passengers that aren't traveling—about to travel on an airplane.

Thank you. I yield back.

Ms. ROYBAL-ALLARD. I just have a follow-up question on the issue that was raised by the ranking member about the credential authentication technology. How long will it take to get to full operating capability?

Mr. PEKOSKE. Madam Chair, we should be able to purchase about 500 of the credential authentication technology systems in fiscal 2019. And then the budget requests another 300 or so more. It is going to take us about 2 more years after that to get the full operating capability, but we are going to be very smart as to how we deploy these systems.

And we are going to start with our pre-check lanes, because one of the concerns the Congress has expressed and I share is that we need to make sure that the individuals who voluntarily give us their background information and their biometrics get some noticeable, tangible benefit from their investment in the pre-check program. Because for us, this now becomes a trusted traveler, and we adjust our security based on that.

And so I want to put the CAT machines—I want to put technology where it will help accelerate a pre-check passenger or a global entry passenger's passage through security so we can focus our efforts more so on the individuals that need a little bit more attention.

Ms. ROYBAL-ALLARD. Has there been any issue with regards to the Clear program, anything that has raised any concerns about that?

Mr. PEKOSKE. There is a difference between the trusted traveler programs and a registered traveler program. A trusted traveler is a government program where we have the full background of individuals and we vetted those individuals and we also have their biometrics.

A registered traveler program is—exists for the sole purpose of validating identity. It doesn't do any government vetting of those passengers. And some registered traveler clients are standard lane passengers and some are pre-check passengers. It kind of varies across the board, alternative the predominance are pre-check passengers.

And we are looking at, how can we best integrate all the capability across? But with the credential authentication technology, because that is going to have risk-based information on passengers, that is a very critical, important function in our screening checkpoint. It is basically your entering argument to screening. And that is something, given that the information that is available to the officers, particularly as we get this live connection with the technology, that is so integral that it is a government function in our view.

And so we are exploring with our registered traveler partner how we move forward given that the CAT deployment is really beginning now and it is going to be in earnest in fiscal 2020, as well.

Ms. ROYBAL-ALLARD. Do you have any further questions?

Mr. FLEISCHMANN. I am good. Thank you, Madam Chairwoman.

Ms. ROYBAL-ALLARD. Okay. We still have a little bit of time, so I am going to just leave it up to you. Are there any questions that we didn't ask that you wished we had or any additional information that you would like to provide the subcommittee?

Mr. PEKOSKE. A couple things, ma'am. I appreciate the opportunity, because it is rare that a witness gets this opportunity. You will see in a very short period of time our first capital investment plan that kind of lays out what we know we need to invest over the future years' homeland security plan. And it is going to be constrained by the levels that the administration has approved in the FYSP, which is a logical presentation, but at least you will get to see all of the projects that we envision, so you can understand the scale of the technology investment that we think is needed.

You know, we have talked about the CT X-rays and we have talked about the credential authentication technology. Those are two that are already underway. CT, you know, to give you kind of a sense of scale, we are going to have 300 with this current fiscal 2019 purchase that we just made. Another 300 if the fiscal 2020 levels get approved. That is 600, but we have about 2,400 X-ray systems in the entire 440 airports that are federalized.

So it makes progress, but we have still got a long way to go. When Congressman Wasserman Schultz was talking about the AIT technology, the technology you put your hands over your heads, that is not even an acquisition program at this point in time. Now, as I mentioned to her, we have certified that technology, which means that if an airport or an airline wants to gift it to us, they have got some standards of performance that the machines need to meet that we—and we will tell them which machines are certified to those standards of performance, so we can accept those gifts, but there is no formal acquisition program for that.

So just context of, hey, you know, more technology investment is needed. And I would be most happy at anybody's convenience to sit down with you and kind of lay out the threat and then look at the capability of the existing screening system, and it will really illuminate why we need to make these technology enhancements—and the other thing is, you know, I think that has a big effect on the screening workforce.

You know, when you are working with more up-to-date tools, particularly the onbody anomaly detection, for example, if you don't need to do as many pat-downs as you are doing—because nobody likes to be patted down and nobody likes to conduct a pat-down—if we can get technology that gives us more certainty in that process and better detectability, I think it is a win for passengers and certainly a win for screening effectiveness.

The other thing that I would emphasize is how important the human dimension of what we do is. And you all know that—you have all expressed appreciation for the work of the TSA workforce. One of the things that has been really something that I reflect on all the time is how complex an agency this is. You know, most people think of TSA and they think of the screening checkpoint as the only part of the agency, and it is a very important part, and cer-

tainly the most visible part of TSA. But there is a lot of work that TSA does that most people don't realize that we are doing.

They don't see the checked luggage that is going to go in the hold of an aircraft that we inspect. They don't see our inspectors walking around airports making sure that there is compliance with our airport security plans and our carrier security plans. They don't see all of the international inspectors that we have all around the world making sure that if you get on a flight at an airport that has a direct flight to the United States, that we have a presence there and we are looking out for the security levels in those airports.

They don't see all of the individuals that work in our intelligence enterprise, that do all the very important vetting work that is important to be able to make sure that we have properly assessed the risk by passenger. And they really don't see everybody that needs to support that enterprise. And we have got thousands and thousands of very dedicated employees that make sure, you know, that our IT systems are up and running, that our pay systems are up and running, that our human capital systems are up and running.

And so it is a very complex enterprise. And I am very proud of every single person in the agency, because without—you know, we need everybody to be able to perform our mission. Congressman Wasserman Schultz talked about the Federal Air Marshal Service. They are designed to be not visible to passengers. And I am so glad that we have that layer of security.

So I would just, you know, take the opportunity just to emphasize in my opening statement, I said, hey, there is two really important things we need in this budget, technology investment and investment in our workforce. And I really appreciate the flexibility of this subcommittee in working our reprogramming requests along the way as we want to move some money around to be able to accomplish some of the initiatives that we know we can self fund, but we just need to change the nature of the funding. And you have been very, very helpful in that regard, and we very much appreciate it.

And you see a couple of—actually, three uniformed officers behind me. We made a change in our policy in TSA about a year ago, where I wanted to see a uniformed presence in the agency and I wanted to have transportation security officers—and they were all supervisory transportation security officers—I wanted to have them nearby all the senior leadership, so that when we were having policy discussions affecting our workforce, that we had people that actually represented the frontline right there in the discussion so that they could give us their input.

And then also over my right shoulder is a member of the Federal Air Marshals Service also on our front office staff that provides me that same perspective from a federal air marshal perspective. And it is really valuable in that a TSO may not call me, but they will definitely call Charles—or Pam, and they will—and an air marshal will call Cara, but they may not call me.

And so we are just trying to improve the levels of communication. But really, I sincerely—I said in my opening statement that I appreciate the oversight that you provide, because your questions cause us to constantly think about what we are doing to make sure that we have thought it through, and you and your staffs have

been there to support us every step of the way. And so we really appreciate it.

Ms. ROYBAL-ALLARD. Well, welcome to all of you, and thank you for everything that you do. As you can tell, there is bipartisan support and we will do everything we can to help you to continue to protect our nation.

Mr. PEKOSKE. Thank you, Chairwoman.

Ms. ROYBAL-ALLARD. Thank you.

Mr. PEKOSKE. I appreciate it. Thank you, Ranking Member. Thanks.

[Material submitted for inclusion in the record follows:]

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE David E. Price
David Pekoske, Administrator
Transportation Security Administration
Committee on Appropriations
Subcommittee on Homeland Security
FY2020 – TSA Budget Hearing
April 2, 2019

General Aviation Security

Background: During the hearing, I asked for example of the work done between TSA and the general aviation community to modernize security programs.

Question 4: Can you provide specific examples of work that you have done with the general aviation community that impact them, especially regarding the modernization of security programs?

- Can you please provide more information about the status of TSA's implementation of the Aviation Security Advisory Committee recommendations, especially regarding general aviation?
- Can you please give me an update on TSA's effort to dedicate a full-time general aviation representative as directed by the Disaster Response and Recovery Act of 2018 (P.L. 115-254).
- How are you prioritizing programs such as DASSP, Gateway, and other security programs used by general aviation aircraft to increase operational flexibility?

Answer: TSA has allocated five full-time personnel working with industry on the efficiency and effectiveness of the highest priority general aviation items: DCA Access Standard Security Program (DASSP), Gateways, and the Maryland Three (MD-3). For example, there is a team whose primary focus is the DASSP application process and gateway operations. This team works with the TSA Security Operations office in the field and Law Enforcement/Federal Air Marshals to facilitate the DASSP application process. This work includes identifies stakeholder issues of concern and improves communication regarding the application process, which is

completed electronically. Currently, the average DASSP application process takes approximately 90 days. This same team also coordinates VIP gateway operations with TSA field personnel. There is one full-time employee whose primary focus is processing MD-3 applications and engaging with MD-3 airports and operators.

As detailed in TSA's Report to Congress entitled, *Implementation Status of the Aviation Security Advisory Committee Recommendations (ASAC)* delivered to the Hill March 6, 2019, the ASAC General Aviation Subcommittee had made 19 recommendations since 2015. Of those recommendations, TSA concurred with 12, non-concurred with five, partially concurred with one, and returned one recommendation to the ASAC General Aviation Subcommittee because the recommendation was unclear. Currently, there are only seven recommendations TSA concurred with that remain in progress. A copy of this report will be provided to Committee members who have not already received a copy.

TSA has an Industry Engagement Manager who is dedicated full time to the General Aviation line of business. This manager is the primary point of contact for the General Aviation industry for questions and information and also serves as the government co-chair on the ASAC General Aviation sub-committee.

Intercity Bus Security Grant Program

Background: In 2018, for the second year in a row, TSA has released a report highlighting the ongoing threat of vehicle ramming attacks from terrorists. In the report, TSA outlined some best practices in partnerships with public and private sector transportation security partners to aid in preventing and mitigating the threat of large capacity vehicle ramming in our homeland. Unfortunately, the President's FY20 DHS budget eliminates the program.

Question 5: Can you please explain the importance of the Intercity Bus Security Grant Program to TSA?

- Did you consult with OMB and the Secretary of DHS regarding the elimination of federal funding for the IBSGP in FEMA's FY20 budget?
- What do you believe would be the consequences of eliminating this program?

Answer: The Intercity Bus Security Grant Program (IBSGP) has been valuable in helping the Transportation Security Administration (TSA) advance security initiatives across the over-the-road bus (OTRB) community. Since fiscal year (FY) 2003, over \$100 million has been awarded to OTRB companies for security projects. We work closely with the Federal Emergency Management Agency (FEMA), which administers the grants, to establish funding priorities to achieve security goals, funding projects that include vehicle security enhancements (CCTV, driver shields, GPS, and automatic vehicle location), facility security enhancements (fencing, lighting, CCTV, access control), training, security planning, and drills/exercises.

Coordination with the Secretary of DHS or Office of Management and Budget regarding the elimination of funding for IBSGP would fall to FEMA as the administrator of the grant program. However, TSA recognizes that a reduction or elimination of funding for the IBSGP may limit opportunities to fund advancements towards security objectives, such as facility and vehicle security enhancements, training, and other objectives. However, there is the need to balance security risks against limited funding and available resources. To that end, TSA provides a number of no-cost resources to the OTRB community (as well as the other surface modes of transportation) to help identify and address a variety of threats, to include vehicle ramming. These resources include:

- First Observer Plus™ security training program
- Intermodal Security Training and Exercise Program (I-STEP) and the Exercise Information System (EXIS)
- Transportation Security Template and Assessment Review Toolkit (T-START)
- Vehicle Ramming Attacks: Threat landscape, Indicators, and Best Practices for Countering the Threat
- Mode-specific Counterterrorism Guides

TSA is also engaged in a range of efforts to enhance efforts to safeguard the Nation's transportation systems, including the OTRB community. These efforts include establishment of the Surface Transportation Security Advisory Committee (as required by section 1969 of the *TSA Modernization Act*), which includes OTRB stakeholders, to enable stakeholders to advise, consult with, report to, and make recommendations to the Administrator on surface transportation security matters.

QUESTIONS FOR THE RECORD SUBMITTED BY

THE HONORABLE Grace Meng**David Pecoske, Administrator****Transportation Security Administration**

Committee on Appropriations

Subcommittee on Homeland Security

FY2020 – TSA Budget Hearing

April 2, 2019

Passenger Security Fees

Background: The FY2020 President’s Budget Request proposes \$2.9 billion annually over 10 years in new and higher federal aviation on top of the \$25 billion they already pay per year, some of which would be funded by increase TSA passenger security fees. However, since 2013 approximately \$1.3 billion per year in TSA fees have been diverted from their intended purpose – aviation security screenings – through budget cap agreements.

Question 6: Under this proposal, what will be the highest amount that this fee will reach? What do you believe is a reasonable limit for fees that passengers should pay?

Answer: Under the proposal, the TSA September 11th Security Fee would increase from \$5.60 per one-way trip to \$6.60 per one-way trip beginning January 1, 2020. Additionally, the proposal would increase the fee from \$6.60 to \$8.25 on October 1, 2020 and would remain at \$8.25 for future years. TSA believes that this fee is a reasonable increase for passengers.

Recruitment and Retention

Background: The TSA Strategy for 2018 – 2026 identifies recruiting and hiring a capable and diverse team while establishing TSA as “a federal employer of choice” to be key priorities. In the 2018 Federal Employee Viewpoint Survey, only about one-third of survey respondents agreed with the statement, “My work unit is able to recruit people with the right skills.” While this is an improvement over 2016 when only 26 percent agreed with this statement, TSA still has a long way to go to achieve its recruitment and retention goals.

Question 7a:

- What steps are TSA senior leaders taking to meet their strategic recruitment and hiring objectives?

Answer: To meet strategic recruitment and hiring objectives, TSA uses a mix of recruitment marketing tactics to reach diverse audiences, including:

- **Job Boards:** TSA posts open Job Opportunity Announcements on a variety of job boards (including LinkedIn, Indeed, CareerBuilder, LocalJobNetwork, Glassdoor, etc.) to reach active job seekers. Through LocalJobNetwork, TSA is able to reach a diverse talent pool with a nationwide network of diversity sites and 15,000+ local career and community-based organizations. On LinkedIn, CareerBuilder and Glassdoor, TSA is leveraging sponsored content, email blasts and banner ads to drive job ads to more targeted audiences and also reach potentially passive candidates in addition to active jobseekers.
- **Social Media:** To position TSA as a federal employer of choice, its social media management team has promoted both direct recruitment content (e.g. TSO Fast Track to Hire events in several cities across the U.S.) and shared a variety of employer brand-focused content, including posts across topics such as:
 - Veterans hiring and appreciation
 - Employee benefits
 - Diversity events/job fairs
 - TSA mission and values
- **Digital Recruitment Marketing and Media:** To engage active/passive jobseekers and reach potential candidates, TSA uses targeting tactics to advertise across a variety of digital channels including programmatic digital banner ads, geo-fenced mobile ads, and digital/streaming radio ads via Pandora, Spotify and iHeart Radio.
- **Traditional advertising:** Based on local talent market insights, TSA uses traditional advertising – radio, billboards, print publications, etc. – to reach both active and passive job seekers in key, local markets. TSA partners with various diversity-focused publications and has placed print advertisements in publications such as:
 - *US Veterans and Military Magazine*
 - *Black EOE Journal*
 - *Professional Women's Magazine*
 - *Hispanic Network Magazine*
 - *HBCU Careers Magazine*
 - *Equal Opportunity Publication Careers & the disABLED*
 - *Diversity in STEAM Magazine*
- **Job fairs, career conferences and hiring events:** From April 2018 through March 2019, TSA attended 633 career-focused events, including:
 - 30 diversity-focused events
 - 119 veteran/military-focused events
 - 2 disabled veteran-focused events

- 3 individuals with disabilities-focused events

Question 7b: What practices are being implemented to help make TSA the federal employer of choice for diverse talent, and how will you define success when it comes to meeting this strategic priority?

Answer: TSA promotes job opportunity announcements by using various recruitment marketing tactics to reach diverse audiences, including: job boards, social media, digital recruitment marketing and media, job fairs, career conferences and hiring events and traditional advertising (e.g., radio, billboards, print publications, etc.).

To identify the ideal candidates for employment, applicants are assessed according to critical competencies for successful performance. For example, the assessment for Transportation Security Officers (TSOs) includes a battery of computer-based tests and a structured interview. These assessments are currently being updated to improve person-job match and promote performance and retention. In addition, new interviewer training will be implemented to provide managers with the tools they need to select qualified candidates.

Measures of effectiveness for recruiting diverse talent can be found within TSA's annual reporting submissions (e.g., MD 715, Federal Equal Opportunity Recruitment Program (FEORP), and the Disabled Veterans Affirmative Action Program (DVAAP) Accomplishment Report). These reports are monitored to make adjustments to recruitment practices as needed.

Lastly, an indicator for determining whether TSA's workplace supports diverse talent is the Federal Employee Viewpoint Survey (FEVS). Annual progress is tracked through the Employee Engagement Index, which is comprised of three sub-indices: Leaders Lead, Supervisors, and Intrinsic Work Experiences. Also tracked as part of the Index are eight key employee engagement drivers: Performance Feedback, Performance Rating, Work-Life Balance, Training and Development, Job Resources, Merit System Principles, Collaborative Management, and Performance Reward and Recognition.

In 2018, all indices and nearly all drivers increased for the second straight year. In particular, from 2016 TSA noted a significant increase in the Merit System Principles driver, which serves to ensure that Federal personnel management practices support fairness and protect employees from arbitrary actions, favoritism, political coercion and reprisal.

Question 7c: Is TSA conducting an analysis of how its recruiting, hiring and retention were affected by the 35-day government shutdown?

Answer: TSA has closely monitored the impact of the recent lapse in appropriations. The table below shares the number of Transportation Security Officer (TSO) separations by month and fiscal year. Immediately after the 35-day government shutdown, there was an increase in TSO separations.

	2016	2017	2018	2019*
October	653	677	668	683
November	439	549	559	580
December	553	564	637	687
January	575	674	737	657
February	478	547	616	708
March	601	645	706	913
April	679	623	725	574
May	732	696	750	22
June	743	747	757	0
July	735	657	735	0
August	735	711	749	0
September	710	741	779	0
Totals	7,633	7,831	8,418	4,824

**The FY2019 values are a current snapshot as Separation Actions are still being processed for the current fiscal year.*

It is difficult to determine the full impact of the furlough on separation actions as individuals may have planned to transfer to another agency, resign, or retire prior to the lapse in government funding.

While the government shutdown may explain a portion of the increase in TSO separations in the February/March 2019 timeframe, the TSO attrition rate is also heavily impacted by the strength of the economy, unemployment levels, prevailing wages, and the competitiveness of the employment market. This economic impact is evident in the trends when evaluating year-to-year attrition increases; as the economy has improved year over year, the TSO attrition rate has climbed.

As a result of the lapse in government funding:

- Approximately 2,000 TSO candidate Airport Assessments were canceled, postponed, or missed.
- Approximately 550 TSO Entries on Duty (EOD) were missed or delayed.
- Recruitment actions for TSA HQ Management, Administrative and Professional (MAP) positions were placed on hold; positions were not posted, qualification reviews were not conducted, selection certificates were not issued, and no conditional or final offers were extended.
- Several HQ and Field based MAP new hires' EOD dates were delayed and re-scheduled.

- TSA canceled a Canine Handler class because final job offers could not be extended in time to get the students registered.

BIOMETRIC TECHNOLOGY

Background: A lot of work is being done in the area of biometrics, with Customs and Border Protection (CBP) being the lead.

Question 8:

- To what extent is TSA working collaboratively with CBP as far as utilizing biometric technology at TSA checkpoints?
- What infrastructure is TSA investing in?
- What technologies are you focused on, and how would this technology integrate into existing checkpoints?

Answer: In October 2018, TSA published the TSA Biometrics Roadmap for Aviation Security & the Passenger Experience (“Biometrics Roadmap”). This roadmap states the TSA commitment to working with U.S. Customs and Border Protection (CBP) in the international space and with certain TSA Pre✓® passengers. These policies cement a relationship that began in April 2018 when TSA and CBP signed a joint policy memo providing direction on the development and implementation of biometric technology at airports. As a result of this partnership, we have collaborated on a series of multi-phased pilots testing CBP’s facial recognition technology, to include the Traveler Verification Service (TVS) for identity verification of volunteer international travelers at the TSA checkpoint.

TSA first collaborated with CBP at the John F. Kennedy International Airport TSA checkpoint in 2017 by testing its facial recognition and matching technology for identity verification. TSA and CBP tested facial recognition technology again at Los Angeles International Airport (LAX) in August 2018 to assess the feasibility of TSA reliance on Traveler Verification Service (TVS) identification at the checkpoint in lieu of manual checks. In October 2018, TSA and CBP began testing the viability of non-checkpoint biometrics throughout the aviation passenger journey at Hartsfield-Jackson Atlanta International Airport with Delta Air Lines. This pilot is ongoing.

The next phase of TSA’s partnership with CBP entails a biometrics pilot at the TDC that uses TSA secure networks to integrate CBP’s TVS with Secure Flight vetting status into biometric matching to test further strengthening, streamlining, and automation of the current process. This pilot is projected to occur in early 2020 pending completion of several technical integration sprints.

While TSA and CBP coordinate efforts on passenger-facing biometrics today, TSA is also laying the groundwork for an eventual transition of relevant storage and matching capabilities to DHS Office of Biometric Identity Management (OBIM), the Department’s enterprise biometric

solution. TSA has engaged OBIM on the build out of its next generation Homeland Advanced Recognition Technology (HART) which will modernize and replace the legacy IDENT system.

For checkpoint passenger use cases, TSA is primarily focusing on facial recognition to improve security effectiveness at the travel document checker (TDC) position. Facial recognition may be integrated with Credential Authentication Technology (CAT) to provide additional means of verifying passenger ID against physical and, eventually, digital credentials (i.e. mobile driver's licenses). The ability to quickly and accurately verify passenger identity, associate that unique ID to their Secure Flight vetting status, and direct them to the correct level of physical (e.g. carry-on baggage) screening is a critical enabler for ensuring high standards of security effectiveness in the airport security checkpoint.

QUESTIONS FOR THE RECORD
SUBCOMMITTEE ON HOMELAND SECURITY
U.S. HOUSE COMMITTEE ON APPROPRIATIONS

Hearing on TSA's FY 2020 Budget- Administrator David Pekoske
Tuesday, April 2, 2019

Congressman Fleischmann

Question 1: Does TSA have data on the number of Tier 1 HSSM shipments that are completed in the United States each year? (please provide a yes or no answer)

- If no, please provide TSA's best estimate of the likely range – from low to high - of the number of annual shipments of Tier 1 HSSMs in the United States. What is the source of data for this estimate?
- If yes, for the latest year for which TSA has data, how many Tier 1 HSSM shipments were there in the United States? What is the source of TSA's data for Tier 1 HSSM shipment numbers?

Answer: The Transportation Security Administration (TSA) neither solicits nor maintains specific data on the number of Tier 1 Highway Security-Sensitive Materials (HSSM) shipments that are completed in the United States each year. Based on available data from the U.S. Department of Transportation and Bureau of Transportation Statistics, TSA estimates that less than one percent of the hazardous materials transported by truck are classified as Tier 1 HSSM.

Question 2: My understanding is that TSA does not have a tracking system ready for operational deployment that would provide TSA with real-time visibility of in-transit Tier 1 HSSM shipments.

- Assume that a terrorist attack using a Tier 1 HSSM shipment occurred causing significant, high-profile loss of life and property. Assume also that TSA – following the precedent set on 9/11 – elected to suspend Tier 1 HSSM shipments. The impact of even a short-term disruption in the HSSM supply chain would cause widespread and significant damage to the national economy. For example, the mining and heavy construction industries rely on just-in-time shipments of commercial explosives and would need to curtail operations within days of a shutdown. TSA would quickly face immense pressure to allow HSSM shipments to resume. Without a tracking system ready for emergency deployment to immediately inject security into the HSSM supply chain, how would TSA assure the public and Congress that it was safe for shipments to resume?¹

¹ For a longer discussion of the emergency scenario, refer to page 54, *Executive Report: Cost and Technology Considerations in Development of a Shipment Tracking Program for Highway Security Sensitive Materials Under Section 1554 of the 9/11 Act of 2007*; Kentucky Transportation Center; December 2013.

- If TSA does have a system ready for operational deployment, please provide the contact information for an individual at TSA who can brief Committee staff on the system and provide a demonstration.

Answer: TSA does not currently employ a tracking system for HSSM. As required by section 1554 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), TSA developed a prototype program, known as “FEDTRAK™” and conducted a cost-benefit evaluation related to deploying, equipping, and using tracking technology. While the project demonstrated some utility for the tracking of certain bulk shipments of hazardous materials, it also identified a number of technological and logistical barriers that a national system for the tracking of hazardous materials shipments would have to overcome. For example, the system would not track trucks that are rented and then used to transport hazardous materials, such as the vehicle Timothy McVeigh used for the attack on the Murrah Building in Oklahoma City. It would also have minimal benefits if motor carrier companies were not required to deploy and use the technology, which the statute prohibits. Finally, there is a high cost for the industry to install and use the equipment. Based on these factors, TSA is not pursuing longer funding work on the FEDTRAK™ project.

Should the risk assessment associated with shipments of Tier 1 HSSM change and indicate an increasing risk, TSA could use Security Directives or other appropriate means to compel motor carriers to comply with specific actions to lessen the vulnerability of these shipments. As a significant number of industry operators currently track their shipments, TSA could mandate via Security Directive that carriers report any adverse occurrences during transportation to TSA and the appropriate law enforcement agency for awareness and action.

In the meantime, TSA worked with industry to develop Security Action Items for Tier 1 HSSM.¹ The security action items address the following subject areas: prevention of unauthorized access, en-route security, high alert level protocols, security inspection policy and procedures, reporting policy and procedures, shipment pre-planning, advance notice of arrival and receipt confirmation procedures with receiving facility, pre-planning routes, and measures to allow for remote monitoring and tracking.

Question 3: My understanding is that a 2004 FMCSA study concluded that a tracking program would generate over \$5 Billion in security benefits. A later study by the Kentucky Transportation Center updated the data from the FMCSA report and reaffirmed FMCSA’s conclusion that the security benefits of a Tier 1 HSSM tracking program would far outweigh costs. In fact, the study concluded that the benefits would outweigh costs by over 40:1 using FMCSA’s evaluation framework. Put another way, the cost of a national tracking program for Tier 1 HSSM shipments would be justified if it prevented a single large-scale security incident in the next 150 years. My understanding is that TSA’s internal economics team verified these study results as did Oak Ridge National Laboratory (ORNL) in a subsequent review commissioned by TSA. I would appreciate it if TSA would provide a complete copy of the ORNL review to the Committee.

¹ The Security Actions Items are not included as they are protected as Sensitive Security Information under 49 CFR part 1520.

Answer: TSA contracted with ORNL Center for Transportation Analysis (CTA) to review security measures used by motor carriers that carry Tier 1 Highway Security-Sensitive Materials (HSSM) and determine the degree of risk reduction that could result with a centralized communications and tracking system referenced in Section 1554 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*. The study did not provide a cost/benefit analysis that compared the cost of implementation and sustained use of the technology to monetized security benefits. Instead, the study focused on whether preventing terrorist attacks using HSSM is possible through a program that combines driver login, very frequent GPS tracking, notification to law enforcement within ten minutes to allow for interdiction, and remote vehicle immobilization.

The study found that the technology could be useful and that the benefits are consistent whether the tracking and immobilization is performed by a private company, carrier dispatch or a public entity. Moreover, a system that does not use all of these components is less effective. For example, using a tracking system without the driver login requirement and without the remote immobilization was effective only five percent of the time. Given that the risk associated with a worst case scenario attack using a Tier 1 HSSM shipment is low and that there are other more cost effective mitigation measures that TSA could fund using its limited resources, to reduce risk in surface transportation, TSA chose not to continue funding this project at an estimated cost of \$20M a year.

A copy of the report (ORNL/TM-2015/475; Risk Assessment for Tier I Highway Security-Sensitive Materials (HSSM): Modeling Transportation Security Risks Using Attack Trees) is attached.



NL.TM-2015.475_R
ASSESSME...

WITNESSES

	Page
Gaynor, Peter T.	68
Prepared statement	71
Answers to submitted questions	105
Kelly, John V.	2
Prepared statement	5
Answers to submitted questions	45
Krebs, Christopher	124
Prepared statement	126
Answers to submitted questions	166
Pekoske, David	200
Prepared statement	203
Answers to submitted questions	232
Schultz, Admiral Karl	168
Prepared statement	171
Answers to submitted questions	195