Question#:	21
Topic:	MPP Process
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: What process does DHS use to determine which individuals to return to Mexico under the Migrant Protection Protocols (MPP)?

Response: Pursuant to MPP, aliens arriving from Mexico who are amenable to the process, and who in an exercise of discretion the officer or agent determines should be subject to MPP, will be issued an NTA and placed into section 240 removal proceedings. They will then be transferred to await proceedings in Mexico. Aliens in the following categories are not amenable to MPP: UACs; citizens or nationals of Mexico; aliens processed for expedited removal; aliens in certain special circumstances; any alien who is more likely than not to face persecution or torture in Mexico; or other aliens at the discretion of the Port Director or Chief Patrol Agent.

If an alien who is potentially amenable to MPP affirmatively states that he or she has a fear of persecution or torture in Mexico, or a fear of returning to Mexico, whether before or after they are processed for MPP or other disposition, that alien will be referred to USCIS so that an asylum officer can assess the claim. If USCIS assesses that an alien who affirmatively states a fear of return to Mexico is more likely than not to face persecution on account of a protected ground or torture in Mexico, the alien may not be processed for MPP. Officers and agents retain all existing discretion to process (or re-process) the alien for any other available disposition, including expedited removal, NTA, waivers, or parole.

Question#:	22
Topic:	MPP Screening
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: How does the Department of Homeland Security (DHS) screen for vulnerabilities, such as medical conditions, to ensure that individuals who are ineligible to be returned under the MPP are not improperly forced to wait in Mexico?

Response: As of January 28, 2019, CBP began conducting health interviews for all aliens in CBP custody. Medical assessments are conducted on every juvenile when they initially enter CBP custody, and on all adult aliens in custody who answer positively to a "referral mandatory" question during the health interview. The medical assessments will normally be conducted by CBP contracted medical professionals, other federal, state, and local credentialed healthcare providers, or CBP Emergency Medical Services (EMS), during exigent circumstances. Migrants who are determined to be "fit to travel" remain amenable to MPP.

Question: In determining whether an individual will be returned under MPP, do DHS officials ask whether the individual has a fear of being returned to Mexico? If not, how does this comply with the legal obligation against refoulement?

Response: No, DHS does not affirmatively ask aliens if they have a fear of being returned to Mexico. There is no legal basis or programmatic warrant to require DHS officials to affirmatively ask aliens if they have a fear of being returned to Mexico. No relevant source of law requires questioning every alien in this context.

If an alien who is potentially amenable to MPP affirmatively states that he or she has a fear of persecution or torture in Mexico, or a fear of return to Mexico, whether before or after they are processed for MPP, that alien will be referred to a USCIS asylum officer to assess whether it is more likely than not that the alien will face persecution or torture if returned to Mexico.

If USCIS determines that an alien who affirmatively states a fear of return to Mexico is more likely than not to face persecution or torture in Mexico, the alien may not be processed for MPP.

As explained, all aliens subject to MPP have the opportunity (and every incentive) to express a fear of return to Mexico, which triggers an interview by an asylum officer. Aliens can raise that fear at any time they are in the United States, including before or after they are processed for MPP or other disposition, or during or in transit to immigration proceedings. There is accordingly no meaningful barrier to an alien's asserting a fear of return to Mexico. Additionally, GOM has accorded all rights and freedoms recognized in [Mexico's] Constitution, the international treaties to which Mexico is a party, and it's Migration Law." Given that the GOM has acceded to both the 1951 Convention relating to the Status of Refugees and its 1967 Protocol, and ratified the *Convention Against Torture and Other Cruel, Inhuman or Degrading*

Question#:	22
Topic:	MPP Screening
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Treatment or Punishment, it is bound by *non-refoulement* obligations, as reflected in Mexico's Law on Refugees, Complementary Protection, and Political Asylum and other migration laws.

Question#:	23
Topic:	Crime in Mexico
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: Does DHS collect any information about how many individuals who have been returned to Mexico have been the victim of crime in Mexico while waiting for their U.S. hearing date? If so, please provide this information. If not, please explain why not.

Response: DHS does not collect information about crime statistics in Mexico. DHS respects the sovereignty of Mexico. It is the Mexican federal, state and local governments' prerogative on how to best provide security needs.

Question#:	24
Topic:	Mexican Work Permits
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: The joint U.S.-Mexico statement says that "Mexico will also offer jobs, health care and education" to individuals subject to MPP. Additionally, when MPP was introduced, DHS said that individuals subject to MPP would have the ability to apply for work permits. However, it has been reported that individuals returned to Mexico are not receiving work authorization or humanitarian visas.

Is the Mexican government providing work permits to individuals returned under MPP?

Response: GOM has committed to provide work permits; when DHS has asked about this, Mexican officials have reiterated their commitment to do so.

Question: Does Mexican immigration law permit the government to issue work authorization to individuals returned under MPP?

Response: Mexican officials have stated publically that individuals returned under MPP will be provided with whatever documentation is needed to live and work in Mexico for the pendency of their removal proceedings in the United States.

Question: What programs are in place to ensure that the Mexican government is providing jobs, health care, and education to individuals returned under MPP?

Response: The United States and Mexico collaborate on MPP implementation. The United States does not have programs "to ensure that the Mexican government is providing jobs, health care, and education to individuals returned under MPP." That would be contrary to Mexico's sovereignty. Rather, in conversations between governments, Mexico has consistently asserted its commitment to provide these services; the United States accepts those commitments in good faith.

Question#:	25
Topic:	MPP NTA's
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: It has been reported that notices to appear for asylum proceedings for MPP returnees routinely do not have the right address. How does DHS ensure that proper notice of hearings is provided to returnees as required by law?

Response: CBP ensures proper NTAs are provided to aliens being returned to Mexico by following the guidelines below:

- Aliens at the port of entry (POE) or at Border Patrol stations, who are processed for the MPP will receive a specific immigration court hearing date and time, found on the NTA. Every effort will be made to schedule similar MPP alien populations (e.g. single adult males, single adult females, family units) for the same hearing dates.
- Any alien who is subject to the MPP will be documented in the CBP database.
- In addition to a list of pro bono legal service providers, CBP provides aliens subject to MPP a tear sheet containing information about the process and directions on what time and date the aliens should appear at the designated POE to be processed into the United States and escorted/transported to court.
- As with any respondent in the U.S. immigration court system, MPP migrants may mail an EOIR-33 Change of Address form to the court to update the address where they reside. Additionally, MPP migrants may file a motion with the Immigration Judge for a change of venue to an immigration court in the jurisdiction of that new address, as is the case with any respondent in removal proceedings.

Question#:	26
Topic:	MPP Identity Documents
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: Recent reporting suggests that U.S. Customs and Border Protection (CBP) has confiscated identity documents of some individuals who have been returned under MPP and sent them to Mexico without their documentation. What is CBP's policy with regard to the identity documents of those subject to MPP?

Response: CBP TEDS policy states that documents determined to be genuine, unaltered, and issued under the proper authority to the migrant, must be returned to the migrant upon release, removal or repatriation or maintained in the detainees' personal property.

Question#:	27
Topic:	Biometric Information
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: What categories of biometric information does CBP collect at ports of entry along the border?

Response: CBP collects photographs and/or fingerprints at ports of entry, pursuant to applicable regulations and in connection with certain enforcement activities. CBP is also collecting DNA samples pursuant to applicable regulations and in connection with the booking process in a pilot program at Eagle Pass, Texas from criminal arrestees and from non-U.S. persons who are detained under the authority of the United States, aged 18-79.

Question: How does CBP collect this information?

Response: CBP collects digital fingerprints using a fingerprint scanner and/or a digital photograph using a camera. CBP may also collect fingerprints and photographs from aliens departing the United States at land ports of entry using a hand-held mobile device (BE-Mobile).

CBP collects DNA samples during the booking process in the Eagle Pass, Texas CODIS DNA pilot. The subject who's DNA is being collected is first informed of the process of collection, and handed a DNA collection swab to rub the inside of the cheek. The sample is placed in a paper envelope and mailed to the FBI for analysis.

Question: How does CBP store the biometric information that it collects at the border?

Response: The Automated Biometric Identification System (IDENT) is the central DHS-wide system for storage and processing of biometric and associated biographic information.

CBP does not store DNA information, but does note in the case processing systems whether a DNA sample was collected. CBP simply collects a DNA pursuant to applicable regulations and in connection with the booking process for forwarding to the FBI lab.

Question: Does CBP collect or store biometric information of U.S. citizens that enter or exit the country?

Response: CBP does collect biometric data from U.S. citizens who apply to participate in CBP's voluntary Trusted Traveler Program (TTP). However, U.S. citizens may elect, on a voluntary basis, to participate and use the facial recognition technology to match against their passport. For those who participate, a photo is taken and submitted to CBP's Traveler Verification System (TVS), solely for the purpose of validating the identity of the traveler and ensuring that the

Question#:	27
Topic:	Biometric Information
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

passport being presented belongs to the bearer of the document. Only CBP has access to this biometric data. All photos of U.S. Citizens are deleted within 12 hours of identity verification.

U.S. citizens who are arrested for a criminal violation have their fingerprints collected in all ports of entry. U.S. citizens who are arrested for a criminal violation in the pilot port of Eagle Pass, Texas entering or leaving the country are further subject to DNA collection.

Question: If so, does CBP provide U.S. citizens the opportunity to opt out of having their biometric information collected or stored by CBP in all instances where CBP collects and stores this information?

If CBP does not currently collect or store biometric information of U.S. citizens, does CBP intend to begin the collection and storage of such information for the expansion of facial recognition technology implementation or otherwise?

Response: Under current regulations, CBP may not require U.S. citizens to submit biometrics upon entry or exit in connection with its biometric entry/exit program. Travelers who do not wish to participate in this facial comparison process may notify a CBP Officer or an airline, airport or cruise line representative in order to seek an alternative means of verifying their identities and documents. CBP discards all photos of U.S. Citizens within 12 hours of identity verification.

CBP does not provide U.S. citizens who are arrested for criminal violations the option to opt out of biometric collection, including fingerprints or under the CODIS DNA collection pilot program at the port of Eagle Pass, Texas. U.S citizen subjects who refuse to comply with CODIS DNA collection are subject to additional felony charges pursuant to Department of Justic regulations.

Question#:	28
Topic:	Facial Recognition Technology
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: When CBP employs facial recognition technology, it must check the traveler's photograph against a database of biometric information that it already maintains in order to confirm the traveler's identity.

What sources does CBP rely on to populate this database?

Response: For all biometric matching deployments, the TVS relies on biometric templates generated from pre-existing photographs that CBP already maintains, known as a "gallery." These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters.

Question: Does CBP input or store photographs or other biometric information collected at the border into such a database?

Response: CBP does input photographs and fingerprints into the DHS system of record, IDENT, collected at the border for foreign nationals who are in scope for biometric entry or exit pursuant to 8 C.F.R. 215 and 235 Generally, this is all foreign nationals between the ages of 14 to 79 other than those in limited, sensitive visa categories, such as diplomats. It does not include U.S. citizens. Biometrics collected at the border by CBP, that are subject to storage, are stored in IDENT.

Question: Does CBP maintain a database of biometric information for U.S. citizens for the purpose of implementing and utilizing facial recognition technology?

Response: No. CBP uses images from the U.S. passport database to compare against those who present a U.S. passport, and then discards the facial images collected for matching purposes within 12 hours of that confirmation and does not store the new photograph.

Question: CBP has suggested that it deletes photographs that are taken of U.S. citizens at ports of entry within 12 hours. How does CBP ensure that U.S. citizens' biometric information is not being improperly stored?

Response: CBP monitors when photos are accessed and/or used in CBP's facial matching service, and deletion of U.S. citizen photographs collected for this purpose is verified during routine data analysis. Additionally, CBP conducts daily audits to ensure adherence to the retention policy. CBP documents the deletion of data and the encryption keys for the cloud service provider are stored using the provider's Key Management Service, on hardware hosted by the provider. This Key Management Service is a FedRAMP-compliant service that fully

Question#:	28
Topic:	Facial Recognition Technology
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

audits every time a key is used. The cloud service provider's auditing services allow the TVS to monitor every time the key is accessed programmatically. The cloud service provider selected for this initiative is required to adhere to the security and privacy controls required by NIST Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing," 66 and the DHS Chief Information Officer.

Question#:	29
Topic:	PII
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: Does CBP collect other sensitive personal information about U.S. citizens, such as license plate numbers? If so, does CBP similarly delete this information within 12 hours?

Response: In order to fulfill CBP's mission of securing the border, CBP routinely collects several biographic data elements from U.S. citizens crossing the border in order to record their entries and exits, verify their identity, identify if any U.S. citizens have active wants or warrants, and to perform threat assessments. Biographic data elements will include items such as name, date of birth, U.S. passport data, and information on the mode of travel used to cross the border, such as license plate information for personal vehicles or flight information for trips on commercial air carriers. This information is stored in CBP and DHS data systems, and is retained and deleted based on the rules set forth in the Systems of Records Notice (SORN) for that particular database. For the databases CBP manages, U.S. citizen data is retained for one year in the Advanced Passenger Information System (APIS); 15 years in the Border Crossing Information (BCI) System; and 75 years in TECS if related to a law enforcement action. For those U.S. citizens who voluntarily join CBP's TTP Global Enrollment, their data is retained in SORN for as long as they are a member, plus three years.

CBP collects personal data as required by current statutory and regulatory requirements. With respect to the license plate data, the agency's retention of the data is determined as follows:

Retention
The Mobile and Covert License Plate Reader devices collect and store information as discussed in DHS/CBP/PIA-049, CBP License Plate Reader Technology (Dec. 11, 2017). These devices store the license plate reads locally on each device only as long as necessary to transmit to the standalone server. Each Sector or Station is responsible for developing procedures for ensuring the devices are "cleared" or information has been transmitted to the local standalone server.

The license plate numbers, date, timestamp, and location of the reads as stored on the standalone server will be retained for no more than two years, unless linked to an active law enforcement investigation.

CBP has authority to inspect baggage and persons traversing the border. *See, e.g.*, 6 U.S.C. § 211(c) (authorizing CBP to "develop and implement screening and targeting capabilities, including the screening, reviewing, identifying, and prioritizing of passengers and cargo across all international modes of transportation, both inbound and outbound"); 19 U.S.C. §§ 482 (search of vehicles and persons), 507 (providing customs officers have the authority to demand assistance of any person in making any arrest, search, or seizure), 1461 (inspection of merchandise and baggage), 1496 (examination of baggage), 1582 (search of persons and

Question#:	29
Topic:	PII
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

baggage), 1589a (enforcement authority of customs officers), 1595a (seizure and forfeiture of merchandise); see also 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer.")

Travel records, including historical records, are essential in assisting CBP Officers with their risk-based assessment of travel and identifying potential links between known and previously unidentified threats. Analyzing these records for these purposes allows CBP to continue to effectively identify suspect travel patterns and irregularities.

Question#:	30
Topic:	Foreign Passengers
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: According to the DHS FY2018 Entry/Exit Overstay Report, "biometric exit solutions were operational at 15 locations, and CBP has received many commitment letters from airport authorities and/or air carriers supporting biometric exit operations. Since its inception, over two million passengers on over 15,000 flights have used the technology on exit." Have all of these two million passengers been foreign nationals?

Response: No, the two million passengers include in-scope aliens under 8 C.F.R. §§ 215.1(a)(1) and 235.8(f)(ii), as well as exempt aliens and U.S. citizens who voluntarily participate in the biometric boarding process.

Question#:	31
Topic:	Cybersecurity
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: What data security practices does CBP employ to protect the biometric information it collects and the databases it maintains from vulnerability to cyberattacks and hacking attempts?

Response: CBP maintains a defense in depth strategy for protecting sensitive data collected into databases. This strategy includes:

- **Network Defenses** – Three-tiered application architecture, Trusted Internet Connections, National Cyber Protection Systems, Intrusion Prevention Systems, full packet capture analysis and data analytics.
- **Application Protections** – Frequent patching, Static and dynamic code scanning, strong authentication, detailed logging, segregation of duties for key functions, encryption, and physical datacenter security controls.
- **Security Oversight** – Security Assessments, Certification and Accreditation, Plan of Action and Milestones (POAM) process for weakness remediation, employee vetting, and workforce security training.
- **Vulnerability Management** – CBP Bug Bounty Program, CBP Penetration Testing, vulnerability scanning every 72 hours, frequent database scanning, web application scanning, DHS National Cybersecurity Assessments and Technical Services (NCATS) assessments.
- **Security Operations Center** – 24x7 monitoring for security events, including Cyber Intelligence, Cyber Threat Hunting, Insider Threat monitoring, and Data Loss Protection monitoring.

Question#:	32
Topic:	Subcontractors
Hearing:	The Secure and Protect Act: a Legislative Fix to the Crisis at the Southwest Border
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: CBP has said that the recent breach of information collected at the border was due to a subcontractor that "violated mandatory security and privacy protocols outlined in their contract." What data security practices does CBP require of subcontractors who have been given access to sensitive information?

Response: CBP enforces applicable mandatory security and privacy controls in accordance with federal standards through the use of Information Sharing Agreements (ISA) to establish the information being shared, and contractually by unilateral agreement to uphold the Homeland Security Acquisition Regulations (HSAR) 15-01. This includes the HSAR DHS special clauses, Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015), and the expanded HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006) and 3052.204-71, Contractor Employee Access (SEP 2012). CBP evaluates contractors via a full field background investigation (FFBI) which requires specific clearance for access to Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI). CBP also examines the contract to determine the need for and level of access to PII and CUI and applies security controls as necessary to authorize the contractor, and by extension subcontractor(s) (in accordance with NIST SP 800-53, DHS Sensitive Systems Policy 4300A, CBP Information Systems Security Policies and Procedures Handbook 1400-05D).

Question: Does CBP certify compliance of subcontractors and vendors with CBP's data security requirements? If so, how?

Response: CBP assures compliance of contractors and subcontractors determined to require 'high risk' access to sensitive PII through the review of security authorization documents and continuous monitoring of deficiencies to verify compliance with federal regulations as established in the contract. The security authorization review includes Independent Verification & Validation (IV&V) of the contractor system, culminating in a Vendor Assessment Report. The vendor assessment consists of 1) Review of Security Authorization Process Documentation; 2) Review of the vendor's Independent Assessment (in accordance with NIST SP 800-53, DHS 4300A, CBP 1400-05D); 3) Security Review for enforcement of implementation of security requirements (minimum of annually); 4) Continuous Monitoring of deficiencies in accordance with NIST SP 800-53, DHS 4300A, CBP 1400-05D policies.