Question#:	1
Topic:	Time and resources
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: As established at the hearing, ICE is removing fewer criminal aliens after being given more resources. Accordingly, I would like to get a better sense of what it is that ICE is spending its time and resources on. Therefore, for FY 2015, please answer the following:

How many total man-hours were spent training ICE personnel on the "enforcement priorities" established by Secretary Johnson on November 20, 2014? If you do not have precise numbers, please provide your best estimate.

Response: U.S. Immigration and Customs Enforcement (ICE) deployed its mandatory training module, "Policies for the Apprehension, Detention and Removal of Undocumented Immigrants," in January 2015. That month, approximately 14,000 ICE agents, officers, and attorneys completed the training, which focused on the priorities set forth in the Secretary's November 2014 memorandum.

ICE deployed a second mandatory training module, "Priority Enforcement Program," (PEP) in June 2015. Approximately 14,000 ICE agents, officers, and attorneys also completed this training. ICE also published for the field reference materials related to the revised enforcement priorities and PEP. Moreover, ICE Enforcement and Removal Operations (ERO) provided additional PEP training to managers in ICE ERO's 24 field offices in August and September 2015. ICE ERO continues to provide PEP training to all new supervisors attending the Supervisory Leadership course in Dallas, Texas. Although ICE does not track this information, given the number of personnel trained, the agency estimates that it may have taken several thousand hours for the entirety of the workforce to be trained.

Question: How many total man-hours were spent on evaluating requests for stays of removal? If you do not have precise numbers, please provide your best estimate. Please also provide the total number of stays or removal granted.

Response: ICE is unable to provide an estimate on man-hours spent evaluating requests for stays of removal as such information is not recorded. ICE ERO field offices adjudicated approximately 8,500 requests for stays of removal in FY 2015. Stays may be granted for a variety of reasons, including allowing requisite time for an alien to get his or her affairs in order prior to self-removal, and Congressional private bill requests.

Question#:	1
Topic:	Time and resources
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: How many total man-hours were spent evaluating whether to exercise prosecutorial discretion of any kind for an alien? Of that number, how many man-hours were spent evaluating requests from aliens for prosecutorial discretion of any kind? If you do not have precise numbers, please provide your best estimate.

Response: ICE does not track the data as requested and cannot make estimates based on available case management data. In the normal course of conducting case management, ICE evaluates cases for both enforcement action and/or whether the exercise of prosecutorial discretion is appropriate on a case-by-case basis, reviewing and considering the facts of each individual case to inform such determinations.

Question: How many meetings did ICE personnel attend with non-profit organizations, attorneys representing aliens, or any other similar groups/individuals? If you do not have precise numbers, please provide your best estimate.

Response: ICE does not statistically track the data as requested and cannot make estimates based on available case management data.

Question: How many phone calls did ICE personnel receive from, or make to, non-profit organizations, attorneys representing aliens, or any other similar groups/individuals? If you do not have precise numbers, please provide your best estimate.

Response: ICE does not statistically track the data as requested and cannot make estimates based on available case management data.

Question: How many emails did ICE personnel receive from, or send to, non-profit organizations, attorneys representing aliens, or any other similar groups/individuals? If you do not have precise numbers, please provide your best estimate.

Response: ICE does not statistically track the data as requested and cannot make estimates based on available case management data.

Question: How many enforcement decisions of any kind made by personnel in ICE's field offices – whether in the form of a declination of an administrative closure, a declination of a case termination, a declination of a stay of removal, or any similar action – were reviewed and/or overturned by personnel at ICE headquarters? Of those decisions to review or overturn, how many were initiated by a request from non-profit organizations, attorneys representing aliens, or any other similar groups/individuals?

Question#:	1
Topic:	Time and resources
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Response: ICE ERO headquarters received and reviewed 155 requests that were originally reviewed and adjudicated by ICE ERO field offices. These requests are reviewed by deportation officers and an appropriate law enforcement chain of command. Of the 155 requests reviewed by ICE ERO headquarters from aliens or their representatives, ICE ERO exercised prosecutorial discretion in 29 of the 155 requests.

Although not formally tracked, the ICE Office of the Principal Legal Advisor (OPLA) headquarters reviewed approximately 150 requests for prosecutorial discretion received from aliens or their representatives that were previously reviewed by OPLA field offices.

Question: How many man-hours were spent undertaking the headquarters-level review referenced in question (1)(g) above? If you do not have precise numbers, please provide your best estimate.

Response: ICE does not track the data as requested and cannot make estimates based on available case management data.

Question#:	2
Topic:	ICE OPLA
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: After this Committee held a hearing on July 21, 2015, I submitted a number of questions for the record, to which ICE did not provide reasonable responses. For example, I asked whether, since January 20, 2009, ICE has ever granted "prosecutorial discretion" in any manner to an alien charged with or convicted of a crime. In a lengthy non-responsive answer, ICE said that it is "unable to report the requested level of detail regarding the granting of prosecutorial discretion, as this information is not maintained in a systematically reportable manner." This is not an accurate statement. ICE maintains multiple databases from which it can pull the requested information, including, but not limited to, the Principal Legal Advisor Network (PLAnet). PLAnet). Accordingly, please provide the requested information, in addition to these new specific data sets:

How many cases did the ICE Office of the Principal Legal Advisor (OPLA) administratively close in FY 2015? Please break down this number between cases involving aliens convicted of any criminal offense, and aliens not convicted of any criminal offense.

How many cases did ICE OPLA terminate in FY 2015? Please break down this number between cases involving aliens convicted of any criminal offense, and aliens not convicted of any criminal offense.

How many cases did ICE OPLA refuse to prosecute in FY 2015? Please break down this number between cases involving aliens convicted of any criminal offense, and aliens not convicted of any criminal offense.

Response: The U.S. Immigration and Customs Enforcement Office of the Principal Legal Advisor (ICE OPLA) does not have the authority to administratively close removal proceedings once they are properly pending against an alien in immigration court. Rather, the U.S. Department of Justice, Executive Office for Immigration Review (EOIR) possesses the authority to administratively close proceedings in the exercise of its independent judgement and discretion. *See generally Matter of Avetisyan*, 25 I&N Dec. 688 (BIA 2012). ICE OPLA defers to EOIR for information regarding the number of cases an immigration judge administratively closed in FY 2015.

Additionally, under the Immigration and Nationality Act's (INA) implementing regulations, ICE OPLA does not have the authority to terminate a removal proceeding once it is properly pending against an alien. This authority similarly rests with the immigration judge, who is a part of the EOIR. The immigration judge's authority to

Question#:	2
Topic:	ICE OPLA
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

dismiss or terminate a pending removal proceeding is found in 8 C.F.R. sections 1239.2(c) and (f).

In general, ICE OPLA does not refuse to prosecute cases but rather reviews most notices to appear (NTAs) prior to their filing with EOIR to ensure that they are legally sufficient and meet the Department of Homeland Security's (DHS) civil enforcement priorities as set forth in Secretary Johnson's November 20, 2014 memorandum entitled, "Policies for the Apprehension, Detention and Removal of Undocumented Immigrants." If a case falls outside of DHS's civil enforcement priorities, ICE OPLA will generally not file the NTA. Also, ICE OPLA rejects NTAs that are not legally sufficient and returns them to the issuing agency for correction.

Based on unverified data currently available through ICE OPLA's records, there were approximately 13,000 cases in FY 2015 in which ICE OPLA rejected an NTA because it was legally insufficient or fell outside DHS's civil enforcement priorities. For context, the available data also reflects that there were more than 180,000 cases in FY 2015 where an NTA was issued or an initial master calendar hearing was held. Unfortunately, ICE OPLA's systems do not permit it to break down these statistics by whether the aliens in question have or have not been convicted of any criminal offense.

Question#:	3
Topic:	Alien encounter
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: How many aliens did ICE encounter in any way, but not take an enforcement action against, in FY 2015?

Of those, please specify how many were convicted of a criminal offense.

Of those, please specify how many had a final order of removal.

Please provide the same information requested in the Question above for each fiscal year since FY 2009.

Response: U.S. Immigration and Customs Enforcement (ICE) does not statistically track all aliens it does not take enforcement action against. DHS is currently exploring new statistical techniques and data collection strategies to better track aliens who are not subject to removal or return.

Question#:	4
Topic:	Aliens with criminal convictions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: How many aliens with criminal convictions did ICE release from its custody as a matter of discretion in FY 2015?

Please provide the same information requested in the Question above for each fiscal year since FY 2009.

Response: Current law authorizes the release of certain aliens during the pendency of removal proceedings, including on bond and recognizance. *See* Immigration and Nationality Act (INA) § 236(a), 8 U.S.C. § 1226(a) (2016). Indeed, this detention authority providing for bond or other conditions of release has been a fixture of immigration law since the Immigration and Nationality Act of 1952. *See* former INA § 242(a). Congress created classes of individuals eligible for custody determinations as well as classes of individuals subject to mandatory detention under INA § 236(c). In instances where U.S. Immigration and Customs Enforcement (ICE) determines to continue detention in its discretion of an alien not subject to mandatory detention, such decisions are subject to review by the Department of Justice's Executive Office for Immigration Review, which may redetermine bond amount imposed or order release without bond. Furthermore, in certain situations, an alien may be released pursuant to the requirements of legal precedent [e.g., Zadvydas v. Davis, 533 U.S. 678 (2001)].

Please see below for numbers of criminal aliens[1] released by ICE, consistent with controlling law and regulation, for Fiscal Years (FY) 2013, 2014, and 2015. ICE began tracking these releases in a statistically reportable manner in FY 2013.

Unique Criminal Aliens Released Pursuant to an ICE Custody Determination by Fiscal Year[2]

Fiscal Year	Individuals Released
2013	**21,769**
2014	**17,360**
2015	**7,293**

[1] ICE defines "criminal aliens" as aliens who have a criminal conviction.

[2] Releases are pursuant to an ICE custody determination under INA § 236(a).

Question#:	4
Topic:	Aliens with criminal convictions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

In March of 2015, ICE instituted enhanced oversight and release procedures with respect to discretionary custody determinations involving certain criminal aliens convicted of certain crimes, including senior manager review of discretionary release decisions for individuals convicted of crimes of violence. DHS is committed to making certain that both mandatory and discretionary releases are executed in a way that promotes public safety and protects our communities.

Question#:	5
Topic:	Final orders of removal
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: As of the date of your response to this question, how many aliens with final orders of removal remain in the United States?

Response: As of April 11, 2016, U.S. Immigration and Customs Enforcement (ICE) records indicate that there are 946,662 aliens with final orders of removal who may remain in the United States.[3] This number includes individuals who cannot lawfully be removed at the present time due to certain protections afforded under the Immigration and Nationality Act, such as temporary protected status or withholding of removal; individuals who may be lawfully removed but who are no longer enforcement priorities; individuals who are enforcement priorities but who have been released under appropriate monitoring conditions due to case-specific circumstances, such as the requirements of *Zadvydas v. Davis*, 533 U.S. 678 (2001); and individuals who are enforcement priorities and are targeted for removal through ICE's increased at-large operations.

Question: Of those, please specify how many have ever been convicted of any criminal offense.

Response: As of April 11, 2016, of the aliens with final orders of removal who remain in the United States, 181,338 have been convicted of a felony, misdemeanor, or other offense.

Question: Of those, please specify how many are detained, by criminal status, and how many are not detained.

Response: As of April 11, 2016, of the 181,338 criminal aliens with final orders of removal who remain in the United States, 6,383 are detained, and 174,995 are not detained by ICE.

Question: Please provide the same information requested in the Question above for each fiscal year since FY 2009.

[3] This figure is based on aliens who have an active case with ICE. Aliens with an active case with ICE include those who are in immigration proceedings, as well as those who have been ordered removed but whom ICE is still supervising on the non-detained docket, coordinating removal, and/or has been unable to confirm departure. Not included in aliens who have an active case with ICE are aliens with cases that are closed, and aliens that were removed by U.S. Customs and Border Protection, or not turned over to ICE.

Question#:	5
Topic:	Final orders of removal
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Response:

	FY 2009	**FY 2010**	**FY 2011**	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**
Final Orders of Removal	901,760	881,298	854,922	857,168	872,504	896,856	931,107
Convicted of Criminal Offense	120,731	128,421	136,928	153,572	167,426	173,773	179,037
Detained[4]	5,673	5,862	6,665	8,389	8,434	7,399	6,564
Non-Detained	115,058	122,559	130,263	145,183	158,992	166,374	172,473

[4] Detained and non-detained data represent snapshot values for a given time. For this report, the end of fiscal year (YE) data was used to represent the fiscal year. The figures contained in this response for YE FY 2009 through FY 2015 are historical and remain static.

Question#:	6
Topic:	Removal proceedings
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: As of the date of your response to this question, how many aliens are currently in removal proceedings?

Response: U.S. Immigration and Customs Enforcement defers this response to the Department of Justice’s Executive Office for Immigration Review as it has the most accurate information regarding cases currently pending on its docket.

Question: Of those, please specify how many have ever been convicted of any criminal offense.

Response: See response above.

Question: Of those, please specify how many are detained – by criminal status – and how many are not detained.

Response: See response above.

Question: Please provide the same information requested in the question above for each fiscal year since FY 2009.

Response: See response above.

Question#:	7
Topic:	Removed from the United States
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: How many individuals who were admitted to the United States as refugees, regardless of any subsequent adjustment of status and naturalization, have been removed from the United States for any reason since September 11, 2001? Please break down the data on these individuals by year, criminality, basis for removal, and nexus to national security concerns of any kind.

Response: The Immigration and Nationality Act's (INA) removal provisions do not distinguish between aliens admitted as refugees and those admitted pursuant to other statutes. Given this, U.S. Immigration and Customs Enforcement (ICE) databases are not configured to report specifically on refugee-centric removals.

Question#:	8
Topic:	Removable criminal aliens
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: In response to a letter that I sent with other members of the Committee in July, ICE said that it could not provide the number of aliens present in the United States who have ever been convicted of a criminal offense, because “it does not have sufficient information to determine alienage or criminality regarding all individuals present in the United States who may be aliens.” However – and understanding that it involves a slightly different set of data – in the Congressional Budget Justification that DHS submitted for FY 2013, ICE estimated that “1.9 million removable criminal aliens” were in the United States at that time. Please provide the total estimated number of removable criminal aliens present in the United States as of the day you respond to these questions.

Response: The Department of Homeland Security’s Office of Immigration Statistics is working to produce an estimate of the number of removable criminal aliens in the United States. At this time, there is not sufficient information to determine alienage or criminality regarding all individuals present in the United States who may be aliens.

Question#:	9
Topic:	Federal Bureau of Prisons
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

Question: As you know, pursuant to United States Sentencing Commission Amendment 782, the Federal Bureau of Prisons is releasing thousands of prisoners from its custody before their original release dates, including thousands of criminal aliens.

1. How many aliens the Bureau of Prisons has already released pursuant to this amendment?

Response: United States Sentencing Commission (USSC) Amendment 782, which was passed in November 2014, lowered the sentencing guidelines applicable to base offense levels in the Drug Quantity Table.[5] Since December 2014, U.S. Immigration and Customs Enforcement (ICE) has been working closely with the Department of Justice Bureau of Prisons (BOP) to identify foreign-born inmates both eligible and approved for such sentence reductions. A total of 1,772 foreign-born inmates were released on October 30, 2015 and November 2, 2015. Beyond this initial 2-day discharge in 2015, the remaining 4,191 releases will be spread out over the course of several decades through the year 2048. Please note these numbers are expected to fluctuate if federal judges grant more motions for sentence reductions. In addition, as federal judges decide appeals, the number of sentence reductions for foreign-born inmates is expected to change.

Question 2: How many aliens the Bureau of Prisons expects to release pursuant to this amendment?

Response: Please see response to Question 1.

Question 3: Of the aliens who have already been released, how many have been taken into ICE custody?

Response: In order to ensure that aliens amenable to removal from the United States would be remanded to ICE custody upon release, ICE worked with BOP to confirm active immigration detainers active were lodged on all aliens subject to removal who were released by BOP during the initial 2-day discharge in 2015. As such, all inmates released in the initial 2-day discharge were interviewed by ICE to confirm alienage,

[5] For the applicable substances, quantities, and subsequent base offense levels in the Drug Quantity Table, please visit http://www.ussc.gov/guidelines-manual/2012/2012-2d11.

Question#:	9
Topic:	Federal Bureau of Prisons
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

criminal history, and removability, as well as to facilitate the completion of the necessary documentation to issue an administrative removal order, or alternatively, the issuance of a charging document to initiate removal proceedings. ICE will do the same for subsequent releases. While ICE intends to expeditiously pursue removal for all individuals with final orders, ICE assesses each case once the alien is remanded to ICE custody in order to make appropriate custodial decisions, to include application of prosecutorial discretion and, for post-order aliens, whether release is appropriate or required pursuant to *Zadvydas v. Davis*, 533 U.S. 678 (2001).

ICE can confirm that, as of May 14, 2016, more than 90 percent of the foreign-born individuals released by BOP in the initial 2-day discharge have already been removed from the United States.

Question 4: Of the aliens who have already been released, how many have not been taken into ICE custody?

Response: ICE took *all* of the 1,772 foreign-born inmates who were released on October 30, 2015 and November 2, 2015 by BOP into its custody. Of the 1,772 individuals taken into ICE custody during the initial 2-day BOP discharge, ICE released only 22 individuals, including 17 who were released pursuant to *Zadvydas after* determining that there was no significant likelihood of removal in the reasonably foreseeable future. In addition, in making its initial custody determinations, ICE identified five individuals with significant medical conditions, rendering their detention and/or removal highly problematic. In these medical cases, ICE exercised prosecutorial discretion with regard to taking these individuals into custody. ICE is working cooperatively with U.S. Probation and Pretrial Services so that appropriate accommodations can be made for these individuals.

Question 5: For each alien who was not taken into ICE custody, can you please provide an explanation to us?

Response: Please see response to Question 4.

Question 6: Of the aliens that you expect the Bureau of Prisons to release in the future, how many does ICE anticipate taking into its custody? For each whom ICE will not take into its custody, please provide a detailed explanation.

Response: Please see response to Question 3.

Question#:	9
Topic:	Federal Bureau of Prisons
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Jeff Sessions
Committee:	JUDICIARY (SENATE)

In addition, due to a recent change in BOP processes, BOP now offers ICE, instead of state or local jurisdictions, the first opportunity to take into custody a removable alien.

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: ICE Functions and Possible Interference with the Enforcement Mission

During your hearing testimony, you did not provide an adequate answer regarding how Immigration and Customs Enforcement (ICE) could see its dedicated detention and removal budget increase by more than $800 million in the last four fiscal years, and yet nevertheless demonstrate what can only be described as a reduction in the agency's capacity to enforce its core immigration mission. The data raise significant questions about whether ICE funds are being used intelligently, appropriately, and even legally.

This issue dovetails with Secretary of Homeland Security Jeh Johnson's answers to questions asked by this committee in the wake of our April 2015 Department of Homeland Security (DHS) oversight hearing. In response to a question about legal hiring in support of ICE's mission, Secretary Johnson stated that "ICE is charged not only with immigration enforcement but with enforcing more than 400 federal statutes involving everything from counter proliferation to child pornography" (emphasis added). Secretary Johnson's answers raise two significant, related concerns: first, that ICE may not view its core mission to be immigration enforcement; and second, that ICE may be distracted by its non-immigration duties.

Please list all of the "more than 400 federal statutes" mentioned by Secretary Johnson.

Do any of these 400 federal statutes generate revenue for ICE? If the answer is yes, please provide the following information:

The statutory authority or authorities that permit the generation of such revenue.

For each of the authorities cited in Question (1)(a), the amount of revenue that has been generated from Fiscal Year (FY) 2009 through FY 2015.

For each of the authorities cited in Question (1)(a), whether the revenue generated is deposited into an offsetting account in the general fund of the United States Treasury, or into the general fund itself.

Response: Following passage of the Homeland Security Act of 2002, U.S. Immigration and Customs Enforcement (ICE) was established as the principal investigative arm of the Department of Homeland Security (DHS) and the DHS component responsible for interior immigration enforcement functions, including the detention and removal program. 6 U.S.C. § 542 note; DHS Reorganization Plan, H.R. Doc. No. 108-32 (2003).

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

ICE was also charged with executing the interior enforcement mission of the former U.S. Customs Service. As a result, ICE possesses all of the investigative authorities previously held by both the former U.S. Customs Service and the former Immigration and Naturalization Service. DHS Delegation of Authority, Number 7030.2, delegated the authority needed to enforce all combined statutory, administrative, and executive authorities that were delegated to ICE from the Secretary of Homeland Security to the ICE Assistant Secretary.

ICE enforces federal laws governing border control, customs, trade, and immigration to promote homeland security and public safety. ICE disrupts and dismantles transnational criminal organizations that exploit our borders by preventing terrorism and enhancing national security, and enforcing and administering our immigration laws. ICE also identifies, apprehends, and removes criminal and other removable aliens from the United States. ICE carries out its mission through two principal operating components: Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO). Additionally, the Management and Administration directorate provides administrative support to these subcomponents; the Office of the Principal Legal Advisor provides ICE’s legal advice, including representing the Department in removal proceedings before the Executive Office for Immigration Review; and the Office of Professional Responsibility investigates allegations of criminal misconduct at ICE.

- ICE ERO officers enforce our Nation’s immigration laws by identifying and apprehending removable aliens, detaining these individuals when necessary, and removing them from the United States. To protect public safety and national security, ICE prioritizes the removal of individuals who pose a danger to national security or a risk to public safety, including aliens apprehended at the border while attempting to unlawfully enter the United States and aliens convicted of crimes, with particular emphasis on violent criminals, felons, and repeat offenders.

- ICE HSI agents conduct transnational criminal investigations to protect the United States against terrorist and other criminal organizations that threaten public safety and national security and bring to justice those seeking to exploit our customs and immigration laws worldwide. As a border enforcement agency, ICE HSI has the authority to investigate cross-border crimes related to illicit trade, travel, immigration, and finance. ICE HSI may utilize over 400 federal statutes and regulations to investigate immigration and customs violations, including export enforcement; human rights violations; narcotics, weapons, and contraband smuggling; financial crimes; cybercrimes; human trafficking and smuggling; child

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

exploitation; intellectual property violations; transnational gangs; and immigration benefit fraud.

Over the last 5 years, ICE HSI criminal investigations have resulted in individuals being charged with civil, criminal, and administrative violations of more than 560 different statutes and regulations, including dozens related to immigration enforcement. The following list represents the diversity of statutes that are under ICE HSI's investigative authority as a criminal investigative agency. Note that this list is not exhaustive and does not include all of ICE HSI's statutory authorities, but rather, it demonstrates the wide range of investigative areas under ICE HSI's authority. Although some of these statutory authorities overlap with the work of other agencies, ICE HSI has authority in these areas as they relate to criminal acts with a nexus to the border.

Statutes and Regulations Charged as a Result of ICE HSI Investigations since 2011

Title 7, U.S.C.
7 U.S.C. § 2024
7 U.S.C. § 2156

Title 8, U.S.C.
8 U.S.C. § 1224
8 U.S.C. § 1252(d)
8 U.S.C. § 1253
8 U.S.C. § 1253(a)(1)
8 U.S.C. § 1304(e)
8 U.S.C. § 1306(a)
8 U.S.C. § 1306(b)
8 U.S.C. § 1306(c)
8 U.S.C. § 1321
8 U.S.C. § 1324
8 U.S.C. § 1324(a)(2)
8 U.S.C. § 1324(b)
8 U.S.C. § 1324(b)(1)
8 U.S.C. § 1324A
8 U.S.C. § 1324A(a)(1)
8 U.S.C. § 1324A(a)(2)
8 U.S.C. § 1324A(f)(1)
8 U.S.C. § 1324(a)(1)(A)(i)
8 U.S.C. § 1324(a)(1)(A)(ii)

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

8 U.S.C. § 1324(a)(1)(A)(iii)
8 U.S.C. § 1324(a)(1)(A)(iv)
8 U.S.C. § 1324(a)(1)(A)(v)
8 U.S.C. § 1324(a)(1)(A)(v)(I)
8 U.S.C. § 1324(a)(1)(A)(v)(II)
8 U.S.C. § 1324(a)(1)(B)(i)
8 U.S.C. § 1324(a)(1)(B)(ii)
8 U.S.C. § 1324(a)(2)(B)(iv)
8 U.S.C. § 1324(a)(3)(A)
8 U.S.C. § 1324C
8 U.S.C. § 1324C(e)(1)
8 U.S.C. § 1325
8 U.S.C. § 1325(a)
8 U.S.C. § 1325(a)(1)
8 U.S.C. § 1325(a)(2)
8 U.S.C. § 1325(a)(3)
8 U.S.C. § 1325(b)
8 U.S.C. § 1325(c)
8 U.S.C. § 1326
8 U.S.C. § 1326(a)
8 U.S.C. § 1326(b)(1)
8 U.S.C. § 1326(b)(2)
8 U.S.C. §1327
8 U.S.C. § 1328

Title 10, U.S.C.
10 U.S.C. § 801
10 U.S.C. § 885

Title 13, U.S.C.
13 U.S.C. § 305

Title 15, U.S.C.
15 U.S.C. § 78(d)
15 U.S.C. § 1125
15 U.S.C. § 1644
15 U.S.C. § 2068

Title 16, U.S.C.
16 U.S.C. § 703

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

16 U.S.C. § 1538
16 U.S.C. § 1538(c)
16 U.S.C. § 1538(c)(1)
16 U.S.C. § 1538(e)
16 U.S.C. § 1540
16 U.S.C. § 3371
16 U.S.C. § 3372
16 U.S.C. § 3372(a)
16 U.S.C. § 3372(a)(1)
16 U.S.C. § 3373
16 U.S.C. § 3373(d)
16 U.S.C. § 3374

Title 17, U.S.C.
17 U.S.C. § 506
17 U.S.C. § 506(a)
17 U.S.C. § 1201

Title 18, U.S.C
18 U.S.C. § 2
18 U.S.C. § 2(a)
18 U.S.C. § 3
18 U.S.C. § 4
18 U.S.C. § 13
18 U.S.C. § 42
18 U.S.C. § 111
18 U.S.C. § 113
18 U.S.C. § 115
18 U.S.C. § 152
18 U.S.C. § 201
18 U.S.C. § 208
18 U.S.C. § 215
18 U.S.C. § 286
18 U.S.C. § 287
18 U.S.C. § 331
18 U.S.C. § 333
18 U.S.C. § 371
18 U.S.C. § 373
18 U.S.C. § 401
18 U.S.C. § 402

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

18 U.S.C. § 471
18 U.S.C. § 472
18 U.S.C. § 473
18 U.S.C. § 474
18 U.S.C. § 480
18 U.S.C. § 492
18 U.S.C. § 500
18 U.S.C. § 506
18 U.S.C. § 506(a)(1)
18 U.S.C. § 510
18 U.S.C. § 511
18 U.S.C. § 513
18 U.S.C. § 541
18 U.S.C. § 542
18 U.S.C. § 543
18 U.S.C. § 544
18 U.S.C. § 545
18 U.S.C. § 546
18 U.S.C. § 548
18 U.S.C. § 549
18 U.S.C. § 553
18 U.S.C. § 554
18 U.S.C. § 555
18 U.S.C. § 611(a)
18 U.S.C. § 641
18 U.S.C. § 659
18 U.S.C. § 661
18 U.S.C. § 662
18 U.S.C. § 665
18 U.S.C. § 666
18 U.S.C. § 701
18 U.S.C. § 709
18 U.S.C. § 712
18 U.S.C. § 716
18 U.S.C. § 751
18 U.S.C. § 758
18 U.S.C. § 841
18 U.S.C. § 841(a)
18 U.S.C. § 842
18 U.S.C. § 844

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

18 U.S.C. § 845
18 U.S.C. § 846
18 U.S.C. § 848
18 U.S.C. § 871
18 U.S.C. § 873
18 U.S.C. § 875
18 U.S.C. § 876
18 U.S.C. § 894
18 U.S.C. § 911
18 U.S.C. § 912
18 U.S.C. § 921
18 U.S.C. § 922
18 U.S.C. § 922(a)
18 U.S.C. § 922(a)(3)
18 U.S.C. § 922(a)(6)
18 U.S.C. § 922(e)
18 U.S.C. § 922(g)
18 U.S.C. § 922(g)(1)
18 U.S.C. § 922(g)(2)
18 U.S.C. § 922(g)(3)
18 U.S.C. § 922(g)(5)
18 U.S.C. § 922(i)
18 U.S.C. § 922(j)
18 U.S.C. § 922(k)
18 U.S.C. § 923
18 U.S.C. § 924
18 U.S.C. § 924(a)
18 U.S.C. § 924(b)
18 U.S.C. § 924(c)
18 U.S.C. § 924(c)(1)
18 U.S.C. § 924(d)
18 U.S.C. § 924(j)
18 U.S.C. § 925
18 U.S.C. § 930
18 U.S.C. § 951
18 U.S.C. § 952
18 U.S.C. § 956
18 U.S.C. § 981
18 U.S.C. § 981(a)(1)
18 U.S.C. § 982

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

18 U.S.C. § 984
18 U.S.C. § 1001
18 U.S.C. § 1002
18 U.S.C. § 1014
18 U.S.C. § 1015
18 U.S.C. § 1015(a)
18 U.S.C. § 1015(b)
18 U.S.C. § 1015(c)
18 U.S.C. § 1015(d)
18 U.S.C. § 1015(e)
18 U.S.C. § 1015(f)
18 U.S.C. § 1028
18 U.S.C. § 1028(a)(1)
18 U.S.C. § 1028(a)(2)
18 U.S.C. § 1028(a)(3)
18 U.S.C. § 1028(a)(4)
18 U.S.C. § 1028(a)(5)
18 U.S.C. § 1028(a)(6)
18 U.S.C. § 1028A
18 U.S.C. § 1029
18 U.S.C. § 1029(a)
18 U.S.C. § 1030
18 U.S.C. § 1036
18 U.S.C. § 1038
18 U.S.C. § 1071
18 U.S.C. § 1073
18 U.S.C. § 1084
18 U.S.C. § 1111
18 U.S.C. § 1112
18 U.S.C. § 1113
18 U.S.C. § 1114
18 U.S.C. § 1117
18 U.S.C. § 1201(a)
18 U.S.C. § 1201(a)(1)
18 U.S.C. § 1201(c)
18 U.S.C. § 1202
18 U.S.C. § 1203
18 U.S.C. § 1203(a)
18 U.S.C. § 1306
18 U.S.C. § 1341

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

18 U.S.C. § 1342
18 U.S.C. § 1343
18 U.S.C. § 1344
18 U.S.C. § 1349
18 U.S.C. § 1351
18 U.S.C. § 1361
18 U.S.C. § 1363
18 U.S.C. § 1423
18 U.S.C. § 1424
18 U.S.C. § 1425
18 U.S.C. § 1425(a)
18 U.S.C. § 1425(b)
18 U.S.C. § 1426
18 U.S.C. § 1426(a)
18 U.S.C. § 1427
18 U.S.C. § 1460
18 U.S.C. § 1461
18 U.S.C. § 1462
18 U.S.C. § 1465
18 U.S.C. § 1470
18 U.S.C. § 1503
18 U.S.C. § 1505
18 U.S.C. § 1507
18 U.S.C. § 1510
18 U.S.C. § 1512
18 U.S.C. § 1512(b)
18 U.S.C. § 1512(b)(1)
18 U.S.C. § 1512(b)(3)
18 U.S.C. § 1513
18 U.S.C. § 1519
18 U.S.C. § 1541
18 U.S.C. § 1542
18 U.S.C. § 1543
18 U.S.C. § 1544
18 U.S.C. § 1545
18 U.S.C. § 1546
18 U.S.C. § 1546(a)
18 U.S.C. § 1546(b)(1)
18 U.S.C. § 1546(b)(2)
18 U.S.C. § 1546(b)(3)

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

18 U.S.C. § 1581(a)
18 U.S.C. § 1584
18 U.S.C. § 1589
18 U.S.C. § 1590
18 U.S.C. § 1591
18 U.S.C. § 1592
18 U.S.C. § 1594
18 U.S.C. § 1621
18 U.S.C. § 1623
18 U.S.C. § 1708
18 U.S.C. § 1715
18 U.S.C. § 1716
18 U.S.C. § 1832
18 U.S.C. § 1951
18 U.S.C. § 1952
18 U.S.C. § 1952(a)(1)
18 U.S.C. § 1952(a)(2)
18 U.S.C. § 1953
18 U.S.C. § 1955
18 U.S.C. § 1956
18 U.S.C. § 1956(a)(1)
18 U.S.C. § 1956(a)(2)
18 U.S.C. § 1956(a)(3)
18 U.S.C. § 1956(h)
18 U.S.C. § 1956(a)(1)(A)
18 U.S.C. § 1956(a)(1)(B)(i)
18 U.S.C. § 1956(a)(2)(A)
18 U.S.C. § 1957
18 U.S.C. § 1958
18 U.S.C. § 1959
18 U.S.C. § 1959(a)(1)
18 U.S.C. § 1959(a)(5)
18 U.S.C. § 1959(a)(6)
18 U.S.C. § 1960
18 U.S.C. § 1961
18 U.S.C. § 1962
18 U.S.C. § 1962(c)
18 U.S.C. § 1962(d)
18 U.S.C. § 1963
18 U.S.C. § 2111

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

18 U.S.C. § 2112
18 U.S.C. § 2119
18 U.S.C. § 2199
18 U.S.C. § 2232
18 U.S.C. § 2237
18 U.S.C. § 2241
18 U.S.C. § 2242
18 U.S.C. § 2244
18 U.S.C. § 2250
18 U.S.C. § 2251
18 U.S.C. § 2251(b)
18 U.S.C. § 2251(d)
18 U.S.C. § 2251A
18 U.S.C. § 2252
18 U.S.C. § 2252(a)
18 U.S.C. § 2252(a)(2)
18 U.S.C. § 2252A
18 U.S.C. § 2253
18 U.S.C. § 2254
18 U.S.C. § 2255
18 U.S.C. § 2260A
18 U.S.C. § 2261
18 U.S.C. § 2285
18 U.S.C. § 2312
18 U.S.C. § 2313
18 U.S.C. § 2314
18 U.S.C. § 2315
18 U.S.C. § 2318
18 U.S.C. § 2319
18 U.S.C. § 2319(b)
18 U.S.C. § 2320
18 U.S.C. § 2320(a)
18 U.S.C. § 2321
18 U.S.C. § 2323(a)(1)
18 U.S.C. § 2323(b)(1)
18 U.S.C. § 2326
18 U.S.C. § 2332A
18 U.S.C. § 2339A
18 U.S.C. § 2340(a)
18 U.S.C. § 2342

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

18 U.S.C. § 2421
18 U.S.C. § 2422
18 U.S.C. § 2423
18 U.S.C. § 2423(a)
18 U.S.C. § 2423(b)
18 U.S.C. § 2423(c)
18 U.S.C. § 2423(d)
18 U.S.C. § 2423(e)
18 U.S.C. § 2424
18 U.S.C. § 3144
18 U.S.C. § 3146
18 U.S.C. § 3148
18 U.S.C. § 3184
18 U.S.C. § 3606
18 U.S.C. § 4213

Title 19, U.S.C.
19 U.S.C. § 507
19 U.S.C. § 1304
19 U.S.C. § 1304(a)
19 U.S.C. § 1305
19 U.S.C. § 1433(b)
19 U.S.C. § 1436
19 U.S.C. § 1436(a)(1)
19 U.S.C. § 1436(a)(2)
19 U.S.C. § 1459
19 U.S.C. § 1497
19 U.S.C. § 1526
19 U.S.C. § 1526(b)
19 U.S.C. § 1581
19 U.S.C. § 1584
19 U.S.C. § 1589A
19 U.S.C. § 1590
19 U.S.C. § 1592
19 U.S.C. § 1595
19 U.S.C. § 1595A(a)
19 U.S.C. § 1595A(d)

Title 21, U.S.C.
21 U.S.C. § 331

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

21 U.S.C. § 331(a)
21 U.S.C. § 331(c)
21 U.S.C. § 331(i)(3)
21 U.S.C. § 331(k)
21 U.S.C. § 333
21 U.S.C. § 333(a)
21 U.S.C. § 333(e)
21 U.S.C. § 351
21 U.S.C. § 352
21 U.S.C. § 371
21 U.S.C. § 811(a)(1)
21 U.S.C. § 812
21 U.S.C. § 841
21 U.S.C. § 841(a)
21 U.S.C. § 841(a)(1)
21 U.S.C. § 841(b)
21 U.S.C. § 841(b)(1)
21 U.S.C. § 841(d)
21 U.S.C. § 841(b)(1)(B)
21 U.S.C. § 842
21 U.S.C. § 843
21 U.S.C. § 843(a)(9)
21 U.S.C. § 843(b)
21 U.S.C. § 844
21 U.S.C. § 844(a)
21 U.S.C. § 845
21 U.S.C. § 846
21 U.S.C. § 848
21 U.S.C. § 851
21 U.S.C. § 852
21 U.S.C. § 853
21 U.S.C. § 854
21 U.S.C. § 856
21 U.S.C. § 860
21 U.S.C. § 861(a)(1)
21 U.S.C. § 863
21 U.S.C. § 881
21 U.S.C. § 951
21 U.S.C. § 952
21 U.S.C. § 952(a)

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

21 U.S.C. § 952(b)
21 U.S.C. § 953
21 U.S.C. § 953(a)
21 U.S.C. § 954
21 U.S.C. § 955
21 U.S.C. § 959
21 U.S.C. § 960
21 U.S.C. § 960(a)
21 U.S.C. § 960(a)(1)
21 U.S.C. § 960(b)
21 U.S.C. § 960(b)(1)
21 U.S.C. § 960(b)(2)
21 U.S.C. § 960(b)(3)
21 U.S.C. § 960(b)(4)
21 U.S.C. § 960(B)(1)(G)
21 U.S.C. § 962
21 U.S.C. § 963

Title 22, U.S.C.
22 U.S.C. § 401
22 U.S.C. § 2778
22 U.S.C. § 2778(c)

Title 26, U.S.C.
26 U.S.C. § 5754
26 U.S.C. § 5861
26 U.S.C. § 5861(d)
26 U.S.C. § 5871
26 U.S.C. § 7201
26 U.S.C. § 7203
26 U.S.C. § 7206
26 U.S.C. § 7207

Title 27, U.S.C.
27 U.S.C. § 203

Title 31, U.S.C.
31 U.S.C. § 5311
31 U.S.C. § 5313
31 U.S.C. § 5314

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

31 U.S.C. § 5316
31 U.S.C. § 5316(a)
31 U.S.C. § 5317
31 U.S.C. § 5317(c)
31 U.S.C. § 5322
31 U.S.C. § 5322(a)
31 U.S.C. § 5322(b)
31 U.S.C. § 5324
31 U.S.C. § 5332
31 U.S.C. § 5363

Title 42, U.S.C.
42 U.S.C. § 1320(a)(7)(B)
42 U.S.C. § 2077
42 U.S.C. § 408
42 U.S.C. § 6928
42 U.S.C. § 7413(c)
42 U.S.C. § 7671

Title 46, U.S.C.
46 U.S.C. § 1903
46 U.S.C. § 1903(a)
46 U.S.C. § 1903(j)
46 U.S.C. § 70503
46 U.S.C. § 70506

Title 47, U.S.C.
47 U.S.C. § 223(a)(1)(E)
47 U.S.C. § 605

Title 49, U.S.C.
49 U.S.C. § 1472
49 U.S.C. § 1472(b)(1)(H)
49 U.S.C. § 46306(b)(7)
49 U.S.C. § 46314
49 U.S.C. § 46504
49 U.S.C. § 46505(b)(1)
49 U.S.C. § 80116(2)(A)
49 U.S.C. § 80302

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Title 50, U.S.C.
50 U.S.C. § 1701
50 U.S.C. § 1702
50 U.S.C. § 1703
50 U.S.C. § 1704
50 U.S.C. § 1705
50 U.S.C. § 192
50 U.S.C. § 2410
50 U.S.C. § 2410(g)
50 U.S.C. § 4305
50 U.S.C. § 4315

Immigration and Nationality Act (INA)
INA § 212(a)(1)(A)(i)
INA § 212(a)(1)(A)(ii)
INA § 212(a)(1)(A)(iv)
INA § 212(a)(2)(A)(ii)
INA § 212(a)(2)(A)(iii)
INA § 212(a)(2)(B)
INA § 212(a)(2)(C)
INA § 212(a)(2)(D)(i)
INA § 212(a)(2)(D)(ii)
INA § 212(a)(2)(D)(iii)
INA § 212(a)(3)(A)(ii)
INA § 212(a)(3)(A)(iii)
INA § 212(a)(3)(B)(ii)
INA § 212(a)(3)(B)(iii)
INA § 212(a)(3)(C)(i)
INA § 212(a)(4)(A)
INA § 212(a)(5)(A)(i)
INA § 212(a)(6)(A)(i)
INA § 212(a)(6)(B)
INA § 212(a)(6)(C)(i)
INA § 212(a)(6)(C)(ii)
INA § 212(a)(6)(D)
INA § 212(a)(6)(E)(i)
INA § 212(a)(6)(F)(i)
INA § 212(a)(6)(G)
INA § 212(a)(7)(A)(ii)
INA § 212(a)(7)(A)(iii)

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

INA § 212(a)(7)(B)(ii)
INA § 212(a)(7)(B)(iii)
INA § 212(a)(8)(A)
INA § 212(a)(9)(A)(i)
INA § 212(a)(9)(A)(ii)
INA § 212(a)(9)(B)(ii)
INA § 212(a)(9)(B)(iii)
INA § 212(a)(9)(C)(ii)
INA § 212(a)(9)(C)(iii)
INA § 212(a)(10)(D)
INA § 237(a)(1)(A)
INA § 237(a)(1)(B)
INA § 237(a)(1)(C)(i)
INA § 237(a)(1)(C)(ii)
INA § 237(a)(1)(D)(i)
INA § 237(a)(1)(E)(i)
INA § 237(a)(1)(G)(i)
INA § 237(a)(1)(G)(ii)
INA § 237(a)(2)(A)(i)
INA § 237(a)(2)(A)(ii)
INA § 237(a)(2)(A)(iii)
INA § 237(a)(2)(A)(iv)
INA § 237(a)(2)(B)(i)
INA § 237(a)(2)(B)(ii)
INA § 237(a)(2)(C)
INA § 237(a)(2)(D)(iii)
INA § 237(a)(2)(D)(iv)
INA § 237(a)(2)(E)(i)
INA § 237(a)(2)(E)(ii)
INA § 237(a)3(A)
INA § 237(a)(3)(B)(i)
INA § 237(a)(3)(B)(ii)
INA § 237(a)(3)(B)(iii)
INA § 237(a)(3)(C)(i)
INA § 237(a)(3)(D)
INA § 237(a)(4)(A)(i)
INA § 237(a)(4)(A)(ii)
INA § 237(a)(4)(B)
INA § 237(a)(5)
INA § 237 (a)(6)

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Title 15, C.F.R.
15 C.F.R. § 774.1

Title 22, C.F.R.
22 C.F.R. § 120
22 C.F.R. § 121
22 C.F.R. § 121.1
22 C.F.R. § 123.1
22 C.F.R. § 127.1
22 C.F.R. § 127.1(a)
22 C.F.R. § 127.1(a)(1)
22 C.F.R. § 127.1(a)(3)

Title 27, C.F.R.
27 C.F.R. § 179

Title 31, C.F.R.
31 C.F.R. § 1010.340
31 C.F.R. § 560
31 C.F.R. § 560.204

Title 41, C.F.R.
41 C.F.R. § 101

ICE HSI has the authority to collect or seize currency and assets on behalf of the Government of the United States. Currency and assets collected through ICE law enforcement efforts are remitted to the Treasury Forfeiture Fund. The funds remitted to Treasury are not used to fund ICE operations, unlike directly appropriated funds and mandatory fees.

The table below shows dollar value of Worksite Enforcement fines collected by ICE HSI since fiscal year (FY) 2010 that were added to the Treasury's General Fund:

ICE HSI Worksite Enforcement Fines Collected	
Fiscal Year	**Total Fines Collected**
2010	$5,848,523.86
2011	$8,364,090.19

2012	$8,677,976.72
2013	$10,741,640.57
2014	$10,556,492.93
2015	$11,462,437.13
2016 (partial)	$376,900.24
Total	$56,028,061.64

The table below shows the dollar value of currency and asset seizures (other than currency) collected by ICE since FY 2009:

ICE HSI Seizures by Fiscal Year, 2009 - 2015

Fiscal Year	Asset Seizures	Currency and Monetary Instruments
2009	$499,405,091	$361,226,150
2010	$728,779,344	$426,593,680
2011	$347,258,085	$562,504,680
2012	$398,468,280	$812,741,400
2013	$693,167,367	$1,310,717,638
2014	$668,433,297	$726,086,241
2015	$346,812,547	$442,375,769
TOTAL	$3,682,324,011	$4,642,245,558

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

The table below shows the dollar value forfeitures from ICE HSI-led investigations and turned over to Treasury since FY 2009.

ICE HSI Forfeitures by Fiscal Year, 2009 – 2015		
Fiscal Year	**Forfeiture Type**	**Financial Value Property**
2009	AF - Administratively Forfeited	$96,184,196
	JC - Judicial Civil	$23,169,423
	JR - Judicial Criminal	$46,239,699
	SF - Summary Forfeiture	$0
	TOTAL	**$165,593,318**
2010	AF - Administratively Forfeited	$71,514,044
	JC - Judicial Civil	$28,938,890
	JR - Judicial Criminal	$61,420,610
	SF - Summary Forfeiture	$0
	TOTAL	**$161,873,544**
2011	AF - Administratively Forfeited	$97,212,256
	JC - Judicial Civil	$25,563,075
	JR - Judicial Criminal	$27,363,012
	SF - Summary Forfeiture	$0
	TOTAL	**$150,138,343**
2012	AF - Administratively Forfeited	$122,522,643
	JC - Judicial Civil	$28,350,225
	JR - Judicial Criminal	$23,342,875
	SF - Summary Forfeiture	$0
	TOTAL	**$174,215,743**
2013	AF - Administratively Forfeited	$979,241,529
	JC - Judicial Civil	$51,913,817
	JR - Judicial Criminal	$22,654,140
	SF - Summary Forfeiture	$0
	TOTAL	**$1,053,809,486**
2014	AF - Administratively Forfeited	$118,994,904
	JC - Judicial Civil	$74,867,521
	JR - Judicial Criminal	$35,483,979
	SF - Summary Forfeiture	$53
	TOTAL	**$229,346,457**

Question#:	1
Topic:	ICE Functions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

2015	AF - Administratively Forfeited	$118,306,734
	JC - Judicial Civil	$21,605,221
	JR - Judicial Criminal	$20,525,854
	SF - Summary Forfeiture	$0
	TOTAL	**$160,437,809**
	Total Forfeitures	**$2,095,414,700**

Question#:	2
Topic:	ICE's expenditures
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Please provide the following information regarding ICE's expenditures:

The amount of funding ICE has spent on its non-detention and removal functions (both in raw dollars and as a percentage of the annual budget) from FY 2009 through FY 2015.

Response: Please see the table below for non-detention and removal operations appropriated funding, both in dollars and as a percentage of U.S. Immigration and Customs Enforcement's (ICE) appropriated budget.

Fiscal Year	Total ICE Appropriated Funding ($000s)	Non-Detention and Removal Operations Appropriated Funding ($000s)[1]	Non-Detention and Removal Operations Funding as % of ICE Budget
FY 2009	$4,989,210	$2,357,997	47.3%
FY 2010	$5,436,952	$2,691,772	49.5%
FY 2011	$5,500,620	$2,730,440	49.6%
FY 2012	$5,550,584	$2,610,677	47.0%
FY 2013	$5,146,632	$2,407,895	46.8%
FY 2014	$5,269,361	$2,459,001	46.7%
FY 2015	$5,958,756	$2,527,312	42.4%

Question: The specific statutory provision or provisions that authorize these non-detention and removal functions.

Response: Under the Homeland Security Act of 2002 and subsequent reorganizations under section 872, ICE was established as the investigative arm of the Department of Homeland Security (DHS) and has all of the investigative authorities previously held by the former U.S. Customs Service and Immigration and Naturalization Service. Under DHS Delegation Number 7030.1, the ICE Assistant Secretary was delegated the authority needed to enforce all combined statutory, administrative, and executive authorities.

In the Consolidated Appropriations Act, 2016 (Pub. L. No. 114-113), Congress appropriated $5,779,041,000 for the "necessary expenses for enforcement of immigration and customs laws, detention and removals, and investigations." ICE's statutory authority includes enforcement of a wide array of immigration and non-immigration

[1] The dollar amount excludes those related to the administrative detention and removal of aliens.

Question#:	2
Topic:	ICE's expenditures
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

laws. Excluding those related to the administrative detention and removal of aliens, ICE may utilize over 400 federal statutes and regulations to investigate immigration and customs violations. Please see the response to question 1 for a list of statues and regulations which represents the diversity of statutes that are under ICE HSI's investigative authority as a criminal investigative agency.

Question: The amount of funding that was specifically allocated by Congress for ICE's detention and removal budget that is not being used for detention and removal operations.

Response: ICE uses the funds appropriated for detention and removal operations on detention and removal operations only, unless a Departmental reprogramming request is approved by Congress.

Question: The specific statutory provision or provisions that authorize the diversion of detention and removal funding to non-detention or non-removal activities.

Response: Pursuant to Section 503 of the Department of Homeland Security Appropriations Act, 2015 (Pub. L. No. 114-4), as extended in the Continuing Appropriations Act, 2016, (Pub. L. No. 114-53), Congress authorizes ICE to reprogram or transfer appropriations made under that Act, subject to the restrictions, limits, and notice requirements specified therein.

Question: Does either DHS or ICE have transfer authority that allows the transfer of funding that was allocated by Congress for ICE's detention and removal purposes to other accounts or for other purposes?

Response: Consistent with the previous response, pursuant to Section 503 of the Department of Homeland Security Appropriations Act, 2015 (Pub. L. No. 114-4), as extended in the Continuing Appropriations Act, 2016, (Pub. L. No. 114-53), Congress authorizes ICE to reprogram or transfer appropriations made under that Act, subject to the restrictions, limits, and notice requirements specified therein.

Question#:	3
Topic:	Best estimate
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Please provide your best estimate regarding the following:

The number of ICE personnel who are dedicated solely to detention and removal functions.

The number of ICE personnel who are dedicated solely to non-detention and removal functions.

The number of ICE personnel who have both detention and removal and non- detention and removal functions.

The amount of work hours ICE personnel dedicate to detention and removal functions (expressed in both raw hours and as a percentage of some set work period).

The amount of work hours ICE personnel dedicate to non-detention and removal functions (expressed in both raw hours and as a percentage of some set work period).

Response: U.S. Immigration and Customs Enforcement (ICE) has over 19,000 employees, of which approximately 5,500 are Deportation Officers and supervisory and managerial law enforcement personnel in Enforcement and Removal Operations. These officers are responsible for the identification, arrest, detention, and removal of aliens in addition to associated case management responsibilities.

With regard to the question about the amount of work hours ICE personnel dedicate to detention and removal functions and non-detention and removal functions, ICE does not track the data as requested and cannot make presumptions or estimates based on available case management data.

ICE is developing a workload staffing model that will, in the future, be able to attribute the number of approximate hours front line personnel spend on mission duties versus administrative duties. The model is expected to be rolled out by the end of fiscal year 2016.

Question#:	4
Topic:	Charter Flights
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: ICE-Funded Charter Flights for Unaccompanied Alien Children

Earlier this year, it was learned, in the course of an investigation of the Department of Health and Human Services' (HHS) handling of the unaccompanied alien children (UAC) influx at the U.S.-Mexico border over the last few years, that ICE was chartering flights to transport UAC from the U.S.-Mexico border to points within the interior of the United States. An internal HHS slideshow that was released to the public clearly stated that the multi-agency effort aimed at handling the UAC situation included "[u]se of ICE charter flights to transport larger numbers of UAC to [HHS Office of Refugee Resettlement, or ORR] facilities." Please provide the following information regarding ICE's involvement in the chartering of flights for UAC:

The total amount of funding that ICE has spent on charter flights for UACs from FY 2009 through FY 2015, and the ICE account from which that funding was drawn.

Response: From June 8, 2014 to September 30, 2015, U.S. Immigration and Customs Enforcement (ICE) has spent approximately $4.8 million on charter flights for unaccompanied children.[2] ICE is unable to track costs associated with chartered movements prior to June 8, 2014 (Fiscal Year (FY) 2014), when ICE began collecting data on unaccompanied children movements as it relates to the Rio Grande Valley (RGV) surge.

Question: The total amount of funding that ICE has spent on commercial flights for UACs from FY 2009 through FY 2015, and the ICE account from which that funding was drawn.

Response: From March 2009 to September 30, 2015, ICE has spent approximately $13.7 million on commercial flights for unaccompanied children utilizing funds appropriated to ICE.[3]

Question: The total number of UAC who have been transported by charter flights from FY 2009 through FY 2015.

[2] This estimated associated cost for moving unaccompanied children by charter flight are exclusive of other direct costs, including, but not limited to salaries and medical expenses.

[3] This estimated associated cost for moving unaccompanied children by commercial flight are exclusive of other direct costs, including, but not limited to salaries and medical expenses.

Question#:	4
Topic:	Charter Flights
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Response: From June 8, 2014 to September 30, 2014, ICE transported about 7,800 unaccompanied children by chartered flights. During FY 2015, ICE transported about 2,400 unaccompanied children by chartered flights through September 30, 2015. ICE is unable to statistically report on chartered movements prior to June 8, 2014 (FY 2014), when ICE began collecting data on unaccompanied children movements as it related to the RGV surge.

Question: The total number of UAC who have been transported by commercial flights from FY 2009 through FY 2015.

Response: ICE is unable to provide specific data regarding the number of unaccompanied children transported via commercial flight for this time period, as our systems do not track these specific data points. However, ICE is in the process of expanding its use of contractor-conducted escorts in FY 2016 and will be able to provide more reliable data going forward.

Question: The total list of destination cities and counties to which UAC have been transported by charter flights from FY 2009 through FY 2015.

Response: The list of destination cities to which unaccompanied children have been transported by charter flights from June 8, 2014 to September 30, 2014 of FY 2014 and FY 2015 through September 30, 2015, for the purpose of placement with the Office of Refugee and Resettlement (ORR), is as follows: Baltimore, MD; Seattle, WA; Brownsville, TX; El Paso, TX; Newark, NJ; Gary, IN; Houston, TX; Mesa, AZ; Lawton, OK; Harrisburg, PA; Miami, FL; Oxnard, CA; Oakland, CA; Richmond, VA; San Diego, CA; San Antonio, TX; St. Louis, MO; Tucson, AZ; Chicago, IL. (Note, however, that the final destination listed by ICE Air Operations may not be the final destination city for the UAC, as upon arrival, the local ERO Field Office may have continued the transfer of the UAC via ground transportation or commercial airline to an ORR facility.)

ICE is unable to statistically report on destination cities and counties to which unaccompanied children have been transported by chartered flights prior to 2014.

Question: The total list of destination cities and counties to which UAC have been transported by commercial flights from FY 2009 through FY 2015.

Response: ICE is unable to provide specific data regarding the number of unaccompanied children transported via commercial flight for this time period as our systems do not track these specific data points.

Question#:	4
Topic:	Charter Flights
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Please provide the names of all charter flight companies that were used by ICE to transport UAC from FY 2009 through FY 2015.

Response: ICE is able to provide a list of charter flight companies used from FY 2010 to the present. ICE has a contract with CSI Aviation for all charter aircraft, and CSI utilizes multiple sub-contractors to accomplish these movements, including Swift Air, Falcon, Vision, World Atlantic, Sun Country, Xtra Airlines, Orange Air, Ameristar, and Capital Airways. ICE did not use charter flight companies prior to the reported period.

Question: The UAC that were apprehended by ICE were apprehended at or near the U.S.-Mexico border. The use of charter flights shows an intent to transport these UAC to distant points from the U.S.-Mexico border. Did you sign off on this policy, which transported illegally present individuals, who were detained along the U.S.-Mexico border, to points in the interior of the United States? If the answer is yes, please indicate the date you signed off on this policy.

Response: There is no such policy. U.S. Customs and Border Protection apprehends the vast majority of unaccompanied children, whereas pursuant to the William Wilberforce Trafficking Victims Protection Reauthorization Act (TVPRA), ICE is responsible for transporting unaccompanied children to ORR. Since the TVPRA was passed by Congress in 2008, ICE has used commercial air and ICE charter flights to transport unaccompanied children to ORR shelters located throughout the United States as required by law.

Question: What is ICE's plan for re-detaining the UAC who are in the interior of the United States and returning them to their countries of origin?

Response: ICE conducts enforcement actions, including those involving unaccompanied children, consistent with the priorities identified in Secretary Johnson’s November 20, 2014 memorandum.

Question: What number of UAC who have been transported by ICE to points in the interior of the United States have also been returned to their countries of origin?

Response: ICE does not track unaccompanied children removals in the requested manner. However, please see below for a list of unaccompanied children removed by nationality from FY 2009 to FY 2015.

Question#:	4
Topic:	Charter Flights
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Country of Citizenship	FY09	FY10	FY11	FY12	FY13	FY14	FY15
BAHAMAS	-	1	-	-	-	1	1
BARBADOS	-	1	-	-	-	-	-
BELIZE	-	-	-	1	-	-	1
BERMUDA	-	-	-	-	2	-	-
BOLIVIA	-	-	1	-	-	-	-
BRAZIL	6	4	7	6	5	3	7
CANADA	-	1	3	1	-	-	1
CAYMAN ISLANDS	-	-	1	-	-	-	-
CHILE	1	-	-	-	-	-	-
CHINA, PEOPLES REPUBLIC OF	1	1	-	-	1	1	3
COLOMBIA	-	3	2	3	-	-	3
COSTA RICA	2	1	-	-	-	1	-
DOMINICA	-	1	-	-	-	-	-
DOMINICAN REPUBLIC	-	-	1	4	3	2	4
ECUADOR	11	7	15	11	11	16	12
EL SALVADOR	96	117	136	136	159	190	178
FINLAND	1	-	-	-	-	-	-
GERMANY	2	1	3	-	-	-	-
GUATEMALA	534	520	515	626	661	686	544
GUINEA	-	1	-	-	-	-	-
HAITI	-	-	-	1	1	-	1
HONDURAS	352	326	297	430	461	503	419
INDIA	-	2	1	-	-	-	1
ISRAEL	-	-	-	-	1	-	-
JAMAICA	-	-	1	1	-	-	-
KENYA	-	-	-	2	1	-	-
KOREA	-	-	1	-	-	-	-
LATVIA	-	-	-	-	-	1	-
MACEDONIA	-	1	-	-	-	-	-
MEXICO	350	690	696	574	548	484	879
MICRONESIA, FEDERATED STATES OF	-	-	-	-	-	1	-
MONGOLIA	1	-	-	-	-	-	-
NICARAGUA	3	6	5	6	3	4	5
PAKISTAN	-	-	-	-	-	1	-
PANAMA	-	-	2	-	-	-	-
PERU	1	2	1	2	2	3	2
PORTUGAL	-	-	-	-	-	1	-
ROMANIA	-	-	-	-	6	1	3
RUSSIA	-	-	3	-	-	-	-
SAUDI ARABIA	-	1	-	-	-	-	-
SIERRA LEONE	-	-	1	-	-	-	-
SOUTH AFRICA	-	-	-	-	-	1	-
SPAIN	-	-	-	2	-	1	-
SRI LANKA	-	-	-	2	-	-	-
ST. KITTS-NEVIS	-	-	-	-	1	-	-
THAILAND	-	1	-	-	-	-	-
TRINIDAD AND TOBAGO	-	-	1	-	-	-	-
UNITED KINGDOM	-	2	-	1	1	-	1
VENEZUELA	-	-	2	-	1	-	-
Total	**1,361**	**1,690**	**1,695**	**1,809**	**1,868**	**1,901**	**2,065**

Question#:	4
Topic:	Charter Flights
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Country of Citizenship	FY09	FY10	FY11	FY12	FY13	FY14	FY15
BAHAMAS	-	1	-	-	-	1	1
BARBADOS	-	1	-	-	-	-	-
BELIZE	-	-	-	1	-	-	1
BERMUDA	-	-	-	-	2	-	-
BOLIVIA	-	-	1	-	-	-	-
BRAZIL	6	4	7	6	5	3	7
CANADA	-	1	3	1	-	-	1
CAYMAN ISLANDS	-	-	1	-	-	-	-
CHILE	1	-	-	-	-	-	-
CHINA, PEOPLES REPUBLIC OF	1	1	-	-	1	1	3
COLOMBIA	-	3	2	3	-	-	3
COSTA RICA	2	1	-	-	-	1	-
DOMINICA	-	1	-	-	-	-	-
DOMINICAN REPUBLIC	-	-	1	4	3	2	4
ECUADOR	11	7	15	11	11	16	12
EL SALVADOR	96	117	136	136	159	190	178
FINLAND	1	-	-	-	-	-	-
GERMANY	2	1	3	-	-	-	-
GUATEMALA	534	520	515	626	661	686	544
GUINEA	-	1	-	-	-	-	-
HAITI	-	-	-	1	1	-	1
HONDURAS	352	326	297	430	461	503	419
INDIA	-	2	1	-	-	-	1
ISRAEL	-	-	-	-	1	-	-
JAMAICA	-	-	1	1	-	-	-
KENYA	-	-	-	2	1	-	-
KOREA	-	-	1	-	-	-	-
LATVIA	-	-	-	-	-	1	-
MACEDONIA	-	1	-	-	-	-	-
MEXICO	350	690	696	574	548	484	879
MICRONESIA, FEDERATED STATES OF	-	-	-	-	-	1	-
MONGOLIA	1	-	-	-	-	-	-
NICARAGUA	3	6	5	6	3	4	5
PAKISTAN	-	-	-	-	-	1	-
PANAMA	-	-	2	-	-	-	-
PERU	1	2	1	2	2	3	2
PORTUGAL	-	-	-	-	-	1	-
ROMANIA	-	-	-	-	6	1	3
RUSSIA	-	-	3	-	-	-	-
SAUDI ARABIA	-	1	-	-	-	-	-
SIERRA LEONE	-	-	1	-	-	-	-
SOUTH AFRICA	-	-	-	-	-	1	-
SPAIN	-	-	-	2	-	1	-
SRI LANKA	-	-	-	2	-	-	-
ST. KITTS-NEVIS	-	-	-	-	1	-	-
THAILAND	-	1	-	-	-	-	-
TRINIDAD AND TOBAGO	-	-	1	-	-	-	-
UNITED KINGDOM	-	2	-	1	1	-	1
VENEZUELA	-	-	2	-	1	-	-
Total	**1,361**	**1,690**	**1,695**	**1,809**	**1,868**	**1,901**	**2,065**

Question#:	5
Topic:	Removal of Illegal Aliens to their Home Countries
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Zadvydas and the Removal of Illegal Aliens to their Home Countries

During your hearing testimony, you claimed that ICE lacked control over a sizeable segment of the population of illegal aliens with criminal convictions in the United States. Specifically, you stated that, in the wake of the Supreme Court's decision in Zadvydas v. Davis, ICE lacks the ability to detain illegal aliens with criminal convictions beyond the 180-day time limit created by the Court.

While Zadvydas addresses the domestic detention of illegal aliens, 8 U.S.C. § 1253(d) actually requires mandatory suspension of visa issuance for both immigrants and nonimmigrants in countries whose governments refuse to accept the return of their own foreign nationals upon being ordered deported from the United States.

1. Is DHS currently enforcing 8 U.S.C. § 1253(d)?

a. If the answer to Question (1) is no, please provide the following:

i. Whether DHS leadership is aware that the Federal Government is required to suspend (in other words, lacks the discretion to not suspend) visa issuance for foreign nationals of countries that refuse to accept return of their foreign nationals.

ii. If DHS leadership is aware of this authority, a detailed explanation as to why 8 U.S.C. § 1253(d) is not being enforced.

iii. Is there a specific federal procedure for a situation where a foreign government rejects receipt of one of its own foreign nationals, when that foreign national is illegally present in the United States and has been ordered removed from the United States pursuant to a final order of removal?

iv. If there is a specific procedure for the above situation, what role (if any) does ICE play in this procedure?

b. If the answer to Question (1) is yes, please provide the following:

i. Any information available to you regarding DHS's efforts to enforce 8 U.S.C. § 1253(d).

ii. Details regarding the impact of use of 8 U.S.C. § 1253(d) in achieving the return of illegal aliens to their countries of origin.

iii. Any statutory adjustments Congress can make to improve 8 U.S.C. § 1253(d).

Response:

1. Is DHS currently enforcing 8 U.S.C. § 1253(d)?

The Department of Homeland Security (DHS) as a whole, as well as U.S. Immigration and Customs Enforcement (ICE) specifically, take very seriously the issue of removing foreign nationals in a timely and efficient manner, and the consequences associated with limitations on the ability to do so.

The Department of State (DOS) and ICE work together to improve cooperation with countries that systematically refuse or delay the repatriation of their nationals. Section 243 (d) of the INA grants authority to the Secretary of State to order consular officers to discontinue granting visas upon notification from the Secretary of Homeland Security that a foreign government is uncooperative in accepting its nationals.[4] After such notification from DHS, DOS invoked INA Section 243(d) against the Government of Guyana between September 7, 2001 and December 14, 2001, which lead Guyana to issues travel documents to Guyanese aliens with final orders of removal.

ICE's commitment to efficient removals is reflected in an April 2011 memorandum of understanding (MOU) with the DOS Bureau of Consular Affairs that outlines the tools DOS and ICE will pursue to gain compliance by foreign governments. Please find a copy of the MOU furnished with this response.

The MOU, among other things, establishes a target average travel document issuance time of 30 days and outlines measures to address those countries that systemically refuse or delay repatriation of their nationals. ICE has participated in the issuance of demarches but does not possess authority to withhold foreign aid, issue visa sanctions, or make sensitive foreign policy decisions. Other processes exist under federal law that could be potentially be useful, in appropriate circumstances, and taking into account foreign policy considerations, , including nonimmigrant discretionary waivers pursuant to INA Sections 212(d)(3) and (4)(4)(A); the suspension of expedited nonimmigrant visa referrals for priority cases, pursuant to 9 F.A.M. Section 601.8; the period of validity for visas

[4] The Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), created the Department of Homeland Security and assigned or transferred many of the functions previously exercised by the Attorney General to the Secretary of Homeland Security.

Question#:	5
Topic:	Removal of Illegal Aliens to their Home Countries
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

pursuant to INA Section 221(c); removal from the designated list of temporary-and-seasonal-worker H-2 eligible countries, pursuant to 8 C.F.R. § 214.2(h)(5)(i)(F) and 8 C.F.R. § 214.2(h)(6)(i)(E); and removal of countries designated for participation in the visa waiver program, pursuant to INA Section 217(c)(5)(A).

a. If the answer to Question (1) is no, please provide the following:

i. Whether DHS leadership is aware that the Federal Government is required to suspend (in other words, lacks the discretion to not suspend) visa issuance for foreign nationals of countries that refuse to accept return of their foreign nationals.

Response: See response above.

ii. If DHS leadership is aware of this authority, a detailed explanation as to why 8 U.S.C. § 1253(d) is not being enforced.

Response: See response above.

iii. Is there a specific federal procedure for a situation where a foreign government rejects receipt of one of its own foreign nationals, when that foreign national is illegally present in the United States and has been ordered removed from the United States pursuant to a final order of removal?

Response: See response above.

iv. If there is a specific procedure for the above situation, what role (if any) does ICE play in this procedure?

Response: DHS and DOS work together to incentivize other countries to accept the removal of their nationals from the United States utilizing the steps outlined in the April 2011 MOU between DHS and DOS.

b. If the answer to Question (1) is yes, please provide the following:

i. Any information available to you regarding DHS's efforts to enforce 8 U.S.C. § 1253(d).

Response: See response above.

Question#:	5
Topic:	Removal of Illegal Aliens to their Home Countries
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

ii. Details regarding the impact of use of 8 U.S.C. § 1253(d) in achieving the return of illegal aliens to their countries of origin.

Response: See response above.

iii. Any statutory adjustments Congress can make to improve 8 U.S.C. § 1253(d).

Response: DHS stands ready to assist in providing technical assistance on any measures that Congress might propose to address the issue of uncooperative countries.

Question#:	6
Topic:	Final order of removal in the United States.
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Please provide a list of all countries that have refused - for any reason, for any duration, and at any point since January 20, 2009 - to accept the return of their own foreign nationals upon the issuance of a final order of removal in the United States.

Response: Please note that there are a wide range of reasons for which countries refuse or delay acceptance of their nationals, from a lack of formal relations with the U.S. Government or lack of a recognized government, to lengthy background investigations and strict evidentiary requirements to prove identity and nationality. A list of this nature could potentially include all countries and would not be reflective of those that systematically refuse or delay cooperation.

U.S. Immigration and Customs Enforcement provides the following list of countries it currently considers to be systematically uncooperative with regard to the repatriation of their nationals.

1. Afghanistan
2. Algeria
3. Burundi
4. Cape Verde
5. China, Peoples Republic of
6. Cuba
7. Eritrea
8. Gambia
9. Ghana
10. Guinea
11. India
12. Iran
13. Iraq
14. Ivory Coast
15. Liberia
16. Libya
17. Mali
18. Mauritania
19. Morocco
20. Sierra Leone
21. Somalia

Question#:	6
Topic:	Final order of removal in the United States.
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

22. South Sudan
23. Zimbabwe

Question#:	7
Topic:	Zadvydas 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: It is arguable that Zadvydas, in addition to being wrongly decided by the Court, interferes with the clear and unequivocal national security functions of the executive branch. Would you agree with the statement that ICE - if it were equipped with the knowledge that an illegal alien in its custody represented a national security threat - was, despite the Zadvydas decision, under no obligation to release that alien after 180 days if the agency were unable to secure that alien's return to his home country? If you disagree with the above statement, please provide a detailed explanation as to why.

Response: The majority opinion in *Zadvydas v. Davis*, 533 U.S. 678 (2001), left open the possibility that continued post-order detention might be appropriate for certain aliens if strong procedural protections were in place. *See id.* at 691-92. After *Zadvydas,* U.S. Immigration and Customs Enforcement promulgated regulations which allow ICE to maintain post-order detention beyond 180 days in limited circumstances. *See* 8 C.F.R. § 241.14. This regulation authorizes continued detention for the following categories of aliens: aliens who have a highly contagious disease that poses a threat to public safety; aliens whose release would trigger serious adverse foreign policy consequences; aliens whose release would pose security or terrorism concerns; and aliens determined to be especially dangerous. Each of these provisions has its own stringent certification procedure that must be completed in order for continued detention to be authorized.

Question#:	8
Topic:	Zadvydas 2
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: As you noted, many of the illegal aliens that ICE releases from custody are individuals whose home countries refuse to accept their return. It appears, however, that ICE, in determining the 180-day period that was arbitrarily set by *Zadvydas*, does not exclude days during which an illegal alien's home country refuses to accept their return. Please provide a detailed explanation as to why ICE does not exclude days during which a foreign government refuses to accept the return of its own national from the 180-day period.

Answer: In *Zadvydas v. Davis*, 533 U.S. 678 (2001), the U.S. Supreme Court held that 8 U.S.C. § 1231(a)(6) authorizes immigration detention, after entry of an administrative final order of removal, for a period reasonably necessary to accomplish the alien’s removal from the United States. The Court recognized 6 months as a presumptively reasonable period of time to allow the government to accomplish an alien’s removal after the removal period has commenced. The Court’s holding did not exempt from that period of time days during which a foreign government refuses to accept the return of its own national.

An alien ordered removed from the United States may have fulfilled his statutory obligation to make a good faith effort to secure travel documents and not have hampered his removal in any way, however, the country of repatriation may still refuse to accept its national’s return. The alien cannot be detained solely because his or her country refuses to issue, or delays the issuance of, a travel document.

If the government can demonstrate that removal is significantly likely in the reasonably foreseeable future, the alien may be held for longer than 6 months. The Court opined that Congress failed to explicitly authorize long-term detention of “unremovable” aliens and that the statute did not confer indefinite discretionary detention authority. The Court found that had Congress intended to allow indefinite detention, it could have made that intent more clear.

Question#:	9
Topic:	Illegal Aliens in the United States 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Estimates of the Illegal Alien Population in the United States

During your hearing testimony, you indicated that there were multiple estimates available regarding the possible number of illegal aliens in the United States. Specifically, you stated that, "depending on which estimate" one believed, there were either approximately 12 million or approximately 15 million illegal aliens in the United States.

Has DHS, or any component of DHS, including ICE, ever produced any internal estimates regarding the number or potential number of illegal aliens in the United States? If the answer is yes, please provide these estimates. If one or more of these estimates is part of one or more internal documents, please provide an unredacted version of the documents.

Response: In 2014, the DHS Office of Immigration Statistics produced a report which estimated the unauthorized immigrant population in the United States in January 2012 to have been 11.4 million. Attached, please find that report.

Question#:	10
Topic:	Illegal Aliens in the United States 2
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Has DHS, or any component of DHS, including ICE, ever produced any internal estimates regarding the costs or potential costs of the presence of illegal aliens in the United States? If the answer is yes, please provide these estimates. If one or more of these estimates is part of one or more internal documents, please provide an unredacted version of the documents.

Response: U.S. Immigration and Customs Enforcement has not produced internal estimates regarding the costs or potential costs of the presence of unauthorized immigrants in the United States.

Question#:	11
Topic:	Illegal Aliens in the United States 3
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: While serving at ICE, have you ever seen any information, whether internally or externally produced, directly or indirectly discussing the number or potential number of illegal aliens in the United States? If the answer is yes, please provide the information. If this information is part of one or more internal documents, please provide an unredacted version of the documents.

Response: In 2014, the DHS Office of Immigration Statistics produced a report which estimated the unauthorized immigrant population in the United States in January 2012 to have been 11.4 million. Attached please find the latest report.

Question#:	12
Topic:	Leadership
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Failure of Administration Leadership to Support ICE Employees

During your hearing testimony, you pushed back against the notion that ICE was not fulfilling its detention and removal obligations. Specifically, you rejected the idea that the "women and men of ICE ... would turn their backs on the deportation of a criminal alien who needed to be removed."

While no one here in the United States Senate questions the dedication of the women and men who fulfill ICE's array of dangerous law enforcement duties, it is clear that ICE leadership lacks the same commitment to the agency's mission. In addition to the Administration's array of amnesty memoranda, which dramatically curtail the ability of ICE agents to enforce existing statutory law, there are reported examples of situations where ICE agents have had criminal aliens that they have detained released upon instructions from ICE leadership.

The above concerns are also in addition to President Obama's overt threat earlier this year to ICE agents who were enforcing immigration law, in defiance of the Administration's preference that they not do so. On February 25, 2015, President Obama stated during a televised MSNBC/Telemundo town hall discussion that ICE employees who did not disobey their statutory obligations to enforce federal immigration law and follow the President's amnesty instructions would face "consequences."

Please explain what President Obama meant by his February statement that there would be "consequences" for ICE employees who followed current federal immigration law.

Has President Obama given you or any other senior officials within ICE any specific instructions or directives regarding what sort of consequences should occur for ICE employees who continue to follow current federal immigration law?

Have any disciplinary measures been instituted against any ICE employees since President Obama's comments for employees who detained illegal aliens or otherwise commenced removal proceedings for illegal aliens?

Response: The Department of Homeland Security’s (DHS) policies regarding the apprehension, detention, and removal of aliens do not require DHS employees to act in an unlawful manner. To ensure this, prior to implementation of these memoranda, DHS and the Department of Justice engaged in a comprehensive legal review to ensure their compliance and consistency with all applicable laws. As a result, the memoranda provide

Question#:	12
Topic:	Leadership
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

U.S. Immigration and Customs Enforcement (ICE) with clearer guidance regarding how best to leverage resources to enforce the nation’s immigration laws, while simultaneously working to strengthen public confidence in our immigration enforcement efforts. ICE is implementing these prosecutorial discretion policies to ensure appropriate resources are dedicated to the identification, apprehension, and removal of removable aliens who pose a danger to national security, border security, or a risk to public safety. In exercising this discretion with respect to use of resources, ICE expects employees to follow the lawful orders of supervisors that are consistent with the memoranda.

The policies and direction provided by Secretary Johnson in his November 20, 2014 memorandum, *Policies for the Apprehension, Detention and Removal of Undocumented Immigrants*, permit DHS personnel to exercise discretion when reviewing the circumstances of an individual case. They do not mandate enforcement action for every case falling within a priority or preclude enforcement action for those falling outside the priorities. For example, the removal of an individual may be prioritized, even if he or she does not fit squarely in an enumerated priority, if in the judgment of a field responsible official, removal would serve an important federal interest. Each case is reviewed based on the facts and circumstances known at the time of apprehension and book-in. In making such judgments, ICE personnel have been instructed to consider factors such as: extenuating circumstances involving the offense of conviction; extended length of time since the offense of conviction; length of time in the United States; military service; family or community ties in the United States; status as a victim, witness, or plaintiff in civil or criminal proceedings; or compelling humanitarian factors such as poor health, age, pregnancy, or a young child or seriously ill relative. These factors are not intended to be dispositive nor is this list intended to be exhaustive. Decisions should be based on the totality of the circumstances.

While ICE may exercise prosecutorial discretion at any stage of an enforcement proceeding, it is generally preferable to exercise such discretion as early in the case or proceeding as possible in order to preserve government resources that would otherwise be expended in pursuing enforcement and removal of higher priority cases. Thus, ICE personnel are expected to exercise discretion and pursue these priorities at all stages of the enforcement process—from the earliest investigative stage to enforcing final orders of removal—subject to their chains of command and to the particular responsibilities and authorities applicable to their specific position.

However, ICE is also committed to implementing safeguards to ensure that releases are executed in a way that promotes public safety and border security, and protects our communities. Thus, in March 2015, ICE instituted additional safeguards, including enhanced supervisory approval for discretionary releases of certain categories of

Question#:	12
Topic:	Leadership
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

individuals with criminal convictions, and the creation of a panel of senior managers to review such discretionary release decisions for individuals convicted of crimes of violence, to ensure compliance with supervisory approval requirements and identify any inconsistencies in release determinations. ICE is also committed to ensuring detention capacity is not used as a determinative factor in the release of an individual with a serious criminal record. ICE will continue to manage its nationwide detention system to ensure that field offices have access to sufficient adult detention space to detain individuals posing a public safety threat until removal, including reprioritizing resources, if necessary, to ensure the promotion of public safety.

As is the case with all federal employees, DHS personnel are required to adhere to Department policies that govern them. Failure to adhere to Department policy may lead to a range of repercussions depending on the facts and circumstances of the particular case. There have been no disciplinary actions initiated against any ICE employee as a result of a failure to adhere to the executive actions taken by Secretary Johnson on November 20, 2014 or President Obama’s statement.

Question#:	13
Topic:	1811 Status
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Some critics of ICE's current dysfunction have pointed to the fact many (if not most) ICE agents are not classified as federal criminal investigators, which would allow them to be hired as part of the GS-1811 job series. They have noted that according "1811 status" to ICE agents would permit them greater law enforcement autonomy and effectiveness.

Has the Obama Administration at any point considered conferring 1811 status on ICE agents who handle detention and removal functions, in order to improve immigration enforcement?

If the Administration has not considered this change, as the director of ICE, would you be in favor of making this change?

Response: U.S. Immigration and Customs Enforcement (ICE), like other federal agencies, utilizes many different job series. Position classification in a particular series is specifically defined by the duties and responsibilities of the position. Job series classification standards are developed under the authority of the Office of Personnel Management (OPM).

The responsibilities of the Criminal Investigator (1811-series) at ICE include conducting investigations of terrorist organizations, criminal organizations, and criminal violations of the immigration and customs laws, as defined in Titles 8, 18, 19, and 31 of the United States Code. The responsibilities of the Deportation Officer (1801-series) focus its specialized law enforcement duties on enforcing the criminal and civil immigration and nationality laws, such as identifying, locating, and arresting aliens, either in custodial settings or at-large, who are subject to exclusion, deportation, or removal from the United States.

In fiscal year (FY) 2014, ICE formed a working group consisting of senior-level Enforcement and Removal Operations (ERO) managers from eight office locations around the country to study the feasibility of combining two 1801-series occupations: the Immigration Enforcement Agent (IEA) and Deportation Officer (DO) positions. In FY 2015, ICE undertook an exhaustive classification review of the IEA and DO positions. Based on this review, ICE updated the IEA and DO position descriptions for the employees executing detention and removal functions and created a single DO career track. ICE considered other 1800 series law enforcement positions but determined that the current 1801 job series most presently fit the duties of the ERO law enforcement position. This transition to a single career track provides the DO occupation with

Question#:	13
Topic:	1811 Status
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

enhanced responsibilities for performing more complex work related to the enforcement of federal criminal and civil laws, to include conducting investigations, executing arrests, preparing cases for prosecution, detention responsibilities, and working with other federal, state, and local law enforcement agencies. This provides opportunities for promotional growth to the GS-12 performance level, and it provides additional flexibility to leadership to better manage a complex workforce.

Each law enforcement position at ICE plays a crucial role in carrying out the ICE mission. Changing all GS-1801 Deportation Officers to GS-1811 Criminal Investigators would not be in line with the important duties and responsibilities of the GS-1801 Deportation Officer position, and it would be contrary to established OPM rules and regulations.

Question#:	14
Topic:	Morale
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: In addition, ICE received a very low employee satisfaction score in the 2015 Best Places to Work in the Federal Government rankings. According to the rankings, ICE ranked an abysmal 318th out of 320 agency subcomponents.

Have you, Secretary Johnson, and the other subcomponent heads considered the possibility that low morale among ICE employees is directly attributable to you preventing them from fulfilling their statutorily duties?

Have you received any complaints from ICE employees that may offer insight into why morale among ICE employees is so low? If the answer is yes, please provide some or all of these complaints for review by Committee staff.

Why do you believe that morale among ICE employees is low?

Response: U.S. Immigration and Customs Enforcement (ICE) studied the reasons for declining morale and has taken steps to reverse the trend. After the census survey of all employees in 2012, ICE undertook a statistical analysis of the results to discover drivers for each of its large organizations. ICE then used those drivers to undertake structured focus groups with 400 employees in these organizations. An overview of the results is presented below.

ICE prioritized three cross-cutting issues and began corrective actions in Fiscal Year (FY) 2013:

1. Setting a clear, unified, and compelling mission;
2. Strengthening employee safety programs; and
3. Strengthening awards.

For FY 2016, ICE released an updated long-term strategic plan together with a revised mission statement.

Additional actions are underway to help employees see how they deliver on the mission:

- ICE Homeland Security Investigations (HSI) narrowed its focus to help employees target the areas that present the highest threat to national security and public safety within the scope of ICE’s mission to battle transnational crime; and

Question#:	14
Topic:	Morale
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

ICE Homeland Security Investigations Domestic Field Focus Group Recommendations

- ICE Enforcement and Removal Operations (ERO) refreshed its positions to ensure they reflect their work to take the most dangerous illegal immigrants off the streets, and then refreshed individual performance goals for the 2016 cycle to reflect this clarified role.

In 2014, ICE launched a unified intranet portal housing all its safety programs. ICE developed and marketed this site with its largest Union, Council 118. ICE also revised its annual performance-based awards programs to ensure all awards tied directly to performance ratings and were standardized across the agency.

ICE is confident these actions have launched the process of reversing declining morale and eagerly awaits the results of OPM's 2016 survey.

ICE Enforcement and Removal Operations Domestic Field Focus Group Recommendations

Ran k	Theme	Recommendation
1	Commitment to Mission	• ERO lacks a well-defined culture or clear identity • ERO's mission and policies/procedures are poorly communicated by leadership and often times not understood by the workforce
2	Communication and Collaboration	• Lack of clear and direct communication from leadership often leads to directives and guidance that are ambiguous, untimely, inconsistent, and contradictory
3	Learning and Development	• Job-specific training for employees and supervisors does not exist or is very limited • Overall, there is a lack of relevant training opportunities for employees and supervisors • Career mobility and development opportunities do not exist for agents and non-agents; there are no defined career tracks
4	Performance Management	• The performance management system at ERO is ineffective and outdated and inhibits employee development • The rewards and recognition process is inconsistent and poorly defined; employees believe the process is subjective and unfair
5	Workplace Safety/ Policy and Procedures	• Workplace safety programs do not exist nor do standard safety policies and procedures • Standardized processes to deal with employees who get physically injured are not in place at ERO

Question#:	14
Topic:	Morale
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Rank	Theme	Recommendation
1	Communication and Collaboration	Develop and launch an internal formal, proactive, and direct communications plan outlining HSI mission, goals, policies, and procedures: • Consolidate emails sent from headquarters to minimize communications and information overload to field • Ensure all policy changes clearly communicate the impact on field operations • Increase transparency around why suggested goals, policies, and process are or are not accepted • Establish regional meetings for supervisors and employees supporting similar areas
2	Performance Management	Overhaul the performance management system to reflect the roles and responsibilities of the workforce; reinforce the leadership role in proactive and clear communications: • Ensure the performance management process engenders development • Refresh performance work plans for agents and non-agents • Create behaviorally anchored rating scale for performance work plans
3	Commitment to Mission	Create a clear and compelling ICE and HSI mission and strategy, aligned to field operations and including standard operating procedures and goals/priorities: • Establish minimum time requirements for which field offices work on priorities • Establish cutoff point for working cases, so effort is not wasted when priorities shift • Create a system to allow field offices to provide input on field-related decisions • Reexamine case quality over quantity for rating agents
4	Learning and Development	Inventory current training opportunities to determine what job-specific trainings need to be developed or updated to support required roles and position-based learning plans: • Consolidate similar training courses • Develop more hands-on (in-the-field) and instructor-led trainings, and conduct more cross-agency training sessions with other law enforcement and judicial agencies
5	Communication and Collaboration	Develop and launch a clear and compelling external media and communications campaign; ensure mission and vision understood by internal and external stakeholders: • Collaborate with the Office of Public Affairs to gather and highlight agency success • Launch local outreach programs with local schools, government, and agencies
6	Commitment to Mission	Conduct workload assessment for agents and non-agents to better understand work allocation and resource needs: • Identify non-investigative tasks that take up significant time for agents and determine ways to eliminate them (e.g., agency car maintenance) • Restructure and optimize support staff for agents
7	Performance Management	Develop an awards process to recognize and reward employees fairly: • Develop a peer recognition program to allow employees to nominate performance by individuals and teams • Increase volume of spot rewards by Special Agents in Charge or leadership
8	Work-life Balance	Encourage offices to establish employee engagement councils to increase networking office camaraderie: • Review existing employee engagement groups (e.g., San Juan or Newark) and replicate leading practices • Select champion for the engagement council and develop priorities, goals, and objectives for the effort
9	Learning and Development	Develop position-specific career paths for agents and non-agents, and create career planning tools and resources: • Assess competencies to better understand required skills proficiency levels

Question#:	14
Topic:	Morale
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

		• Update position descriptions and recruiting materials • Create a new employee handbook with SOPs, list of resources, and key contacts for new employees
10	Learning and Development	Analyze and revise agency and self-funded lateral rotational program (across ICE and between offices) with communications about how it works, who is eligible, and why it is important for career development

Question#:	15
Topic:	Section 274d 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Use of Fine Authority under Section 274d of the Immigration and Nationality Act

Under the authority of § 274d of the Immigration and Nationality Act (INA) (8 U.S.C. § 1324d), DHS currently possesses the authority to fine any illegal alien who willfully refuses to leave the United States after being given a final order of removal $500 per day, until such time as the alien leaves the United States.

Given this current statutory authority, as well as the current large volume of illegal aliens in the United States, DHS could incentivize detentions and removals and generate substantial revenue, which it frequently claims it needs to fulfill key components of its statutory obligations, if it simply enforced § 274d of the INA.

Below are some examples of the volume of revenue that could be generated if DHS were to enforce this law:

It would generate $459,184,500 in revenue per day if levied against all 918,369 non-detained illegal aliens who are present in the United States, are on their own recognizance, and have been ordered deported pursuant to a final order of removal but nevertheless remain in the United States in defiance of that order.

It would generate approximately $89,513,500 in revenue per day even if levied against only the 179,027 illegal aliens with criminal convictions who are present in the United States and have been ordered deported pursuant to a final order of removal but nevertheless remain in the United States in defiance of that order.

Assuming a total ICE budget authorization of $6.5 billion, if only 900,000 of the 918,369 non-detained illegal aliens who are present in the United States, are on their own recognizance, and have been ordered deported pursuant to a final order of removal but nevertheless remain in the United States in defiance of that order were charged the required daily $500 penalty for remaining in the United States, ICE could completely self-fund in less than 15 days.

1. Is DHS currently enforcing § 274d of the INA?

Response: The Department of Homeland Security (DHS) prioritizes the removal of aliens who pose the most serious risk to public safety, national security, and border

Question#:	15
Topic:	Section 274d 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

security, and, like the former Immigration and Naturalization Service, has not implemented this Immigration and Nationality Act (INA) civil penalty provision.

a. If the answer to Question (1) is no, please provide the following:

i. Whether DHS leadership is aware that it currently possesses the authority to fine illegal aliens for their illegal presence in the United States in the wake of a final order of removal.

Response: The Secretary of Homeland Security is charged with administration and enforcement of the nation's immigration laws and the Department's leadership is aware of the scope and importance of that responsibility.

ii. If DHS leadership is aware of this authority, a detailed explanation as to why § 274d of the INA is not being enforced.

Response: While the INA reflects authority to collect a prescribed civil penalty amount for certain acts that prevent aliens' removal from the United States, the provision in question does not impose a mandate and does not establish a process for such penalty collection. In order to levy this type of civil fine, due process requires that the government must provide a notice of hearing and the opportunity to be heard. The economic impact of implementing such processes must be weighed against the operational benefit of achieving removal of such individuals. For instance, the resources that such legal proceedings would consume, both in terms of a court's adjudication time and the Executive Branch's initiation and prosecution of the civil penalty case, would need to be weighed against whether a willful failure or refusal to leave can be proven, the severity of the violation and other, competing matters, such as prosecution of violent criminal offenders and vigorous defense of DHS's immigration enforcement authorities. Moreover, many aliens with final orders of removal do not violate § 1324d, while others work actively to avoid detection, and many lack meaningful assets, which would severely impact the ability to collect fines pursuant to this provision.

iii. Whether you, as the head of ICE, have the independent authority to instruct ICE personnel to enforce § 274d of the INA.

Response: The DHS Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement (ICE), Delegation Number: 7030.2, authorizes the Assistant Secretary, now Director, to administer and enforce 8 U.S.C. § 1324d. However, there are no codifying regulations for this statutory provision.

Question#:	15
Topic:	Section 274d 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

iv. If you do not have the independent authority to instruct ICE personnel to enforce § 274d of the INA, who at DHS has the ability to either enforce this provision or instruct other DHS personnel to enforce this provision.

Response: See prior response.

v. Given that § 274d of the INA says that the federal government "shall" levy the statutorily prescribed penalty, please explain why DHS and/or ICE is not enforcing this statute.

Response: See response to (1)(a)(ii).

b. If the answer to Question 1 is yes, please provide the following:

i. How much revenue DHS has generated pursuant to enforcement of § 274d of the INA from Fiscal Year (FY) 2005 through FY 2015.

Response: Not applicable.

ii. The account into which DHS deposits revenue generated pursuant to enforcement of § 274d of the INA.

Response: Not applicable.

iii. Line-item information about how DHS has spent the revenue collected pursuant to enforcement of § 274d of the INA from FY 2005 through FY 2015.

Response: Not applicable

iv. Any challenges that DHS has encountered in enforcing § 274d of the INA.

Response: Not applicable.

Question#:	16
Topic:	Section 274d 2
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: If ICE does not have the authority to enforce § 274d of the INA, which other component of DHS - Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), or some other component - has the authority to enforce § 274d of the INA?

Response: U.S. Immigration and Customs Enforcement has the authority to enforce Section 274D of the Immigration and Nationality Act, but the substantial practical limitations, including the legal processes required to effectuate a fine under 274D, make pursuing such fines impractical.

Question#:	17
Topic:	Section 274d 3
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Do you agree with the statement that enforcement of § 274d of the INA would serve as a substantial financial disincentive for entering and remaining in the United States illegally? If you do not agree with this statement, please provide a detailed explanation as to why.

Response: While the Immigration and Nationality Act reflects authority to collect a prescribed civil penalty amount for certain acts that prevent aliens' removal from the United States, the provision in question does not establish a process for such penalty collection. In order to levy this type of civil fine, due process requires that the government must provide a notice of hearing and the opportunity to be heard. The economic impact of implementing such processes must be weighed against the operational benefit of achieving removal of such individuals. For instance, the resources that such legal proceedings would consume, both in terms of a court's adjudication time and the Executive Branch's initiation and prosecution of the civil penalty case, would need to be weighed against whether a violation has occurred, and, if so, the severity of the violation and other, competing matters, such as prosecution of violent criminal offenders and vigorous defense of the Department of Homeland Security's immigration enforcement authorities. Moreover, many aliens with final orders of removal work actively to avoid detection and lack meaningful assets, rendering any collection processes undertaken pursuant to this provision futile.

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Status of Acknowledged 11,315 Criminal Aliens Currently in Federal Detention

According to information supplied to the Committee on October 26, 2015, there were, as of October 26, 2015, 11,315 illegal aliens with criminal convictions who were in federal custody awaiting deportation.

1. **Please provide the following information regarding these 11,315 illegal aliens with criminal convictions:**

Response: To clarify, this figure represents aliens with final orders of removal in U.S. Immigration and Customs Enforcement (ICE) custody as of September 12, 2015. Please note that upon review, ICE records indicate that the total number was 11,314. The following responses reflect ICE records as of January 16, 2016.

a. **How many were convicted of committing a homicide crime (i.e., murder of any degree, manslaughter of any type or degree, etc.)?**

   Response: Of the 11,314 aliens, 141 were convicted of a homicide-related crime.

b. **How many were convicted of committing a rape or other sexual assault?**

   Response: Of the 11,314 aliens, 234 were convicted of rape or sexual assault.

c. **How many were convicted of committing some other violent crime?**

   Response: Of the 11,314 aliens, 1,699 aliens were convicted of another violent crime.

d. **How many were convicted of committing burglary, identity theft, or other theft crime?**

   Response: Of the 11,314 aliens, 1,653 were convicted of burglary, identity theft, or another theft crime.

e. **How many were convicted of drug-related offenses?**

   Response: Of the 11,314 aliens, 2,099 were convicted of a drug-related offense.

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

f. How many were convicted of committing a driving under the influence of drugs or alcohol offense (felony or misdemeanor)?

Response: Of the 11,314 aliens, 1,881 were convicted of a DUI.

g. Since the receipt of this information from ICE, how many of these 11,315 illegal aliens with criminal convictions have been released from federal custody (if applicable)? For each instance where any of these individuals has since been released from federal custody, please provide detailed information about both the alien's criminal history and the circumstances that led to the alien's release (including the ICE official who authorized the alien's release).

Response: Of the 11,314 aliens with final orders of removal in ICE custody as of September 12, 2015, 2,077 were subsequently released from ICE custody as of January 16, 2016. The table below provides a breakdown of the types of specific criminal convictions associated with the 2,077 placed in a non-custodial setting as of January 16, 2016. An alien may have more than one criminal conviction. As such, the total number of criminal convictions is greater than the total number of criminal aliens released from ICE custody.

The detention of aliens subject to a final order of removal is governed by section 241 of the Immigration and Nationality Act and the implementing regulations at 8 C.F.R. § 241. When countries delay or refuse the repatriation of their nationals, ICE is frequently required to release them from custody pursuant to the decision of the U.S. Supreme Court in *Zadvydas v. Davis*, 533 U.S. 678 (2001). *See also Clark v. Martinez,* 543 U.S. 371 (2005).

Convictions	**Number of Convictions**[5]
Traffic Offense	280
Driving Under Influence Liquor	233
Larceny	189
Illegal Entry (INA SEC.101(a)(43)(O), 8USC1325 only)	122
Burglary	113

[5] Please note that an alien may have more than one criminal conviction. As such, the total number of criminal convictions is greater than the total number of criminal aliens released from ICE custody.

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Convictions	**Number of Convictions**[5]
Assault	103
Drug Possession	79
Dangerous Drugs	72
Robbery	71
Fraud	69
Cocaine—Possession	67
Marijuana—Possession	61
Probation Violation	54
Trespassing	54
Resisting Officer	53
Disorderly Conduct	51
Battery	50
Domestic Violence	45
Cocaine—Sell	41
Drug Trafficking	41
Shoplifting	36
Aggravated Assault—Weapon	35
Fraud - Illegal Use Credit Cards	34
Illegal Re-Entry (INA SEC.101(a)(43)(O), 8USC1326 only)	30
Forgery	29
Narcotic Equip—Possession	27
Stolen Property	27
Fraud—Impersonating	27
Vehicle Theft	26
Marijuana—Sell	26
Public Order Crimes	26
Amphetamine—Possession	26
Failure To Appear	25
Weapon Offense	23
Fraud—False Statement	23
Receive Stolen Property	23

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Convictions	**Number of Convictions**[5]
Damage Property	23
Possession Stolen Property	23
Sex Assault	22
Identity Theft	22
Possession Of Weapon	22
Burglary—Forced Entry—Residence	18
Obstruct Police	17
Violation of a Court Order	17
Unauthorized Use of Vehicle (includes joy riding)	16
Contempt Of Court	15
Aggravated Assault—Family—Strongarm	15
Carrying Concealed Weapon	15
Burglary Tools—Possession	14
Liquor—Possession	13
Homicide—Willful Kill—Weapon	13
Hit and Run	13
Harassing Communication	12
Kidnapping	12
Larceny—From Building	11
Threat Terroristic State Offenses	11
Crimes Against Person	11
Immigration (Possess of Fraud. Immigration Docs)	11
Heroin—Possession	10
Public Peace	10
Drugs—Health or Safety	10
False Citizenship	10
Flight To Avoid (prosecution, confinement, etc.)	10
Licensing Violation	10
Racketeer Influenced and Corrupt Organizations Act (RICO)	9
Homicide	9

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Convictions	**Number of Convictions**[5]
Driving Under Influence Drugs	9
Amphetamine—Sell	8
Cocaine	8
Aggravated Assault—Non-family—Gun	8
Property Crimes	8
Marijuana	8
Conspiracy [use when no underlying offense, such as 18 U.S.C. SEC. 371]	8
Sex Offense Against Child—Fondling	7
Parole Violation	7
Aggravated Assault—Non-family—Strongarm	7
Aggravated Assault—Gun	7
Cruelty Toward Wife	7
Aggravated Assault—Non-family—Weapon	7
Counterfeiting	6
Pass Forged (identify in comments)	6
Lewd or Lascivious Acts with Minor	6
Health—Safety	6
Cocaine—Smuggle	6
Cruelty Toward Child	6
Forgery Of (identify in comments)	6
Conservation—Fish	6
Sex Offense	5
Counterfeiting Of (identify in comments)	5
Aggravated Assault—Police Officer—Strongarm	5
Burglary—No Forced Entry—Residence	5
Making False Report	5
Indecent Exposure	5
Aggravated Assault—Family—Weapon	5
Synthetic Narcotic—Possession	5
Neglect Child	5
Liquor	5

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Convictions	**Number of Convictions**[5]
Heroin—Sell	5
Robbery—Residence—Gun	5
Witness—Dissuading	5
Homicide—Willful Kill-Gun	4
Robbery—Residence—Weapon	4
Carrying Prohibited Weapon	4
Simple Assault	4
Intimidation	4
Forgery Of Checks	4
Robbery—Street—Weapon	4
Marijuana (describe offense)	4
Sexual Exploitation of Minor—Sex Performance	4
Money Laundering—Remarks	4
Statutory Rape—No Force	4
Obstructing Justice	4
Stolen Vehicle	4
Possession Forged (identify in comments)	4
Prostitution	4
Perjury	3
Robbery—Business Weapon	3
Synthetic Narcotic—Sell	3
Burglary—No Forced Entry—Non-Residence	3
Aggravated Assault—Public Officer—Strongarm	3
Marijuana—Smuggle	3
Rape—Strongarm	3
Smuggling Aliens	3
Escape (identify type institution in comments)	3
Heroin	3
Indecent Exposure to Minor	3
Robbery—Residence—Strongarm	3
Fraud By Wire	3
Embezzle	3

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Convictions	**Number of Convictions[5]**
Larceny—From Banking-Type Institution	3
Escape From Custody	2
Sale Of Stolen Property	2
Molestation of Minor	2
Possession Counterfeited (identify in comments)	2
Sex Assault—Carnal Abuse	2
Fraud—Insufficient Funds Check	2
Larceny—From Auto	2
Mail Fraud	2
Obstructing Court Order	2
Failing to Move On	2
Damage Property—Private	2
Bribery	2
Firing Weapon	2
Obstruct (specify Judiciary, Congress, Legislature, Commission in comments)	2
Arson	2
False Imprisonment	2
Smuggle Contraband Into Prison	2
Burglary—Forced Entry—Non-Residence	2
Robbery—Business—Gun	2
Hallucinogen—Possession	2
Theft And Use Vehicle Other Crime	2
Possession Stolen Vehicle	2
Family Offense	2
Smuggle Contraband	1
Illegal Arrest	1
Homicide—Negligent Manslaughter—Vehicle	1
Enticement of Minor for Indecent Purposes	1
Sexual Exploitation of Minor—Material—Transport	1
Rape—Remarks	1

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Convictions	**Number of Convictions**[5]
Exploitation of a Minor	1
Kidnap Adult	1
Opium Or Derivatives—Possession	1
Pass Counterfeited (identify in comments)	1
Aggravated Assault—Public Officer—Gun	1
Heroin—Smuggle	1
Possession Tools For Forgery/Counterfeiting	1
Riot	1
Procure for Prostitute Who is an Adult	1
Burglary—Banking-Type Institution	1
Strip Stolen Vehicle	1
Robbery—Banking-Type Institution	1
Theft And Sale Vehicle	1
Gratuity—Receiving	1
Conservation - License-Stamp	1
Carjacking-Armed	1
Robbery—Business—Strongarm	1
Sexual Exploitation of Minor—Material—Film	1
Burning Of (Identify object in comments)	1
Aggravated Assault—Police Officer—Gun	1
Pocketpicking	1
Hallucinogen—Sell	1
Kidnap Minor	1
Procure For Prostitute (pimping)	1
Robbery—Street—Gun	1
Gambling	1
Robbery—Street—Strongarm	1
Abortifacient (selling, mfg., delivering, etc.)	1
Kidnap Minor—Parental	1
Homicide—Willful Kill—Non-family—Gun	1
Conservation—Animals	1
Tax Revenue	1

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Convictions	**Number of Convictions[5]**
Kickback—Receiving	1
Theft And Strip Vehicle	1
Contributing to Delinquency of Minor	1
Assembly—Unlawful	1
Sex Assault—Disabled	1
Transport Counterfeited (identify in comments)	1
Sex Assault—Sodomy—Girl—Strongarm	1
Barbiturate—Possession	1
Sex Offender Registration Violation	1
Bookmaking	1
Gang Activity	1
Espionage	1
Embezzle—Public Property (U.S., state, city property)	1
Obstruct Criminal Invest	1
Amphetamine	1
Total	**3,131**

h. **For each of the 11,315 illegal aliens with criminal convictions who were in custody as of October 26, 2015, how many have been in federal custody for more than:**

Of the 11,314 aliens with final orders of removal in ICE custody as of September 12, 2015, 2,068 were detained as of January 16, 2016. Of the 2,068 that were detained as of January 16, 2016, 1,130 have criminal convictions. The following breakdown is reflective of length of stay for the 1,130 final order criminal aliens.[6] Since September 12, 2015, an alien may have been released from ICE custody and subsequently booked back into ICE custody.

1) **30 days or less?**

[6] Length of stay is reflective of an alien's current detention stay, as of January 16, 2016.

Question#:	18
Topic:	Aliens Currently in Federal Detention
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Response: Of these 1,130 final order criminal aliens detained as of January 16, 2016, 17 have been detained for 30 days or less.

2) 31 to 90 days?

Response: Of these 1,130 final order criminal aliens detained as of January 16, 2016, 8 have been detained for 31-90 days.

3) 91 to 180 days?

Response: Of these 1,130 final order criminal aliens detained as of January 16, 2016, 220 have been detained for 91-180 days.

The remaining 885 final order criminal aliens detained as of January 16, 2016 have been detained for longer than 180 days. Many of these aliens have pending cases with the Executive Office for Immigration Review or appeals with the Board of Immigration Appeals or United States Court of Appeals. Additionally, many cases are pending the issuance of travel documents necessary for removal from the United States.

Question#:	19
Topic:	ICE-issued grants
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Contrast between Administration's Treatment of Sanctuary Jurisdictions and Jurisdictions Refusing to Accept Syrian Refugees

The Obama Administration has adopted different approaches for addressing immigration issues that affect states and localities. While the Administration has essentially opted not to address so-called sanctuary jurisdictions' very public expressions of intent to not comply with federal immigration detainers, and seems uninterested in apprehending criminal aliens that are in local custody, the Administration has nevertheless quickly vowed to pressure state and local governments that have decided they will not accept any Syrian refugees because of the potential national security risks associated with that population. These concerns have recently been justified based on counterterrorism data suggesting that the Islamic State of Iraq and Syria (ISIS) is intentionally seeking to enter the United States via the refugee flow from the war-torn region.

Specifically, Robert Carey, the Director of HHS ORR, sent a letter to several state governors' offices, demanding their compliance with the Administration's plans to settle refugees in those jurisdictions. After conceding that states must agree with ORR resettlement plans in accordance with the Refugee Act of 1980, Carey added that "[s]tates that continue to use ORR funding must ensure that assistance and services are delivered without regard to race, religion, nationality, sex, or political opinion." Carey went on to note that states that denied "ORR-funded benefits and services to Syrian refugees ... would not be in compliance with the State Plan requirements [and applicable statutes] ... and could be subject to enforcement action, including suspension or termination," presumably of federal grant funding. Carey went on to note that states could also theoretically be prosecuted under Title VI of the Civil Rights Act for not providing "Federal financial assistance," such as Medicaid and TANF, to refugees.

Please provide a full list of any ICE-issued grants (including law enforcement-related grants) that could theoretically be suspended, cancelled, or withdrawn by ICE in the event a state or local government opts to not permit the settlement of Syrian refugees in their jurisdiction (if applicable).

What language in ICE-issued grant agreements would permit the suspension, cancellation, or withdrawal of ICE-issued grant funding for such a state or local decisions (if applicable)?

Did you or any other ICE employee edit, or in any way make suggestions about the content of, Director Carey's November 25 letter? If the answer is yes, please provide

Question#:	19
Topic:	ICE-issued grants
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

additional information about contributions, including the names of the ICE employees who contributed to the letter in any way.

Response: For questions regarding Director Carey's letter, we refer you to the Office of Refugee Resettlement. U.S. Immigration and Customs Enforcement (ICE) does not have statutory authority to issue grants, law enforcement-related or otherwise. Therefore, ICE could not suspend, cancel, or withdraw any grant if a state or local government elected to not permit Syrian refugee settlement in their jurisdiction.

Question#:	20
Topic:	Sanctuary jurisdictions
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: During your hearing testimony last Wednesday, Senator Al Franken (D-Minn.) expressed a fundamental misunderstanding of the basis for sanctuary jurisdictions' refusals to cooperate with federal immigration detainers. Specifically, Senator Franken commented that sanctuary jurisdictions were refusing to cooperate with federal immigration detainers in order to ensure that illegal aliens who wanted to report crime were not afraid to do so. Senator Franken's commentary ignores the fact that federal immigration detainers apply only to illegal aliens who have been arrested for (or convicted of) a crime.

Is the Obama Administration's support for sanctuary jurisdictions' ignoring of federal immigration law and refusals to honor federal immigration detainers based on its misunderstanding that federal immigration detainers would impact those who report crime?

Response: U.S. Immigration and Customs Enforcement (ICE) is unable to comment on the specific reasons why a particular jurisdiction does not cooperate with ICE. The Priority Enforcement Program (PEP) focuses ICE's enforcement resources in local and state jails to identify criminal aliens convicted of offenses falling within the parameters of PEP while preserving community trust. As outlined in Secretary Johnson's November 20, 2014 memorandum *Secure Communities*, under PEP, only those with particular criminal convictions who are arrested by a state or local law enforcement agency (LEA) are subject to enforcement action.

ICE Field Office Directors have reached out to local jurisdictions regarding PEP, and are working towards fostering renewed cooperation with jurisdictions that have previously indicated an unwillingness to recognize ICE detainers. Many local law enforcement agencies, including more than half of jurisdictions that were previously not cooperating, have now agreed to participate in PEP.

PEP is a balanced, common-sense approach toward enforcing the nation's immigration laws and working cooperatively with our LEA partners, placing the focus on where it should be: on criminals and national security and public safety threats.

Question#:	21
Topic:	Gwendolyn Keyes-Fleming 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Concerns Regarding Qualifications and Conduct of Gwendolyn Keyes-Fleming

Gwendolyn Keyes-Fleming, who previously served as chief of staff to Administrator Gina McCarthy at the Environmental Protection Agency (EPA), left EPA earlier this year to assume the role of ICE's Principal Legal Advisor. Bluntly stated, Ms. Keyes-Fleming appears to have had zero experience with immigration law or issues prior to commencing her position as ICE's lead attorney.

Beyond her notable lack of relevant experience, EPA's Office of Inspector General also released a report (EPA OIG report) earlier this year in which it specifically identified Ms. Keyes-Fleming, by name, as one of several senior officials at EPA who took to no action to address (and may have even omitted sharing important information about) the inappropriate sexual harassment by senior EPA official Peter Jutro. The EPA OIG report demonstrates that Ms. Keyes-Fleming did not act on knowledge of Mr. Jutro's sexual harassment upon becoming aware of such conduct, which allowed the conduct to continue, to the detriment of numerous victims.

Below are some notable determinations that were in the EPA OIG report:

Mr. Jutro appears to have sexually harassed 17 women total while employed by EPA.

Mr. Jutro appears to have sexually harassed 6 of those women after being appointed to serve as the Acting Administrator of EPA's Office of Homeland Security (OHS) in February 2014.

Ms. Keyes-Fleming - who apparently also played a key role in having Mr. Jutro appointed to his position - appears to have known about Mr. Jutro's pattern of sexual harassment prior to helping him get appointed.

Ms. Keyes-Fleming had direct, personal knowledge of at least two of these episodes of harassment - one of which literally happened right outside her office door.

In June 2014 - at a point in time when Ms. Keyes-Fleming clearly knew about Mr. Jutro's harassing conduct - she and other senior-level EPA officials renewed his appointment to lead OHS.

It was only after Mr. Jutro photographed and kissed a Smithsonian Institute intern in his

Question#:	21
Topic:	Gwendolyn Keyes-Fleming 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

office in late July 2014 that EPA leadership placed Mr. Jutro on indefinite unpaid administrative leave.

Despite her knowledge of Mr. Jutro's inappropriate behavior for several weeks, Ms. Keyes-Fleming was part of a group of senior-level EPA officials who actively obstructed OIG's investigation of Mr. Jutro's behavior, and concealed additional instances of his harassing conduct from OIG investigators.

Because Ms. Keyes-Fleming refused to do her job at EPA, Mr. Jutro was never dealt with by EPA, and he was ultimately allowed to retire from federal service with full benefits, without so much as a note in his file about his serial sexual harassment at EPA.

When I asked Secretary Johnson in writing earlier this year about the hiring of Ms. Keyes-Fleming, her lack of qualifications to be ICE's lead attorney, and her central role in the cover-up of sexual harassment inside EPA, Secretary Johnson wrote that Mr. Jutro "was selected, after a lengthy search, by the DHS Counsel General, in consultation with Assistant Secretary Saldana, the leader of ICE" (emphasis added), and that she was "carefully vetted before she was offered the position of Principal Legal Advisor."

Secretary Johnson specifically identifies you as one of two people at DHS who are primarily responsible for hiring Ms. Keyes-Fleming to be ICE's Principal Legal Advisor. During your efforts to bring Ms. Keyes-Fleming to ICE, did you know about her EPA OIG-determined role in covering up sexual harassment at EPA?

Secretary Johnson also noted that Ms. Keyes-Fleming was "carefully vetted" for this position. Were you involved in any way in the vetting of Ms. Keyes-Fleming?

Response: Ms. Keyes Fleming has the full confidence of the Department, including ICE. In total, Ms. Keyes Fleming has more than 17 years of experience as a law enforcement lawyer. As the District Attorney of DeKalb County, Georgia, Ms. Keyes Fleming oversaw a significant staff, which prosecuted approximately 11,000 felony cases annually. In her most recent position as the Chief of Staff to the Administrator of the U.S. Environmental Protection Agency (EPA), Ms. Keyes Fleming worked directly with the Administrator in overseeing the policy and management priorities of an Agency with approximately 15,000 employees and an $8 billion annual budget. While serving as the Region 4 Regional Administrator of the EPA, Ms. Keyes Fleming led efforts to maintain and enhance the quality of work life for approximately 1,000 employees while effectively managing a budget of over $500 million.

Question#:	22
Topic:	Gwendolyn Keyes-Fleming 2
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: If you assert that you had not known about Ms. Keyes-Fleming's role the EPA sexual harassment cover-up before the decision to hire her had been made, would you still have wanted to hire her if you had known about her role in the cover-up?

4. Were any career ICE attorneys ever under consideration for the position of Principal Legal Advisor?

a. If your answer to Question (4) is yes, please name some of the attorneys who were considered.

5. Were any external (non-ICE) attorneys with demonstrable immigration experience ever under consideration for the position of Principal Legal Advisor?

a. If your answer to Question (5) is yes, please name some of the attorneys who were considered.

6. Whether your answer is yes or no to Questions 4 or 5, what sort of formalized hiring process (if any) does ICE have in place for the position of Principal Legal Advisor?

7. Please explain why an attorney such as Ms. Keyes-Fleming, who had literally zero immigration experience at the time she was hired to be the Principal Legal Advisor, is qualified to serve in that position?

8. Do you believe it is wise for an agency whose primary task is immigration enforcement to have a chief legal advisor who has zero experience handling that agency's subject matter?

9. Is Ms. Keyes-Fleming involved in any way in any review of ICE employee sexual harassment or discrimination claims?

Response: Ms. Keyes Fleming has the full confidence of the Department, including ICE. In total, Ms. Keyes Fleming has more than 17 years of experience as a law enforcement lawyer. As the District Attorney of DeKalb County, Georgia, Ms. Keyes Fleming oversaw a significant staff, which prosecuted approximately 11,000 felony cases annually. In her most recent position as the Chief of Staff to the Administrator of the U.S. Environmental Protection Agency (EPA), Ms. Keyes Fleming worked directly with

Question#:	22
Topic:	Gwendolyn Keyes-Fleming 2
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

the Administrator in overseeing the policy and management priorities of an Agency with approximately 15,000 employees and an $8 billion annual budget. While serving as the Region 4 Regional Administrator of the EPA, Ms. Keyes Fleming led efforts to maintain and enhance the quality of work life for approximately 1,000 employees while effectively managing a budget of over $500 million.

Question#:	23
Topic:	Assaults of ICE Agents
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Recent Assaults of ICE Agents by Mexican Nationals

On April 19, 2015, at least two U.S. Border Patrol agents were injured on the Rio Grande River in the vicinity of Anzalduas Park near McAllen, Texas. Initial reports indicated that these two Border Patrol agents were attacked with stones and rocks from the Mexican side of the Rio Grande River after their boat capsized, and that one of those Border Patrol agents suffered injuries that required hospitalization.

Have there been any similar such incidents of violence by Mexican nationals (or other unknown nationals or individuals) against ICE personnel during ICE enforcement operations at the U.S.-Mexico border? If the answer is yes, please provide additional details.

Response: While the data are not constrained to any specific nationality or location within the United States, from January of 2013 to December of 2015, U.S. Immigration and Customs Enforcement (ICE) investigated 73 criminal assaults on ICE agents and officers.

Question#:	24
Topic:	Federal Recordkeeping Requirements 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Compliance with Federal Recordkeeping Requirements

Reports over the last few years have indicated that high-level Administration officials, including cabinet-level officials, have used personnel e-mail accounts and other personal means of communication to conduct official business. Such conduct, except under narrow circumstances, is illegal under federal law.

Do you acknowledge that it is illegal under Federal law, except under narrow circumstances, to use personal e-mail accounts and other personal means of communication to conduct official business?

Response: Yes.

Have you ever used a personal e-mail account under the name Sarah Saldana to conduct official business? If the answer is yes, please provide additional information about the e-mail account, including the e-mail address and the occasions and circumstances of use.

Response: No.

Have you ever used a personal e-mail account under any other name (such as a pseudonym) or identity to conduct official business? If the answer is yes, please provide additional information about the e-mail account, including the e-mail address, the name or identity associated with the e-mail account, and the occasions and circumstances of use.

Response: No.

Have any other senior-level officials within your Department ever used a personal e-mail account to conduct official business? If the answer is yes, please provide additional information about the individual(s) involved, the e-mail account(s) involved, and the occasions and circumstances of use.

Response: All U.S. Immigration and Customs Enforcement employees have been informed to follow communication methods in a manner consistent with controlling law and policy. Please see the attached policy report.

Question#:	25
Topic:	Federal Recordkeeping Requirements 2
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Ted Cruz
Committee:	JUDICIARY (SENATE)

Question: Part of the reason for these stringent recordkeeping requirements has to do with being able to assure the proper level of security for the use and transfer of sensitive information. Unauthorized use of personal e-mail accounts or other personal means of communication runs the risk of exposing sensitive federal information systems to intrusion or damage.

Has ICE experienced any cyber-security-related breach or damage incidents as the result of your or another employee's use of personal e-mail accounts and other personal means of communication to conduct official business? If the answer is yes, please provide additional information about these incidents, including the dates, circumstances, and responses.

Response: U.S. Immigration and Customs Enforcement (ICE) began blocking access to personal webmail accounts from the ICE Network in November 2011. The last significant security incident linked to webmail occurred in 2011 prior to the blocking of webmail use. Examples of webmail security incidents that occurred before the block included a user who uploaded a spreadsheet containing Sensitive Personally Identifiable Information of other employees to the user's personal webmail account, and a user who downloaded a malicious attachment from their personal webmail account.

ICE is currently unaware of any cyber-security-related breach or damage incidents as the result of an employee's use of personal email accounts or other personal means of communication to conduct official business since the blocking of webmail use described above. Generally, ICE discourages employees from using non-official electronic messaging accounts to conduct official business. However, if an employee chooses to use non-official electronic messaging accounts to conduct official business, pursuant to The Presidential and Federal Records Act Amendments of 2014, the employee is required to copy his or her official ICE email account during transmission of the message. Alternatively, he or she may forward the message to his or her official ICE email account within 20 calendar days. See Public Law 113-187 available at www.archives.gov/about/laws/p-l-113-187.pdf.

Entry/Exit Overstay Report

Fiscal Year 2015

U.S. Department of Homeland Security

Message from the Secretary

January 19, 2016

I hereby present the following "Entry/Exit Overstay Report" prepared by the Department of Homeland Security (DHS). Pursuant to the requirement contained in Division F, Title I of P.L. 114-113, the Consolidated Appropriations Act, 2016, and 8 U.S.C. 1376, DHS is submitting this report on overstay data.

DHS has generated this report to provide data on departures and overstays, by country, for foreign visitors to the United States who were expected to depart in Fiscal Year (FY) 2015 (October 1, 2014-September 30, 2015).

This report is being provided to the following Members of Congress:

The Honorable Harold Rogers
Chairman, House Committee on Appropriations

The Honorable Nita M. Lowey
Ranking Member, House Committee on Appropriations

The Honorable Bob Goodlatte
Chairman, House Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member, House Committee on the Judiciary

The Honorable Michael McCaul
Chairman, House Committee on Homeland Security

The Honorable Bennie Thompson
Ranking Member, House Committee on Homeland Security

The Honorable Thad Cochran
Chairman, Senate Committee on Appropriations

The Honorable Barbara Mikulski
Vice Chairwoman, Senate Committee on Appropriations

The Honorable Charles Grassley
Chairman, Senate Committee on the Judiciary

The Honorable Patrick Leahy
Ranking Member, Senate Committee on the Judiciary

The Honorable Ron Johnson
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Thomas R. Carper
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

Inquiries relating to this report may be directed to the DHS Office of Legislative Affairs at (202) 447-5890.

Sincerely,

Jeh Charles Johnson

Executive Summary

Pursuant to the requirement contained in Division F, Title I of P.L. 114-113, the Consolidated Appropriations Act, 2016, and 8 U.S.C. 1376, the Department of Homeland Security is submitting this report on overstay data. This report is submitted to provide data on departures and overstays, by country, for foreign visitors who were admitted to the United States though air and sea Ports of Entry (POEs), and who were expected to depart in FY 2015 (October 1, 2014-September 30, 2015).

An overstay is a nonimmigrant who was lawfully admitted to the United States for an authorized period but stayed or remains in the United States beyond his or her lawful admission period. DHS identifies two types of overstays—those individuals for whom no departure has been recorded (Suspected In-Country Overstay) and those individuals whose departure was recorded after their lawful admission period expired (Out-of-Country Overstay). The overstay identification process is conducted through arrival, departure and immigration status information, consolidated to generate a complete picture of individuals traveling to the United States as described below.

U.S. Customs and Border Protection (CBP) receives passenger manifest data on all commercial and private air and commercial sea arrivals to and departures from the United States. These manifests indicate who is onboard the aircraft or vessel. In the land environment, CBP receives traveler data on third country nationals departing to Canada. Additionally, CBP is able to reconcile a significant portion of travelers who arrive through our borders with both Canada and Mexico as the majority of those travelers are frequent crossers and CBP is able to close a previous arrival when a new arrival is recorded.

Upon arrival in the United States, CBP officers interview every traveler to determine the purpose and intent of travel. CBP officers also confirm the accuracy of the biographic manifest data provided by the carriers, who are subject to fines for any missing or inaccurate data. For most foreign nationals, the person’s fingerprint biometrics and digital photograph are collected.

For departing travelers, air and sea carriers provide biographic manifest data for all travelers prior to leaving the United States. The carriers are required by law to provide specific sets of data, which include name and passport number, and they are subject to fines for missing or inaccurate data. The biographic departure data are then matched against arrival data to determine who has complied with the terms of admission and who has overstayed. CBP maintains a separate system specifically for this purpose. This system also receives other DHS data relevant to whether a person is lawfully present-such as immigration benefit information or information on student visitors to the United States.

It is very important to point out that determining lawful status is more complicated than simply matching entry and exit data. For example, a person may receive a six month stay at the time of entry but then apply for and receive an extension of that six months while in the United States—which is relevant in determining if a person is truly an overstay or not.

Arrivals to and departures from the United States are by definition fluid, and for the purposes of a written report, "cutoff dates" were established. Unless otherwise noted, for the charts embedded within this report, the totals refer to departures that were expected to take place between October 1, 2014 and September 30, 2015.

This report is limited to foreign nationals who entered the United States as nonimmigrant visitors for business (i.e., B-1 and WB visas) or pleasure (i.e., B-2 and WT visas) through an air or sea POE. DHS has determined that there were a total of 44,928,381 nonimmigrant admissions to the United States for business or pleasure through air or sea POEs that were expected to depart in FY 2015, which represents the vast majority of annual nonimmigrant admissions. Of this number, DHS calculated a total overstay rate of 1.17 percent, or 527,127 individuals. In other words, 98.83 percent had left the United States on time and abided by the terms of their admission.

This report breaks the overstay rates down further to provide a better picture of those overstays that remain in the United States beyond their period of admission and for whom no evidence of a departure or transition to another immigration status. At the end of FY 2015, there were 482,781 Suspected In-Country Overstays. The overall Suspected In-Country Overstay rate for this scope of travelers is 1.07 percent of the expected departures.

Due to continuing departures by individuals in this population, by January 4, 2016, the number of Suspected In-Country Overstays for FY 2015 had dropped to 416,500, rendering the Suspected In-Country Overstay rate as 0.9 percent. In other words, as of January 4, 2016, DHS has been able to confirm the departures of more than 99 percent of nonimmigrant visitors scheduled to depart in FY 2015 via air and sea POEs, and that number continues to grow.

This report separates Visa Waiver Program (VWP) country overstay numbers from non-VWP country numbers. For VWP countries, the FY 2015 Suspected In-Country Overstay rate is 0.65 percent of the 20,974,390 expected departures. For non-VWP countries, the FY 2015 Suspected In-Country Overstay rate is 1.60 percent of the 13,182,807 expected departures. DHS is in the process of evaluating whether and to what extent the data presented in this report will be used to make decisions on the VWP country designations.

For Canada and Mexico the FY 2015 Suspected In-Country Overstay rate is 1.18 percent of the 7,875,054 expected departures and 1.45 percent of the 2,896,130 expected departures respectively. Consistent with the methodology for other countries, this represents only travel through air and sea ports of entry and does not include data on land border crossings.

Entry/Exit Overstay Report

Table of Contents

I. Background

The purpose of this report is to identify country-by-country overstay rates for certain classes of admission.

U.S. Customs and Border Protection (CBP) collects biographic information on all nonimmigrant arrivals to the United States through an inspection by a CBP officer. In the air and sea environment, CBP officers validate the manifest information provided by commercial and private aircraft operators. For many nonimmigrants, submission of biometric information is also required upon admission and is captured in the presence of a CBP officer.[1] In addition, CBP has strengthened the document requirements at air, land, and sea Ports of Entry (POEs) by reducing the number of accepted travel documents one may use to enter the United States, [2] which in turn has increased CBP's ability to quickly and accurately collect information on arriving aliens, particularly at the land borders.

The United States did not build its border, aviation, and immigration infrastructure with exit processing in mind. Consequently, United States airports do not have designated areas exclusively for travelers leaving the United States. Instead, departures of travelers are recorded biographically using outbound passenger manifests provided by commercial carriers. Under regulations governing the Advance Passenger Information System, carriers are required to validate the manifest information against the travel document being presented before a traveler is permitted to board their aircraft or sea vessel.

In the land environment, travelers arrive at land POEs via various modes of transportation, including cars, trains, buses, ferries, bicycles, trucks, and on foot. There are major physical infrastructure, logistical, and operational hurdles to collect an individual's biographic and biometric data upon departure. Due to the existing limitations in collecting departure data in the land environment, this report does not include departure and overstay information from those travelers who entered the United States through a land POE. CBP is addressing these limitations through various efforts, including increased information sharing and partnerships, targeted operations, analyzing land POE departure traffic, and several pilots to experiment with innovative means of collecting biometric information from individuals departing via land POEs.

The Department of Homeland Security (DHS) anticipates the ability to provide a broader scope of data in future Entry/Exit Overstay Reports. Efforts by CBP, as described in this report, are ongoing and will continue to improve the existing process and availability of departure data.

[1] 8 C.F.R. § 235.1(f)(1)(ii)

[2] The Western Hemisphere Travel Initiative is a joint U.S. State Department/DHS initiative that implemented § 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108-458), which limited the documents that could be used to enter the United States.

II. Existing Operations

Congress transitioned entry/exit policy and operations to CBP through the *Fiscal Year (FY) 2013 DHS Appropriations Act* (Pub. L. No. 113-6) in order to centralize the entry/exit mission in one place within DHS. The entry/exit mission is to successfully capture and match the arrival and departure records of foreign nationals who visit the United States in order to help determine who is lawfully abiding by, or violating, immigration law. Capture of departure information also contributes significantly to CBP security-related missions, such as counterterrorism or other law enforcement functions.

A. Air and Sea Environments

Today, in the air/sea environments, CBP obtains entry records through both carrier-provided manifest data and inspections conducted by CBP officers. CBP obtains biographic data on travelers who lawfully enter or depart the United States by air or sea.[3] Air and sea carriers are required by law to submit passenger manifests to CBP, which are then recorded as arrivals or departures from the United States.[4] Air carriers are required to provide data not simply on who has made a reservation for a particular flight, but who is actually on the aircraft at the time the aircraft departs.[5] Airlines are subject to fines for making errors regarding who is or is not on any particular aircraft.[6]

Although CBP currently obtains biographic arrival and departure information on almost all foreign nationals in the air/sea environment, and biometric entry data in the air environment, CBP plans to improve the existing process in the future, as follows:

- Biometric Exit Mobile: During the summer of 2015, CBP began collecting a sample of biometric exit data using mobile fingerprint collection devices on selected flights departing from major air POEs. This has afforded a small amount of biometric departure data and provided a significant law enforcement benefit for existing outbound operations. The current airports using this technology are: Chicago/O’Hare (ORD); Atlanta/Hartsfield (ATL); New York (JFK); Newark (EWR); Los Angeles (LAX); San Francisco (SFO); Miami (MIA); Dallas/Ft. Worth (DFW); Washington/Dulles (IAD); and Houston/George Bush (IAH). The goals of the program are to: 1) determine the percentage of reconciled departures that without biometrics would have gone unresolved; 2) identify enforcement needs for a comprehensive biometric exit solution across all air ports of entry; and, 3) validate carrier provided manifest information.

[3] In addition, the Department obtains biometric information on all nonimmigrants who enter the United States via air and sea, except for those who are exempt by regulation, which includes those over the age of 79 or under 14, diplomats, and certain other discrete categories. See 8 C.F.R. § 215.1(f)(1)(ii).
[4] 8 C.F.R. § 231.1, see also 70 Fed. Reg. 17849 (Apr. 7, 2005) (describing the specific data elements for each passenger that carriers are required to provide).
[5] 19 C.F.R. §§ 122.49(a); 122.74(a).
[6] 8 U.S.C. § 1221(g).

- Biometric Exit Field Trial: In late 2016, CBP will deploy a biometric exit field trial, which will test new technologies in collecting biometric data from departing air environment foreign nationals. This will be a comprehensive pilot that incorporates additional biometric modalities and is designed to inform a future nationwide deployment.

- New Reporting Environment: The *FY 2015 DHS Appropriations Act* provided $9.9 million for a new reporting environment for the Arrival and Departure Information System, which will allow CBP to track entry/exit and overstay data on a monthly or weekly basis, as needed. These funds are being used to build the new reporting environment during 2016.

B. Land Environment

The collection of departure information in the land environment is more difficult than in the air/sea environment due to the lack of electronically captured and provided information of who is exiting the United States. In the land environment, there is no such requirement for advance reporting of arrivals and departures, as the majority of travelers cross the borders using their own vehicle or as a pedestrian.

1. Northern Border

On the Northern border, CBP is addressing this limitation through a partnership with the Canada Border Services Agency. The Beyond the Border agreement[7] provides for an entry/exit initiative that has been implemented, under which Canada and the United States have agreed to exchange entry records for land crossings between the two countries, so that an entry into one is recorded as an exit from the other.

On June 30, 2013, Canada and the United States began exchanging entry data for third-country nationals, permanent residents of Canada, and U.S. lawful permanent residents, who enter through land POEs along the shared border, where information is collected electronically. As a result of this initiative, the United States now has a working land border exit system on its Northern border for non-U.S. and non-Canadian citizens. CBP is currently matching 99.13 percent of the entry information received from Canada to an entry in the Arrival Departure Information System.

Both countries plan to expand the program to include all travelers in the future.

[7] United States-Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness, Action Plan, Dec. 2011. Accessible at http://www.whitehouse.gov/sites/default/files/us-canada_btb_action_plan3.pdf.

2. Southern Border

The Southwest border with Mexico does not provide the same opportunities as the Northern border with Canada, because Mexico's infrastructure and data collection capabilities at the shared U.S.-Mexico border are currently more limited. As a result, CBP is exploring the best methods of obtaining data from travelers departing the United States and entering Mexico by land, including:

- "Pulse and surge" operations:[8] These operations are ongoing and provide some outbound departure information on travelers departing the United States and entering Mexico.

- Land Exit Pilot: In early 2016, CBP deployed a pilot at the Otay Mesa POE in California that collects biographic data from all departing travelers and biometric information from departing foreign national travelers in the pedestrian environment. The Otay Mesa pilot will help CBP identify future technologies and processes that could be used for cost-effective biographic and biometric exit data collection at land POEs.

- Southern Border traffic analysis: CBP has also completed a study analyzing the traffic patterns and reentry of travelers who enter the United States through the southwest land border. CBP plans to use it to determine the optimal places for CBP to place its existing resources in order to best collect departure information and target overstays.

To account for limited information available on foreign nationals departing into Mexico through the southwest border, CBP employs several measures: ongoing Pulse and Surge operations provide some outbound departure information on travelers departing the United States and entering Mexico; land I-94 forms (forms provided upon entry that are to be returned upon departure) voluntarily turned in at the borders by foreign nationals leaving the country are collected and recorded; and subjects who enter the United States and subsequently return to the United States without an identified exit are reconciled for the prior trip due to subsequent entry.

C. Overstay Definition

An overstay is a nonimmigrant who was lawfully admitted to the United States for an authorized period but stayed in the United States beyond his or her lawful admission period. This also includes a nonimmigrant admitted for "duration of status" who fails to maintain that status. "Duration of status" is a term used for foreign nationals who are admitted for a specific purpose, which expires when that purpose expires—such as a student program that runs for four years of study.

[8] "Pulse and Surge" operations are strategies whereby CBP officers monitor outbound traffic on the U.S. southern border. See Testimony of Commissioner Alan Bersin, Commissioner of U.S. Customs and Border Protection, before the Senate Caucus on International Narcotics Control, Mar. 9, 2011. Accessible at http://www.dhs.gov/news/2011/03/09/testimony-commissioner-alan-bersin-us-customs-and-border-protection-senate-caucus. Although the purpose of "pulse and surge" is to counter traffic in drugs, currency, and firearms into Mexico, data collected during these operations can be used to create departure records for foreign nationals.

The Department classifies individuals as overstays by matching departure and status change records to arrival records collected during the admission process. The Department identifies individuals as having overstayed if their departure record shows they departed the United States after their lawful admission period expired.[9] (i.e., Out-of-Country Overstays). While these individuals are considered overstays, there is evidence indicating they are no longer physically present in the United States. DHS also identifies individuals as possible overstays if there are no records of a departure or change in status[10] prior to the end of their authorized admission period (i.e., Suspected In-Country Overstays).

In this report, the Department presents ADIS system-generated overstay rates by country of citizenship for nonimmigrant visitors for business or pleasure[11] who were admitted to the United States through an air or sea[12] POE, regardless of overstay type. These classes of admission made up 85 percent of the total number of visits by nonimmigrants who arrived by air or sea and who were expected to depart in FY 2015. While significant progress has been made, challenges remain with integration of systems used in the travel continuum for reporting on visa categories beyond business or pleasure. In light of these and other data limitations, DHS is in the process of evaluating whether and to what extent the data presented in this report will be used to make decisions on VWP country designations. Enhancements are currently underway focusing on the remaining visa categories, most notably starting with student visitor classes (F, M and J visas). Subsequent annual Entry/Exit Overstay Reports expect to include additional classes of visitors to the United States as integration of these systems progress.

[9] In these cases, DHS sanctions the individual who overstayed their authorized period of stay in the U.S. according to existing immigration law, which is based on a sliding scale of penalties depending on the length of time unlawfully present in the United States. See, e.g., 8 U.S.C. § 1202(g) (nonimmigrant visa is voided at conclusion of authorized period of stay, if an individual remains in the United States beyond the authorized period); 8 U.S.C. § 1187(a)(7) (referring to VWP, "if the alien previously was admitted without a visa under this section, the alien must not have failed to comply with the conditions of any previous admission as such a nonimmigrant"); and 8 U.S.C. § 1182(a)(9)(B)(i)(I) and (II) (alien inadmissible for 3 years if unlawfully present for more than 180 days but less than a year; alien inadmissible for 10 years if unlawfully present for a year or more, pursuant to various provisions of the Immigration and Nationality Act).

[10] Pending immigration benefit applications and approved extensions of stay, change of nonimmigrant status, or adjustment of status to lawful permanent residence may extend the authorized period of stay. For example, upon entering the United States a person may be granted a six-month period of admission, but thereafter lawfully change immigration status prior to the expiration of that period, and in turn be authorized to stay beyond the initial six months. Generally, these options are not available to those who enter under VWP. 8 C.F.R. § 245.1(a)(8); 8 C.F.R. § 248.2(a)(6).

[11] Visitors for business or pleasure include the following classes of admission: visitor for business (B-1), visitor for pleasure (B-2), visa waiver visitor for business (WB), and visa waiver visitor for pleasure (WT).

[12] The sea overstay rates are only reflective of the population that initially entered the United States through a sea POE but is not reflective of all traveler arrivals where the vessel both departs from and subsequently arrives at the same location (commonly referred to as "closed loop" cruises.) For example, if a foreign national already within the United States departs from the Port Canaveral, Florida Seaport for a seven day cruise in the Caribbean and subsequently re-enters at Port Canaveral, then that arrival would not be taken into account for the purposes of this report.

D. Overstay Identification and Action

CBP maintains arrival/departure information for all foreign nationals based on border crossings and carrier data. This information is used to generate daily overstay lists. These system-generated overstay lists are sent for checks against the CBP Automated Targeting System (ATS) and the U.S. Citizenship and Immigration Services CLAIMS3 database, reducing the overall list size by providing additional checks and identifying persons who have departed the United States or changed into another nonimmigrant or immigrant status. The ATS then applies screening rules, as defined by U.S. Immigration and Customs Enforcement (ICE), to prioritize system-identified overstays. This creates a prioritized overstay list which is sent to ICE.

The Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU) at ICE is dedicated to the enforcement of nonimmigrant visa violations. Each year, CTCEU analyzes records of hundreds of thousands of potential status violators from various investigative databases and DHS entry/exit registration systems. To better manage investigative resources, CTCEU relies on a prioritization framework for these leads established in consultation with interagency partners within the national intelligence and federal law enforcement communities. Those identified as posing a potential national security threat to the United States are prioritized and referred to ICE HSI field offices for investigation. Leads that do not meet national security criteria for ICE HSI are referred to ICE’s Enforcement and Removal Operations.

HSI Special Agents and analysts continuously monitor threat reports and proactively address emergent issues. This practice has contributed to ICE’s counterterrorism mission by initiating or supporting high-priority national security initiatives based upon specific intelligence. The goal is to identify, locate, prosecute where applicable, and remove those overstays posing real or potential national security threats to the United States. This is accomplished through both broad intelligence-driven criteria on subjects that exhibit similar characteristics of known radical organizations and their participants and by activity which focuses ICE investigations on those subjects that are considered to pose a higher risk to national security.

Pursuant to DHS immigration enforcement priorities, ICE Enforcement and Removal Operations (ERO) will review and take appropriate enforcement action derived from information gained from the DHS data. Additionally, ERO also encounters overstays who meet a DHS priority via its enforcement programs such as Fugitive Operations and the Criminal Alien Program.

In January 2012, CTCEU initiated the use of the National Counterterrorism Center (NCTC) in support of its Overstay Program to screen overstays by identifying potential matches to derogatory intelligence community holdings.

III. Overstay Rates

Tables 1 and 2 below present the overstay rates for countries that participate in the Visa Waiver Program (VWP) (Table 1) and countries that do not (Table 2). Table 3 includes nationals of Canada and Mexico only. It is important to note that the total number of FY 2015 overstays, as identified in this report, does not equal the total number of FY 2015 overstays that currently remain in the United States. That number is likely lower. This is because foreign nationals identified as possible overstays can and do subsequently depart the United States, or have been found to have adjusted their lawful status. For purposes of this report, these are still considered overstays.

For all charts, "Expected Departures" is the number of travelers from each country that were admitted to the United States as a nonimmigrant and whose expected departure date occurred within FY 2015. "Out-of-Country Overstays" refers to cases in which the Department received a departure record for a traveler, and the record indicated that the traveler departed after the authorized period of admission expired. "Suspected In-Country Overstays" refers to cases in which DHS has no departure record, or any other encounter indicating the traveler departed in FY 2015, and no evidence that the person transitioned into a lawful immigration status. The "Overstay Rate" is the percentage of travelers from each country who overstayed their period of admission to the United States, regardless of type.[13]

These charts represent data from FY 2015 only. The Department determined that there were a total of 44,928,381 nonimmigrant admissions to the United States for business or pleasure through air or sea POEs that were expected to depart in FY 2015. Of this number, the Department calculated a total overstay rate of 1.17 percent, or 527,127 individuals. In other words, 98.83 percent had left the United States on time and abided by the terms of their admission.

At the end of FY 2015, Suspected In-Country Overstays were 482,781 individuals, with a Suspected In-Country Overstay rate of 1.07 percent. This data indicates that 98.93 percent had departed the United States or transitioned to a lawful immigration status.

Upon finalizing this report, DHS identified approximately 66,500 travelers who are listed in this report as Suspected In-Country Overstays, but have subsequently departed the United States as of January 4, 2016. Therefore, as of January 4, 2016, the Department identified approximately 416,500 Suspected In-Country Overstays or a revised FY 2015 Suspected In-Country Overstay rate of 0.9 percent. In other words, as of January 4, 2016, DHS has been able to confirm the

[13] Rates are shown for countries as well as passport-issuing authorities and places of origin recognized by the United States. With respect to all references to "country" or "countries" in this document, section 4(b)(1) of the Taiwan Relations Act of 1979 (Pub. L. No. 96-8), provides that "[w]henever the laws of the United States refer or relate to foreign countries, nations, states, governments, or similar entities, such terms shall include and such laws shall apply with respect to Taiwan." 22 U.S.C. § 3303(b)(1). Accordingly, references to "country" or "countries" in the VWP authorizing legislation, section 217 of the Immigration and Nationality Act (8 U.S.C. § 1187), are read to include Taiwan. This is consistent with the United States' one-China policy, under which the United States has maintained unofficial relations with Taiwan since 1979. Taiwan entered the VWP on October 2, 2012.

departures of more than 99 percent of nonimmigrant visitors scheduled to depart in FY 2015 via air and sea POEs, and that number continues to grow.

For VWP countries, the FY 2015 Suspected In-Country Overstay rate is 0.65 percent of the 20,974,390 expected departures. For non-VWP countries, the FY 2015 Suspected In-Country Overstay rate is 1.60 percent of the 13,182,807 expected departures.

For Canada and Mexico the FY 2015 Suspected In-Country Overstay rate is 1.18 percent of the 7,875,054 expected departures and 1.45 percent of the 2,896,130 expected departures respectively.

Table 1

FY 2015 Overstay rates for nonimmigrant visitors admitted to the United States for business or pleasure (WB/WT/B-1/B-2) via air and sea POEs for VWP Countries[14,15]

Country of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
Andorra	1,221	2	3	5	0.41%	0.24%
Australia	1,306,352	878	3,964	4,842	0.37%	0.30%
Austria	210,854	119	2,694	2,813	1.33%	1.28%
Belgium	290,103	158	1,477	1,635	0.56%	0.51%
Brunei	1,143	1	10	11	0.96%	0.87%
Chile	306,598	584	6,553	7,137	2.33%	2.14%
Czech Republic	97,708	186	1,422	1,608	1.65%	1.46%
Denmark	326,334	158	1,812	1,970	0.60%	0.56%
Estonia	20,247	43	191	234	1.16%	0.94%
Finland	153,136	91	747	838	0.55%	0.49%
France	1,767,377	1,434	11,973	13,407	0.76%	0.68%
Germany	2,107,035	1,160	21,394	22,554	1.07%	1.02%
Greece	71,430	320	1,333	1,653	2.31%	1.87%
Hungary	75,904	356	1,860	2,216	2.92%	2.45%
Iceland	51,231	36	199	235	0.46%	0.39%
Ireland	453,597	316	1,797	2,113	0.47%	0.40%

[14] Effective January 12, 2009, citizens or nationals from VWP countries are required to obtain an approved travel authorization via ESTA to be eligible to travel to the United States by air or sea under the VWP. Upon admission into the United States, visitors are classified either under a WT (waiver-tourist) or a WB (waiver-business) status.

[15] Citizens or nationals of VWP countries may also obtain and travel to the United States on a B-1/B-2 visa and seek admission under the B-1 or B-2 nonimmigrant classification.

Table 1

FY 2015 Overstay rates for nonimmigrant visitors admitted to the United States for business or pleasure (WB/WT/B-1/B-2) via air and sea POEs for VWP Countries[14,15]

Country of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
Italy	1,184,715	1,336	17,661	18,997	1.60%	1.49%
Japan	3,014,769	455	5,603	6,058	0.20%	0.19%
Korea, South	1,121,890	1,352	7,120	8,472	0.76%	0.63%
Latvia	18,698	86	273	359	1.92%	1.46%
Liechtenstein	2,048	2	12	14	0.68%	0.59%
Lithuania	26,502	102	480	582	2.20%	1.81%
Luxembourg	14,279	7	75	82	0.57%	0.53%
Malta	5,504	3	44	47	0.85%	0.80%
Monaco	1,136	1	4	5	0.44%	0.35%
Netherlands	709,633	461	7,723	8,184	1.15%	1.09%
New Zealand	298,093	245	1,206	1,451	0.49%	0.40%
Norway	312,600	193	1,230	1,423	0.46%	0.39%
Portugal	165,533	500	3,322	3,822	2.31%	2.01%
San Marino	702	0	16	16	2.28%	2.28%
Singapore	127,804	106	375	481	0.38%	0.29%
Slovakia	44,274	116	927	1,043	2.36%	2.09%
Slovenia	23,669	43	235	278	1.17%	0.99%
Spain	896,833	1,668	10,891	12,559	1.40%	1.21%
Sweden	576,422	354	2,428	2,782	0.48%	0.42%
Switzerland	438,910	279	2,123	2,402	0.55%	0.48%
Taiwan	356,225	704	1,184	1,888	0.53%	0.33%
United Kingdom	4,393,881	2,504	16,446	18,950	0.43%	0.37%
TOTAL	**20,974,390**	**16,359**	**136,807**	**153,166**	**0.73%**	**0.65%**

Table 2

FY 2015 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries (excluding Canada and Mexico)

Country Of Citizenship	Expected Departures	Out–of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
Afghanistan	2,136	13	219	232	10.86%	10.25%
Albania	6,123	24	183	207	3.38%	2.99%
Algeria	9,353	53	240	293	3.13%	2.57%
Angola	10,987	25	268	293	2.67%	2.44%
Antigua and Barbuda	13,485	29	204	233	1.73%	1.51%
Argentina	690,275	237	7,498	7,735	1.12%	1.09%
Armenia	5,962	11	195	206	3.46%	3.27%
Azerbaijan	5,758	8	72	80	1.39%	1.25%
Bahamas, The	220,305	232	1,510	1,742	0.79%	0.69%
Bahrain	7,003	12	68	80	1.14%	0.97%
Bangladesh	28,888	96	1,147	1,243	4.30%	3.97%
Barbados	53,643	57	310	367	0.68%	0.58%
Belarus	11,996	21	229	250	2.08%	1.91%
Belize	24,029	43	531	574	2.39%	2.21%
Benin	2,016	16	129	145	7.19%	6.40%
Bhutan	442	4	106	110	24.89%	23.98%
Bolivia	52,795	54	1,118	1,172	2.22%	2.12%
Bosnia and Herzegovina	6,762	21	146	167	2.47%	2.16%
Botswana	1,832	2	16	18	0.98%	0.87%
Brazil	2,350,140	1,284	35,707	36,991	1.57%	1.52%
Bulgaria	26,311	69	389	458	1.74%	1.48%
Burkina Faso	3,765	24	654	678	18.01%	17.37%
Burma	4,057	15	114	129	3.18%	2.81%
Burundi	863	2	81	83	9.62%	9.39%
Cabo Verde	4,295	10	276	286	6.66%	6.43%
Cambodia	2,497	9	46	55	2.20%	1.84%
Cameroon	7,779	77	607	684	8.79%	7.80%
Central African Republic	160	0	11	11	6.88%	6.88%
Chad	677	14	104	118	17.43%	15.36%
China	1,763,669	2,554	15,692	18,246	1.04%	0.89%
Colombia	935,500	721	16,434	17,155	1.83%	1.76%

Table 2

FY 2015 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries (excluding Canada and Mexico)

Country Of Citizenship	Expected Departures	Out–of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
Comoros	135	0	3	3	2.22%	2.22%
Congo (Brazzaville)	1,323	5	86	91	6.88%	6.50%
Congo (Kinshasa)	5,003	23	427	450	9.00%	8.53%
Costa Rica	224,101	123	1,986	2,109	0.94%	0.89%
Croatia	20,781	32	194	226	1.09%	0.93%
Cuba	46,826	170	895	1,065	2.27%	1.91%
Cyprus	8,357	19	94	113	1.35%	1.12%
Côte d'Ivoire	5,337	35	216	251	4.70%	4.05%
Djibouti	347	3	93	96	27.67%	26.80%
Dominica	6,830	11	258	269	3.94%	3.78%
Dominican Republic	303,095	316	6,990	7,306	2.41%	2.31%
Ecuador	348,064	260	5,612	5,872	1.69%	1.61%
Egypt	74,705	175	1,245	1,420	1.90%	1.67%
El Salvador	137,535	166	3,118	3,284	2.39%	2.27%
Equatorial Guinea	1,212	11	39	50	4.13%	3.22%
Eritrea	2,339	69	382	451	19.28%	16.33%
Ethiopia	14,296	122	492	614	4.30%	3.44%
Fiji	7,361	26	142	168	2.28%	1.93%
Gabon	1,862	12	108	120	6.45%	5.80%
Gambia, The	1,795	20	181	201	11.20%	10.08%
Georgia	6,561	13	803	816	12.44%	12.24%
Ghana	21,846	106	894	1,000	4.58%	4.09%
Grenada	9,109	26	236	262	2.88%	2.59%
Guatemala	236,043	296	5,419	5,715	2.42%	2.30%
Guinea	2,200	19	175	194	8.82%	7.95%
Guinea-Bissau	133	0	6	6	4.51%	4.51%
Guyana	41,747	63	920	983	2.36%	2.20%
Haiti	121,581	559	3,312	3,871	3.18%	2.72%
Holy See	22	0	0	0	0.00%	0.00%
Honduras	161,467	204	4,075	4,279	2.65%	2.52%
India	881,974	1,463	12,885	14,348	1.63%	1.46%
Indonesia	84,103	94	922	1,016	1.21%	1.10%

Table 2

FY 2015 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries (excluding Canada and Mexico)

Country Of Citizenship	Expected Departures	Out–of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
Iran	24,997	122	564	686	2.74%	2.26%
Iraq	11,147	93	681	774	6.94%	6.11%
Israel	352,627	346	2,375	2,721	0.77%	0.67%
Jamaica	240,126	338	6,614	6,952	2.90%	2.75%
Jordan	33,286	179	1,397	1,576	4.74%	4.20%
Kazakhstan	17,301	38	409	447	2.58%	2.36%
Kenya	18,336	87	475	562	3.07%	2.59%
Kiribati	119	1	1	2	1.68%	0.84%
Korea, North	29	0	1	1	3.45%	3.45%
Kuwait	45,762	344	913	1,257	2.75%	2.00%
Kyrgyzstan	2,128	10	148	158	7.43%	6.95%
Laos	1,513	27	252	279	18.44%	16.66%
Lebanon	39,438	76	930	1,006	2.55%	2.36%
Lesotho	286	0	6	6	2.10%	2.10%
Liberia	4,575	134	412	546	11.93%	9.01%
Libya	1,245	13	56	69	5.54%	4.50%
Macedonia	6,014	24	226	250	4.16%	3.76%
Madagascar	872	1	7	8	0.92%	0.80%
Malawi	1,685	6	74	80	4.75%	4.39%
Malaysia	80,451	94	1,430	1,524	1.89%	1.78%
Maldives	243	0	1	1	0.41%	0.41%
Mali	2,801	16	154	170	6.07%	5.50%
Marshall Islands	52	1	2	3	5.77%	3.85%
Mauritania	1,371	12	173	185	13.49%	12.62%
Mauritius	3,094	4	27	31	1.00%	0.87%
Micronesia, Federated States of	25	0	4	4	16.00%	16.00%
Moldova	7,230	19	359	378	5.23%	4.97%
Mongolia	9,972	29	302	331	3.32%	3.03%
Montenegro	3,972	13	148	161	4.05%	3.73%
Morocco	24,695	66	390	456	1.85%	1.58%
Mozambique	1,849	2	36	38	2.06%	1.95%
Namibia	1,560	4	10	14	0.90%	0.64%
Nauru	23	0	0	0	0.00%	0.00%

Table 2

FY 2015 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries (excluding Canada and Mexico)

Country Of Citizenship	Expected Departures	Out–of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
Nepal	15,332	72	492	564	3.68%	3.21%
Nicaragua	58,759	78	1,167	1,245	2.12%	1.99%
Niger	760	7	25	32	4.21%	3.29%
Nigeria	183,907	627	6,781	7,408	4.03%	3.69%
Oman	5,067	16	41	57	1.13%	0.81%
Pakistan	71,803	180	1,435	1,615	2.25%	2.00%
Palau	55	0	2	2	3.64%	3.64%
Panama	144,320	133	773	906	0.63%	0.54%
Papua New Guinea	686	6	2	8	1.17%	0.29%
Paraguay	28,781	22	466	488	1.70%	1.62%
Peru	268,000	312	4,550	4,862	1.81%	1.70%
Philippines	226,777	436	3,265	3,701	1.63%	1.44%
Poland	171,243	204	2,345	2,549	1.49%	1.37%
Qatar	13,909	68	108	176	1.27%	0.78%
Romania	63,850	165	1,153	1,318	2.06%	1.81%
Russia	289,059	239	2,705	2,944	1.02%	0.94%
Rwanda	2,652	18	92	110	4.15%	3.47%
Saint Kitts and Nevis	11,387	17	237	254	2.23%	2.08%
Saint Lucia	14,100	33	363	396	2.81%	2.57%
Saint Vincent and the Grenadines	9,097	29	335	364	4.00%	3.68%
Samoa	1,856	15	110	125	6.74%	5.93%
Sao Tome and Principe	36	0	0	0	0.00%	0.00%
Saudi Arabia	139,483	544	965	1,509	1.08%	0.69%
Senegal	7,786	23	269	292	3.75%	3.45%
Serbia	20,149	40	336	376	1.87%	1.67%
Seychelles	275	1	2	3	1.09%	0.73%
Sierra Leone	2,824	63	86	149	5.28%	3.05%
Solomon Islands	140	0	0	0	0.00%	0.00%
Somalia	144	2	2	4	2.78%	1.39%
South Africa	120,220	139	974	1,113	0.93%	0.81%

Table 2

FY 2015 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries (excluding Canada and Mexico)

Country Of Citizenship	Expected Departures	Out–of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
South Sudan	235	4	7	11	4.68%	2.98%
Sri Lanka	16,391	34	439	473	2.89%	2.68%
Sudan	3,734	34	278	312	8.36%	7.45%
Suriname	13,111	7	93	100	0.76%	0.71%
Swaziland	626	5	12	17	2.72%	1.92%
Syria	13,430	57	440	497	3.70%	3.28%
Tajikistan	953	7	44	51	5.35%	4.62%
Tanzania	5,711	38	127	165	2.89%	2.22%
Thailand	83,482	172	1,349	1,521	1.82%	1.62%
Timor-Leste	39	0	1	1	2.56%	2.56%
Togo	1,715	15	133	148	8.63%	7.76%
Tonga	2,398	13	150	163	6.80%	6.26%
Trinidad and Tobago	170,215	107	873	980	0.58%	0.51%
Tunisia	8,436	15	135	150	1.78%	1.60%
Turkey	161,878	238	2,227	2,465	1.52%	1.38%
Turkmenistan	1,039	6	52	58	5.58%	5.00%
Tuvalu	43	0	1	1	2.33%	2.33%
Uganda	6,761	34	259	293	4.33%	3.83%
Ukraine	73,230	185	2,299	2,484	3.39%	3.14%
United Arab Emirates	30,623	204	393	597	1.95%	1.28%
Uruguay	76,856	41	1,880	1,921	2.50%	2.45%
Uzbekistan	8,008	34	502	536	6.69%	6.27%
Vanuatu	106	0	2	2	1.89%	1.89%
Venezuela	574,651	487	12,242	12,729	2.22%	2.13%
Vietnam	72,732	394	2,285	2,679	3.68%	3.14%
Yemen	3,537	28	219	247	6.98%	6.19%
Zambia	3,434	14	73	87	2.53%	2.13%
Zimbabwe	6,559	19	140	159	2.42%	2.13%
TOTAL	**13,182,807**	**17,958**	**210,825**	**228,783**	**1.74%**	**1.60%**

Table 3

FY 2015 Overstay rates for Canadian and Mexican nonimmigrants admitted to the United States for business or pleasure via air and sea POEs

Country of Citizenship	Expected Departures	Out–of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Total Overstay Rate	Suspected In-Country Overstay Rate
Canada	7,875,054	6,871	93,035	99,906	1.27%	1.18%
Mexico	2,896,130	3,158	42,114	45,272	1.56%	1.45%
TOTAL	**10,771,184**	**10,029**	**135,149**	**145,178**	**1.34%**	**1.25%**

This chart represents Canadian and Mexican nonimmigrant visitors for business or pleasure admitted at air or sea POEs who were expected to depart in FY 2015. Canada and Mexico have relatively high proportions of travelers who are admitted to the United States at land POEs. Unlike all other countries, over 95 percent of travelers from Canada or Mexico enter the United States by land. As mentioned, overstay data concerning land entries will be incorporated into future iterations of this report as projects progress.

IV. Conclusion

Identifying overstays is important for national security, public safety, immigration enforcement, and immigration benefit application processing.

Over the years, the Department has significantly improved the process and data collection for the entry process—collecting data on all admissions to the United States by foreign nationals, reducing the number of documents that are usable for entry to the United States, collecting biometric data on most foreign travelers to the United States, and checking that data against criminal and terrorist watchlists. Despite the different structure of the exit process, the Department has been able to resolve many of the issues regarding the collection of departure information from foreign nationals. Further efforts, including partnerships with other governments and the private sector (e.g., airlines, airports, cruise lines, etc.), are ongoing and will continue to improve the existing process for improved data integrity.

During the past two years, DHS has made significant progress in terms of its ability to accurately report data on overstays—progress that was made possible by congressional realignment of Department resources in order to better centralize the overall mission in identifying overstays. The Department will continue to roll out additional pilot programs during FY 2016, both biometric and biographic, that will improve the ability of CBP to accurately collect and report this data. DHS looks forward to continuing to update congressional members and staffs on its progress.

V. Appendix

Fiscal Year (FY) 2014 VWP, non-VWP, Mexico and Canada Overstay Tables

The ability to accurately and reliably estimate overstay rates is dependent on the completeness and accuracy of arrival and departure records. During the generation of the FY 2014 overstay data, DHS identified significant discrepancies regarding the data received from certain air carriers, which resulted in artificially elevated overstay rates, especially for the Netherlands, Italy, and San Marino. The nature of these errors is described in more detail below. Given the serious concerns raised with respect to the accuracy and reliability of the FY 2014 data, DHS determined that a FY 2014 report should not be issued.

These data quality issues have since been resolved, and the FY 2015 Entry/Exit Overstay Report tables are an accurate depiction of country-by-country overstay numbers for these categories of travelers. The FY 2014 data included in this Appendix is provided solely to provide transparency with regard to DHS processing of overstay data.

This Appendix contains data on departures and overstays, by country, for foreign visitors to the United States who were expected to depart in FY 2014 (October 1, 2013-September 30, 2014). The data in this Appendix is presented in the same format as the data presented in the FY 2015 Entry/Exit Overstay Report (to which this Appendix is attached).

As mentioned, U.S. Customs and Border Protection’s (CBP) departure data primarily comes from passenger manifests for international flights, provided by the airline carriers. In some cases in FY 2014, it was apparent that there were errors in these manifests that contributed to larger errors in the FY 2014 Entry/Exit Overstay Report. Air carriers KLM (Royal Dutch Airlines) and Emirates had disproportionately high instances of passengers listed as “not on board” departing flights, despite the passengers having checked in for the flight.

Although CBP believes that a majority of these passengers were in fact aboard the flights, it should be noted that CBP cannot confirm this with absolute certainty as there is no record of the passengers’ travel in the final departure manifest. CBP receives data from the carriers at multiple points in the arrival and departure process to best ensure data completeness. Since carriers provide manifest information well before a traveler actually boards the aircraft, CBP must rely on the carriers to identify which passengers boarded the aircraft and which did not at the time of the actual departure.

The Department concluded that these errors could erroneously identify certain VWP countries as having significant overstay rates, which could impact their ability to remain in the program. The FY 2015 data, which are now available, confirmed that these data errors have been corrected.

Because of the significant data errors for FY 2014, none of the overstay percentages for FY 2014 will be used to make any decisions as to whether any country will remain in the VWP.

Table 1

FY 2014 Overstay rates for nonimmigrant visitors admitted to the United States for business or pleasure (WB/WT/B-1/B-2) via air and sea POEs for VWP Countries

Country of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Overstay Rate	Suspected In-Country Overstay Rate
Andorra	1,215	1	5	6	0.49%	0.41%
Australia	1,273,201	907	4,721	5,628	0.44%	0.37%
Austria	213,380	124	1,681	1,805	0.85%	0.79%
Belgium	291,453	182	3,540	3,722	1.28%	1.21%
Brunei	1,317	-	20	20	1.52%	1.52%
Chile	241,828	235	3,673	3,908	1.62%	1.52%
Czech Republic	94,274	202	1,696	1,898	2.01%	1.80%
Denmark	303,053	171	5,352	5,523	1.82%	1.77%
Estonia	20,700	52	354	406	1.96%	1.71%
Finland	153,091	94	1,355	1,449	0.95%	0.89%
France	1,782,939	1,614	26,864	28,478	1.60%	1.51%
Germany	2,049,501	1,329	15,992	17,321	0.85%	0.78%
Greece	70,071	427	1,416	1,843	2.63%	2.02%
Hungary	71,335	376	2,320	2,696	3.78%	3.25%
Iceland	51,415	30	120	150	0.29%	0.23%
Ireland	448,556	352	1,940	2,292	0.51%	0.43%
Italy	1,166,428	1,360	31,164	32,524	2.79%	2.67%
Japan	3,069,506	414	6,149	6,563	0.21%	0.20%
Korea, South	1,023,581	1,404	9,729	11,133	1.09%	0.95%
Latvia	17,473	100	316	416	2.38%	1.81%
Liechtenstein	2,024	2	12	14	0.69%	0.59%
Lithuania	24,775	93	468	561	2.26%	1.89%
Luxembourg	14,396	3	264	267	1.85%	1.83%
Malta	5,786	11	58	69	1.19%	1.00%
Monaco	1,018	-	30	30	2.95%	2.95%
Netherlands	702,670	489	30,596	31,085	4.42%	4.35%
New Zealand	278,394	255	1,074	1,329	0.48%	0.39%
Norway	304,916	184	4,473	4,657	1.53%	1.47%
Portugal	164,499	525	3,383	3,908	2.38%	2.06%
San Marino	761	-	48	48	6.31%	6.31%
Singapore	127,267	102	540	642	0.50%	0.42%
Slovakia	41,645	115	724	839	2.01%	1.74%
Slovenia	21,122	33	255	288	1.36%	1.21%
Spain	867,187	1,734	11,969	13,703	1.58%	1.38%
Sweden	552,708	374	5,700	6,074	1.10%	1.03%
Switzerland	437,076	273	3,319	3,592	0.82%	0.76%

Taiwan	331,503	567	1,639	2,206	0.67%	0.49%
United Kingdom	4,216,065	2,636	17,914	20,550	0.49%	0.42%
TOTAL	**20,438,129**	**16,770**	**200,873**	**217,643**	**1.06%**	**0.98%**

Table 2

FY 2014 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries

Country Of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Overstay Rate	Suspected In-Country Overstays
Afghanistan	1,374	7	146	153	11.14%	10.63%
Albania	5,695	23	200	223	3.92%	3.51%
Algeria	7,640	25	149	174	2.28%	1.95%
Angola	9,967	29	247	276	2.77%	2.48%
Antigua and Barbuda	13,494	25	283	308	2.28%	2.10%
Argentina	720,391	193	9,214	9,407	1.31%	1.28%
Armenia	5,488	18	153	171	3.12%	2.79%
Azerbaijan	4,876	12	113	125	2.56%	2.32%
Bahamas, The	211,681	221	1,151	1,372	0.65%	0.54%
Bahrain	6,197	15	66	81	1.31%	1.07%
Bangladesh	23,000	69	1,726	1,795	7.80%	7.50%
Barbados	52,949	35	252	287	0.54%	0.48%
Belarus	10,968	19	166	185	1.69%	1.51%
Belize	22,507	49	421	470	2.09%	1.87%
Benin	1,829	4	102	106	5.80%	5.58%
Bhutan	281	2	55	57	20.29%	19.57%
Bolivia	46,025	62	817	879	1.91%	1.78%
Bosnia and Herzegovina	5,807	22	96	118	2.03%	1.65%
Botswana	1,507	2	25	27	1.79%	1.66%
Brazil	2,129,716	1,226	27,563	28,789	1.35%	1.29%
Bulgaria	24,629	79	415	494	2.01%	1.69%
Burkina Faso	2,643	17	258	275	10.41%	9.76%
Burma	2,946	9	55	64	2.17%	1.87%
Burundi	816	2	105	107	13.11%	12.87%
Cabo Verde	3,633	7	140	147	4.05%	3.85%
Cambodia	3,246	7	61	68	2.10%	1.88%
Cameroon	6,538	32	342	374	5.72%	5.23%
Central African Republic	177	1	13	14	7.91%	7.34%
Chad	499	1	45	46	9.22%	9.02%

Table 2
FY 2014 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries

Country Of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Overstay Rate	Suspected In-Country Overstays
China	1,436,742	2,214	15,792	18,006	1.25%	1.10%
Colombia	809,836	751	12,810	13,561	1.68%	1.58%
Comoros	88	-	-	0	0.00%	0.00%
Congo (Brazzaville)	1,106	7	53	60	5.43%	4.79%
Congo (Kinshasa)	3,975	29	269	298	7.50%	6.77%
Costa Rica	200,780	155	1,716	1,871	0.93%	0.85%
Croatia	18,600	37	163	200	1.08%	0.88%
Cuba	34,978	357	1,707	2,064	5.90%	4.88%
Cyprus	7,465	23	152	175	2.34%	2.04%
Côte d'Ivoire	4,938	20	169	189	3.83%	3.42%
Djibouti	206	1	56	57	27.67%	27.18%
Dominica	7,096	11	236	247	3.48%	3.33%
Dominican Republic	254,043	284	5,319	5,603	2.21%	2.09%
Ecuador	275,532	198	3,409	3,607	1.31%	1.24%
Egypt	70,690	264	1,715	1,979	2.80%	2.43%
El Salvador	111,752	121	1,743	1,864	1.67%	1.56%
Equatorial Guinea	1,001	11	42	53	5.30%	4.20%
Eritrea	1,528	71	211	282	18.46%	13.81%
Ethiopia	13,122	115	644	759	5.78%	4.91%
Fiji	6,795	20	133	153	2.25%	1.96%
Gabon	1,776	8	49	57	3.21%	2.76%
Gambia, The	2,005	17	223	240	11.97%	11.12%
Georgia	4,666	11	420	431	9.24%	9.00%
Ghana	21,719	97	887	984	4.53%	4.08%
Grenada	8,782	37	216	253	2.88%	2.46%
Guatemala	215,219	263	4,756	5,019	2.33%	2.21%
Guinea	1,607	12	116	128	7.97%	7.22%
Guinea-Bissau	117	1	8	9	7.69%	6.84%
Guyana	31,977	47	532	579	1.81%	1.66%
Haiti	101,151	521	2,270	2,791	2.76%	2.24%
Holy See	18	-	-	0	0.00%	0.00%
Honduras	148,665	169	3,376	3,545	2.39%	2.27%
India	766,936	1,254	10,399	11,653	1.52%	1.36%
Indonesia	79,171	89	888	977	1.23%	1.12%

Table 2

FY 2014 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries

Country Of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Overstay Rate	Suspected In-Country Overstays
Iran	16,429	85	441	526	3.20%	2.68%
Iraq	9,855	91	602	693	7.03%	6.11%
Israel	322,281	362	2,371	2,733	0.85%	0.74%
Jamaica	197,858	249	4,155	4,404	2.23%	2.10%
Jordan	26,022	117	912	1,029	3.95%	3.50%
Kazakhstan	15,070	36	628	664	4.41%	4.17%
Kenya	15,225	82	483	565	3.71%	3.17%
Kiribati	141	-	-	0	0.00%	0.00%
Korea, North	37	-	-	0	0.00%	0.00%
Kuwait	36,826	208	958	1,166	3.17%	2.60%
Kyrgyzstan	2,891	27	548	575	19.89%	18.96%
Laos	2,119	45	509	554	26.14%	24.02%
Lebanon	34,317	90	918	1,008	2.94%	2.68%
Lesotho	289	-	8	8	2.77%	2.77%
Liberia	3,420	67	296	363	10.61%	8.65%
Libya	1,368	6	76	82	5.99%	5.56%
Macedonia	5,328	18	216	234	4.39%	4.05%
Madagascar	694	-	14	14	2.02%	2.02%
Malawi	1,483	2	53	55	3.71%	3.57%
Malaysia	80,411	90	1,392	1,482	1.84%	1.73%
Maldives	193	-	5	5	2.59%	2.59%
Mali	2,972	12	212	224	7.54%	7.13%
Marshall Islands	80	4	2	6	7.50%	2.50%
Mauritania	1,038	4	105	109	10.50%	10.12%
Mauritius	2,633	3	28	31	1.18%	1.06%
Micronesia, Federated States of	29	2	1	3	10.35%	3.45%
Moldova	6,703	31	292	323	4.82%	4.36%
Mongolia	9,077	35	107	142	1.56%	1.18%
Montenegro	3,214	8	76	84	2.61%	2.36%
Morocco	22,700	78	473	551	2.43%	2.08%
Mozambique	1,637	5	24	29	1.77%	1.47%
Namibia	1,510	2	27	29	1.92%	1.79%
Nauru	13	-	-	0	0.00%	0.00%
Nepal	11,895	39	414	453	3.81%	3.48%
Nicaragua	53,654	80	830	910	1.70%	1.55%
Niger	765	5	28	33	4.31%	3.66%

Table 2

FY 2014 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries

Country Of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Overstay Rate	Suspected In-Country Overstays
Nigeria	150,307	510	4,079	4,589	3.05%	2.71%
Oman	4,120	18	60	78	1.89%	1.46%
Pakistan	55,551	141	1,232	1,373	2.47%	2.22%
Palau	37	-	2	2	5.41%	5.41%
Panama	138,963	109	658	767	0.55%	0.47%
Papua New Guinea	719	-	7	7	0.97%	0.97%
Paraguay	26,131	32	479	511	1.96%	1.83%
Peru	239,498	291	2,823	3,114	1.30%	1.18%
Philippines	197,513	467	2,978	3,445	1.74%	1.51%
Poland	152,845	228	2,327	2,555	1.67%	1.52%
Qatar	11,926	91	155	246	2.06%	1.30%
Romania	57,059	166	1,343	1,509	2.65%	2.35%
Russia	325,039	268	2,395	2,663	0.82%	0.74%
Rwanda	2,105	8	99	107	5.08%	4.70%
Saint Kitts and Nevis	10,667	19	224	243	2.28%	2.10%
Saint Lucia	13,429	25	319	344	2.56%	2.38%
Saint Vincent and the Grenadines	8,602	26	320	346	4.02%	3.72%
Samoa	1,685	13	76	89	5.28%	4.51%
Sao Tome and Principe	54	-	-	0	0.00%	0.00%
Saudi Arabia	110,985	401	1,170	1,571	1.42%	1.05%
Senegal	7,927	36	293	329	4.15%	3.70%
Serbia	17,422	33	295	328	1.88%	1.69%
Seychelles	276	1	1	2	0.73%	0.36%
Sierra Leone	2,509	19	118	137	5.46%	4.70%
Solomon Islands	163	-	3	3	1.84%	1.84%
Somalia	100	2	3	5	5.00%	3.00%
South Africa	115,482	144	992	1,136	0.98%	0.86%
South Sudan	143	-	2	2	1.40%	1.40%
Sri Lanka	13,935	30	458	488	3.50%	3.29%
Sudan	2,685	14	214	228	8.49%	7.97%
Suriname	10,872	5	52	57	0.52%	0.48%
Swaziland	598	1	7	8	1.34%	1.17%
Syria	13,297	144	720	864	6.50%	5.41%

Table 2
FY 2014 Overstay rates for nonimmigrants with B-1/B-2 visas admitted to the United States for business or pleasure via air and sea POEs for non-VWP Countries

Country Of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Overstay Rate	Suspected In-Country Overstays
Tajikistan	849	7	29	36	4.24%	3.42%
Tanzania	4,556	29	104	133	2.92%	2.28%
Thailand	78,810	105	1,278	1,383	1.76%	1.62%
Timor-Leste	26	-	-	0	0.00%	0.00%
Togo	1,455	8	93	101	6.94%	6.39%
Tonga	1,880	5	74	79	4.20%	3.94%
Trinidad and Tobago	146,970	94	694	788	0.54%	0.47%
Tunisia	8,062	15	167	182	2.26%	2.07%
Turkey	152,041	185	2,802	2,987	1.97%	1.84%
Turkmenistan	913	3	47	50	5.48%	5.15%
Tuvalu	47	1	-	1	2.13%	0.00%
Uganda	6,467	26	221	247	3.82%	3.42%
Ukraine	63,231	146	1,450	1,596	2.52%	2.29%
United Arab Emirates	23,470	178	386	564	2.40%	1.64%
Uruguay	66,244	51	1,114	1,165	1.76%	1.68%
Uzbekistan	7,758	49	534	583	7.52%	6.88%
Vanuatu	88	-	2	2	2.27%	2.27%
Venezuela	779,882	369	6,896	7,265	0.93%	0.88%
Vietnam	54,041	269	936	1,205	2.23%	1.73%
Yemen	2,493	13	160	173	6.94%	6.42%
Zambia	3,323	9	96	105	3.16%	2.89%
Zimbabwe	5,327	18	87	105	1.97%	1.63%
TOTAL	11,961,355	16,133	173,136	189,269	1.58%	1.45%

Table 3
FY 2014 Overstay rates for Canadian and Mexican nonimmigrants admitted to the United States for business or pleasure via air and sea POEs

Country of Citizenship	Expected Departures	Out-of-Country Overstays	Suspected In-Country Overstays	Total Overstays	Overstay Rate	Suspected In-Country Overstay Rate
Canada	7,721,124	7,710	82,493	90,203	1.17%	1.07%
Mexico	2,673,330	2,912	34,315	37,227	1.39%	1.28%
TOTAL	**10,394,454**	**10,622**	**116,808**	**127,430**	**1.22%**	**1.12%**

Population Estimates
MARCH 2013

Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2012

BRYAN BAKER AND NANCY RYTINA

This report provides estimates of the size of the unauthorized immigrant population residing in the United States as of January 2012 by period of entry, region and country of origin, state of residence, age, and sex. The estimates were obtained using the residual methodology employed for previous estimates of the unauthorized population (see Hoefer, Rytina, and Baker, 2012). The unauthorized immigrant population is the remainder or residual after the legally resident foreign-born population—legal permanent residents (LPRs), naturalized citizens, asylees, refugees, and nonimmigrants—is subtracted from the total foreign-born population. Data to estimate the legally resident population were obtained primarily from the Department of Homeland Security (DHS), whereas the American Community Survey (ACS) of the U.S. Census Bureau was the source for estimates of the total foreign-born population.

In summary, an estimated 11.4 million unauthorized immigrants were living in the United States in January 2012 compared to 11.5 million in January 2011. These results suggest little to no change in the unauthorized immigrant population from 2011 to 2012. Of all unauthorized immigrants living in the United States in 2012, 42 percent entered in 2000 or later. Entrants since 2005 accounted for 14 percent of the total. Fifty-nine percent of unauthorized immigrants in 2012 were from Mexico.

DEFINITIONS

Legal Residents

The legally resident immigrant population as defined for these estimates includes all persons who were granted lawful permanent residence; granted asylum; admitted as refugees; or admitted as nonimmigrants for a temporary stay in the United States and not required to leave by January 1, 2012. Nonimmigrant residents refer to certain aliens who were legally admitted temporarily to the United States such as students and temporary workers.

Unauthorized Residents

The unauthorized resident immigrant population is defined as all foreign-born non-citizens who are not legal residents (see above). Most unauthorized residents either entered the United States without inspection or were admitted temporarily and stayed past the date they were required to leave. Unauthorized immigrants applying for adjustment to LPR status under the Immigration and Nationality Act (INA) are unauthorized until they have been granted lawful permanent residence, even though they may have been authorized to work. Persons who are beneficiaries of Temporary Protected Status (TPS)—an estimated several hundred thousand—are not technically unauthorized but were excluded from the legally resident immigrant population because data are unavailable in sufficient detail to estimate this population.

METHODOLOGY AND DATA

Two populations are estimated in order to derive the unauthorized population estimates: 1) the total foreign-born population living in the United States on January 1, 2012 and 2) the legally resident population on the same date. The unauthorized population estimate is the residual when 2) is subtracted from 1). Foreign-born residents who entered the United States prior to 1980 were assumed to be legally resident since most

Homeland Security

Office of Immigration Statistics
POLICY DIRECTORATE

were eligible for LPR status.[1] Therefore, the starting point for the estimates was January 1, 1980. The steps involved in estimating the components of each population are shown in **APPENDIX 1**. Data on the foreign-born population that entered during 1980–2011 by country of birth, state of residence, year of entry, age, and sex were obtained from the 2011 ACS. The ACS is a nationwide sample survey that collects information from U.S. households on social, demographic, and economic characteristics, including country of birth and year of entry of the foreign-born population. The ACS consists of non-overlapping samples from which information is collected monthly over the course of a year. The ACS was selected for the estimates because of its large sample size, about 3.3 million households in 2011 compared to 100,000 for the March 2012 Current Population Survey, the primary alternative source of national data on the foreign-born population.

Data on persons who obtained LPR status by country of birth, state of residence, age, sex, category of admission, and year of entry were obtained from DHS administrative records maintained in an application case tracking system of U.S. Citizenship and Immigration Services (USCIS). Data on refugees arriving in the United States by country of origin were obtained from the Department of State. Data on persons granted asylum by country of origin were obtained from USCIS for those granted asylum affirmatively and from the Executive Office for Immigration Review of the Department of Justice for those granted asylum defensively in removal proceedings. Data on nonimmigrant admissions by country of citizenship, state of residence, age, sex, and class of admission were obtained from I-94 arrival-departure records in the TECS system of the U.S. Customs and Border Protection. Estimates of the unauthorized population were generated for the ten leading countries of birth and states of residence, age, and sex. The Cuban-born population living in the United States was excluded from the estimates since, according to immigration law, most Cubans are admitted or paroled into the United States and are eligible a year later to apply to adjust to LPR status.

Changes for the 2012 Estimates

Previously released DHS estimates of the unauthorized population for January 2010 by country of origin and state of residence have been updated in this report to facilitate comparison with estimates for 2011 and 2012. The original 2010 estimates were derived from the 2009 ACS, which used foreign-born population estimates based on the 2000 Census updated for births, deaths, and internal and international migration, whereas the 2011 and 2012 estimates used foreign-born population estimates based on the 2010 Census. The Census Bureau urges caution in comparing population estimates that use different Census base years (U.S. Census Bureau, 2011). The Pew Hispanic Center calculated that that the estimated 1.5 million person increase in the foreign-born population between the 2009 and 2010 ACS surveys would have been only 0.6 million if the 2009 ACS estimates had been based on the 2010 Census (Passel and Cohn, 2012a). DHS updated the 2010 unauthorized population estimates by recalculating the expected number of 1980-2009 foreign-born entrants using the January 1, 2011 estimate of foreign-born entrants and increasing it by the mortality and emigration expected to have occurred in the previous 12 months. The 2011 report provided an updated estimate for only the total 2010 unauthorized population. This report provides updated estimates of the 2010 unauthorized population by region/country of origin and state of residence. In addition, the base year for comparisons in Figure 2, Table 3, and Table 4 has been updated from 2000 to 2010.

Limitations

Annual estimates of the unauthorized immigrant population are subject to sampling error in the ACS and considerable nonsampling error because of uncertainty in some of the assumptions required for estimation as indicated below. Caution is recommended in interpreting year-year changes in the size of the unauthorized population.

Assumptions about undercount of the foreign-born population in the ACS and rates of emigration. The estimates are sensitive to the assumptions that are made about these components (see **RESULTS**).

Accuracy of year of entry reporting. Concerns exist among immigration analysts regarding the validity and reliability of Census survey data on the year of entry question, "When did this person come to live in the United States?" Errors also occur in converting DHS administrative dates for legally resident immigrants to year of entry dates.

Assumptions about the nonimmigrant population estimate. The estimates are based on admission dates and length of visit by class of admission and country of citizenship and not actual population counts.

Sampling error in the ACS. The 2011 ACS data are based on a sample of the U.S. population. Thus the estimates of the total foreign-born population that moved to the United States in the 1980–2011 period are subject to sampling variability. The estimated margin of error for the estimate of the foreign-born population in the 2011 ACS at the 90 percent confidence level is plus or minus approximately 125,000.

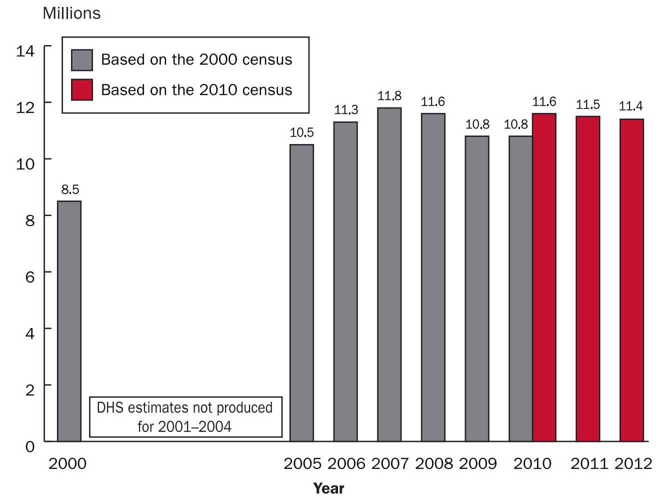
Accuracy of state of residence for the non-naturalized legally resident population. State of residence for the non-naturalized legally resident 1980–2011 entrants is assumed to be the state of residence on the date the most recent status (e.g., refugee or LPR) was obtained; however, the accuracy of the estimates may be affected by state-to-state migration that occurred between the date of the status change and January 1, 2012.

RESULTS

An estimated 11.4 million unauthorized immigrants were living in the United States on January 1, 2012 compared to 11.5 million on January 1, 2011(see Figure 1). These estimates suggest little change in the size of the unauthorized population between 2011 and 2012.Trends in the unauthorized population reported by DHS are consistent with the most recent estimates by the Pew Hispanic Center. Pew estimates show 11.2 million unauthorized immigrants residing in the United States in March 2010 (Passel and Cohn, 2011) and 11.1 million in March 2011 (Passel and Cohn, 2012b).

[1] Under Section 249 of the INA, the registry provision, qualified persons who have resided continuously in the United States since prior to January 1, 1972 may apply for LPR status. Additionally, persons who had resided continuously in the United States since prior to January 1, 1982 as unauthorized residents were eligible to adjust for LPR status under the Immigration Reform and Control Act (IRCA) of 1986.

Figure 1.
Unauthorized Immigrant Population: 2000–2012



Source: U.S. Department of Homeland Security.

Long Term Trend

The unauthorized immigrant population grew from 2–4 million in 1980 (Warren and Passel, 1987) to 8.5 million in 2000 and 11.6 million in 2010 (see Figure 1). The population likely peaked around 2007 at 11.8 million (Hoefer, Rytina, and Baker, 2011) or 12.0 million (Passel and Cohn, 2011). It is unlikely that the unauthorized immigrant population has increased since 2007 given relatively high U.S. unemployment, improved economic conditions in Mexico, record low numbers of apprehensions of unauthorized immigrants at U.S. borders, and greater levels of border enforcement.

The sensitivity of the estimates to assumptions about undercount and emigration is illustrated with several examples. Doubling the unauthorized immigrant undercount rate from 10 percent to 20 percent increases the estimated unauthorized population in 2012 from 11.4 million to 12.9 million. By lowering or raising emigration rates 20 percent and holding all other assumptions constant, the estimated unauthorized immigrant population would range from 10.6 million to 12.3 million. Doubling the unauthorized immigrant undercount rate and lowering or raising emigration rates by 20 percent would expand the range of the estimated unauthorized immigrant population from 11.9 to 13.8 million.

Period of Entry

Of the 11.4 million unauthorized immigrants in 2012, 1.5 million (14 percent) entered the United States on January 1, 2005 or later (see Table 1). Larger numbers came during 2000–2004 (3.2 million or 28 percent) and 1995–1999 (2.9 million or 26 percent). Fewer came between 1990–1994 (1.7 million or 15 percent) or during the 1980s (2.0 million or 17 percent).

Components of the Unauthorized Immigrant Population in 2012

The size of each component of the unauthorized immigrant population estimates for 2012 is displayed in Table 2. See **APPENDIX 1** for a detailed explanation of each entry in Table 2. For the foreign-born population, the starting point was the estimated 31.8 million foreign-born residents in the 2011 ACS that entered the United States during 1980–2011. This population was increased by 2.3 million, or 7 percent, by adjustments for the shift in the reference date from mid-year 2011 to January 1, 2012 and the addition of undercounts for the populations of nonimmigrants, legally resident immigrants, and unauthorized immigrants. The estimated undercount of the unauthorized immigrant population in the ACS was 1.1 million and represents 49 percent of all adjustments to the foreign-born population.

For the legally resident population, the starting point was the flow of 26.6 million LPRs, refugees, and asylees during 1980–2011. By January 2012, the 26.6 million had been reduced by 5.8 million to 20.8 million due to mortality and emigration. Emigration accounted for 4.0 million, or 69 percent, of the 5.8 million. The addition of the nonimmigrant population, estimated at 1.9 million, resulted in a total estimated legally resident population of 22.7 million on January 1, 2012. Subtracting the 22.7 million legally resident immigrants from the total 34.1 million foreign-born population on January 1, 2012 that entered the United States during 1980–2011 yields the final estimated unauthorized population of 11.4 million.

Estimates by Region and Country of Birth

An estimated 8.9 million (78 percent) of the total 11.4 million unauthorized immigrants living in the United States in 2012 were from North America, including Canada, Mexico, the Caribbean, and Central America (see Figure 2). The next leading regions of origin were Asia (1.3 million) and South America (0.7 million).

Mexico continued to be the leading source country of unauthorized immigration to the United States (see Table 3). There were 6.7 million unauthorized immigrants from Mexico in 2012, representing 59 percent of the unauthorized population. The next leading source countries were El Salvador (690,000), Guatemala

Table 1.

Period of Entry of the Unauthorized Immigrant Population: January 2012

Period of entry	Estimated population January 2012	
	Number	Percent
All years	11,430,000	100
2005–2011	1,540,000	14
2000–2004	3,250,000	28
1995–1999	2,920,000	26
1990–1994	1,720,000	15
1985–1989	1,110,000	10
1980–1984	890,000	8

Detail may not sum to totals because of rounding.
Source: U.S. Department of Homeland Security.

Table 2.

Components of the Unauthorized Immigrant Population: January 2012

	2012
1) Foreign-born population	
a. Foreign-born population, entered 1980–2011, 2011 ACS	31,770,000
b. Adjustment for shift in reference date from July 1, 2011 to January 1, 2012	470,000
c. Undercount of nonimmigrants in ACS	190,000
d. Undercount of other legally resident immigrants (LPRs, recent refugee/asylee arrivals) in ACS	520,000
e. Undercount of unauthorized immigrant population in ACS	1,140,000
f. Estimated foreign-born population, January 1, 2012 (a.+b.+c.+d.+e.)	34,090,000
2) Legally resident population	
g. LPR, refugee, and asylee flow January 1, 1980–December 31, 2011	26,640,000
h. Mortality 1980–2011	1,840,000
i. Emigration 1980–2011	4,010,000
j. LPR, refugee, and asylee resident population, January 1, 2012 (g.–h.–i.)	20,790,000
k. Nonimmigrant population on January 1, 2012	1,870,000
l. Estimated legally resident population, January 1, 2012 (j.+k.)	22,660,000
3) Unauthorized immigrant population	
m. Estimated resident unauthorized immigrant population, January 1, 2012 (f.–l.)	11,430,000

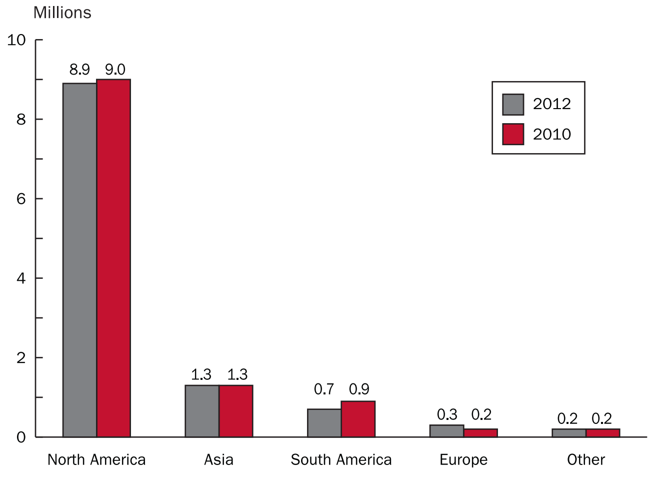
Detail may not sum to totals because of rounding.
Source: U.S. Department of Homeland Security.

(560,000), Honduras (360,000), and Philippines (310,000). The ten leading countries of origin represented 85 percent of the unauthorized immigrant population in 2012.

Estimates by State of Residence

California remained the leading state of residence of the unauthorized immigrant population in 2012, with 2.8 million (see Table 4). The next leading state was Texas with 1.8 million unauthorized residents, followed by Florida (730,000), New York (580,000), and Illinois (540,000). The ten leading states represented 73 percent of the unauthorized population in 2012.

Figure 2.
Region of Birth of the Unauthorized Immigrant Population: January 2012 and 2010



Source: U.S. Department of Homeland Security.

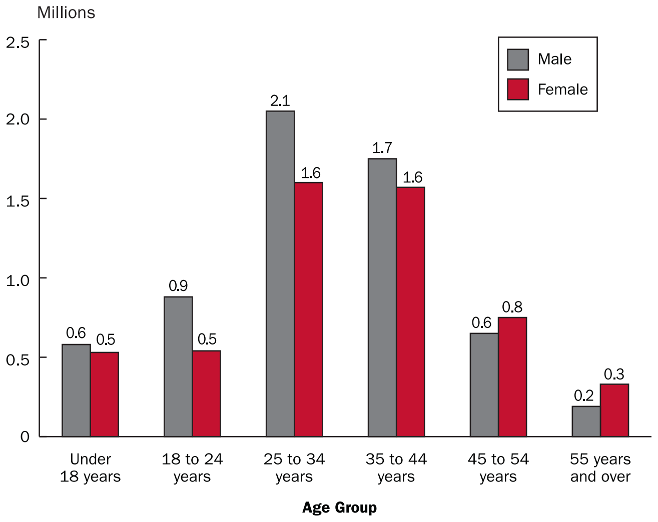
Estimates by Age and Sex

In 2012, 61 percent of unauthorized immigrants were ages 25 to 44 years, and 53 percent were male (see Figure 3 and Table 5). Males accounted for 58 percent of the unauthorized population in the 18 to 34 age group in 2012 while females accounted for 57 percent of the 45 and older age groups.

NEXT STEPS

The estimates presented here will be updated periodically based on annual data of the foreign-born population collected in the ACS and on the estimated lawfully resident foreign-born population derived from various administrative data sources.

Figure 3.
Age by Sex of the Unauthorized Immigrant Population: January 2012



Source: U.S. Department of Homeland Security.

Table 3.

Country of Birth of the Unauthorized Immigrant Population: January 2012 and 2010

Country of birth	Estimated population in January		Percent of total	
	2012	2010	2012	2010
All countries	11,430,000	11,590,000	100	100
Mexico	6,720,000	6,830,000	59	59
El Salvador	690,000	670,000	6	6
Guatemala	560,000	520,000	5	4
Honduras	360,000	380,000	3	3
Philippines	310,000	290,000	3	2
India	260,000	270,000	2	2
Korea	230,000	220,000	2	2
China	210,000	300,000	2	3
Ecuador	170,000	210,000	2	2
Vietnam	160,000	190,000	1	2
Other countries	1,760,000	1,720,000	15	15

Detail may not sum to totals because of rounding.
Source: U.S. Department of Homeland Security.

Table 4.

State of Residence of the Unauthorized Immigrant Population: January 2012 and 2010

State of residence	Estimated population in January		Percent of total	
	2012	2010	2012	2010
All states	11,430,000	11,590,000	100	100
California	2,820,000	2,910,000	25	25
Texas	1,830,000	1,780,000	16	15
Florida	730,000	730,000	6	6
New York	580,000	690,000	5	6
Illinois	540,000	550,000	5	5
New Jersey	430,000	440,000	4	4
Georgia	400,000	430,000	3	4
North Carolina	360,000	390,000	3	3
Arizona	350,000	350,000	3	3
Washington	270,000	260,000	2	2
Other states	3,110,000	3,040,000	27	26

Detail may not sum to totals because of rounding.
Source: U.S. Department of Homeland Security.

Table 5.

Age by Sex of the Unauthorized Immigrant Population: January 2012

Age	Total		Male		Female	
	Number	Percent	Number	Percent	Number	Percent
All ages	11,430,000	100	6,100,000	100	5,330,000	100
Under 18 years	1,120,000	10	580,000	10	530,000	10
18 to 24 years	1,410,000	12	880,000	14	540,000	10
25 to 34 years	3,660,000	32	2,050,000	34	1,600,000	30
35 to 44 years	3,320,000	29	1,750,000	29	1,570,000	29
45 to 54 years	1,400,000	12	650,000	11	750,000	14
55 years and over	520,000	5	190,000	3	330,000	6

Detail may not sum to totals because of rounding.
Source: U.S. Department of Homeland Security.

APPENDIX 1

Components for Estimating the Unauthorized Immigrant Population

The material below describes how the components for the total foreign-born and legally resident populations were estimated. The unauthorized population estimate is the residual when the legally resident population is subtracted from the total foreign-born population. Note that the labels for each component correspond with the entries in Table 2.

1) Foreign-born population

a. Foreign-born population, entered 1980–2011

The estimated total foreign-born population that entered between 1980–2011 was obtained from the ACS's FactFinder. FactFinder is the Census-maintained online data portal for obtaining ACS estimates from the full sample for a particular year. Data on the distribution of the foreign born by country of origin, state of residence, year of entry, age, and sex were obtained from the 2011 Public Use Microdata Sample (PUMS). The overall FactFinder estimate for the total foreign-born population entering in the post-1979 period was reduced to remove PUMS estimates of the post-1979 Cuban-born population. Further, a three-year moving average was applied to PUMS data for year of entry to reduce heaping effects.

b. Shift in reference date to January 1, 2012

The reference date for the 2011 ACS, the most recently available ACS data, was shifted from mid-year 2011 to January 1, 2012 by multiplying the population of 2011 entrants by 1.71, which is the average of three ratios: the ratio of the estimated population in the 2011 ACS that entered the United States during 2010 compared to the population in the 2010 ACS that entered in 2010 and the comparable ratios for the 2009 entrants in the 2009 and 2010 ACS surveys and the 2008 entrants in the 2008 and 2009 ACS surveys.

c. Undercount of nonimmigrants in the ACS

Undercount refers to the number of persons who should have been counted in a survey or census, but were not. A rate of 10 percent was used to estimate the nonimmigrant undercount. This rate was used in DHS unauthorized population estimates for 2000 and 2005–2011 (U.S. Department of Homeland Security, 2003; Hoefer et al., 2012).

d. Undercount of LPRs, refugees, and asylees in the ACS

The undercount rate for LPRs, refugees, and asylees in the ACS was assumed to be 2.5 percent. This was the same rate used in DHS estimates for 2000 and 2005–2011 (U.S. Department of Homeland Security, 2003; Hoefer et al., 2012).

e. Undercount of unauthorized immigrants in the ACS

The undercount rate for unauthorized immigrants in the ACS was assumed to be 10 percent. This was the same rate used in previous DHS estimates for 2000 and 2005–2011 (U.S. Department of Homeland Security, 2003; Hoefer et al., 2012).

f. Estimated foreign-born population, January 1, 2012

The sum of 1a. through 1e. (above) is the estimated foreign-born population on January 1, 2012 that entered the United States during the 1980–2011 period.

2) Legally Resident Population

g. LPR, refugee, and asylee flow, entered 1980–2011

The 1980–2011 flow was calculated separately for LPRs, refugees, and asylees. LPRs consist of two groups: new arrivals and those who have adjusted status. New arrivals include all persons with immigrant visas issued by the Department of State who were admitted at a U.S. port of entry. For new arrival LPRs, the date of entry into the United States is the same as the date of approval for LPR status. For LPRs adjusting status, year of entry was assumed to be the year of last entry between 1980 and 2011 prior to adjustment.

Refugees and asylees included in the legally resident flow had not adjusted to LPR status as of January 1, 2012. The refugee and asylee flow was estimated based on the average time spent in the status before adjustment to LPR status—2.2 years for refugees and 3.9 years for asylees adjusting in 2011. The refugee and asylee portion of the legally resident flow therefore included refugees who arrived in the United States during the 2.2 years prior to 2012 and persons granted asylum during the 3.9 years preceding 2012.

h. Mortality of legally resident flow 1980–2011

Data are not collected on the mortality of legally resident immigrants. They were survived to 2012 by sex and age (taking into account subsequent naturalization) using mortality rates by age and sex from 1999–2001 life tables (Arias et al., 2008).

i. Emigration of legally resident flow 1980–2011

Emigration is a major component of immigrant population change. In the absence of data that directly measure emigration from the United States, researchers have developed indirect estimates based largely on Census data. For this report, annual emigration rates were calculated from estimates of emigration of the foreign-born population based on 1980 and 1990 Census data (Ahmed and Robinson, 1994). In addition, refugees and asylees, with little likelihood of returning to their country of origin, were assumed not to emigrate. The effective rate of emigration for legally resident immigrants granted LPR status in 1991–1992 was about 19 percent during the twenty-year period through January 2012 (about 0.9 percent per year). For the entire LPR population that entered in 1980–2011, the average emigration rate was about 1.1 percent per year.

j. LPR, refugee, and asylee population on January 1, 2012

Subtracting mortality (2h.) and emigration (2i.) from the LPR, refugee, and asylee flow during 1980–2011 (2g.)

results in the estimated LPR, refugee, and asylee resident population on January 1, 2012.

k. Nonimmigrant population on January 1, 2012

The number of nonimmigrants living in the United States on January 1, 2012 was estimated by counting days of presence between July 1, 2011 and June 30, 2012 and dividing the result by 366. The estimate was restricted to classes of admission such as students, temporary workers, and exchange visitors where the length of stay typically exceeds two months. The estimate does not include border crossers or visitors for business or pleasure. Year of entry for the 2012 nonimmigrant population was based on the distribution of year of entry for nonimmigrants used in previous DHS unauthorized immigrant population estimates (U.S. Department of Homeland Security, 2003; Hoefer et al., 2012).

l. Estimated legally resident immigrant population on January 1, 2012

Adding the population of LPRs, refugees, and asylees on January 1, 2012 (2j.) to the nonimmigrant population on the same date (2k.) results in the total estimated legally resident immigrant population in the United States on January 1, 2012.

3) Unauthorized immigrant population

m. Estimated unauthorized immigrant population on January 1, 2012

Subtracting the estimated legally resident immigrant population (2l.) from the total foreign-born population on January 1, 2012 (1f.) yields the estimate of the unauthorized immigrant population.

APPENDIX 2

Country of Birth and State of Residence of the Unauthorized Immigrant Population: January 2000 and 2005–2012

Country of birth and state of residence	Estimated population in January									
	2000	2005	2006*	2007	2008	2009	2010	2010**	2011	2012
Country of birth										
Total.	8,460,000	10,490,000	11,310,000	11,780,000	11,600,000	10,750,000	10,790,000	11,590,000	11,510,000	11,430,000
Mexico	4,680,000	5,970,000	6,570,000	6,980,000	7,030,000	6,650,000	6,640,000	6,830,000	6,800,000	6,720,000
El Salvador	430,000	470,000	510,000	540,000	570,000	530,000	620,000	670,000	660,000	690,000
Guatemala.	290,000	370,000	430,000	500,000	430,000	480,000	520,000	520,000	520,000	560,000
Honduras.	160,000	180,000	280,000	280,000	300,000	320,000	330,000	380,000	380,000	360,000
Philippines.	200,000	210,000	280,000	290,000	300,000	270,000	280,000	290,000	270,000	310,000
India	120,000	280,000	210,000	220,000	160,000	200,000	200,000	270,000	240,000	260,000
Korea	180,000	210,000	230,000	230,000	240,000	200,000	170,000	220,000	230,000	230,000
China	190,000	230,000	170,000	290,000	220,000	120,000	130,000	300,000	280,000	210,000
Ecuador.	110,000	120,000	150,000	160,000	170,000	170,000	180,000	210,000	210,000	170,000
Vietnam.	160,000	150,000	150,000	120,000	80,000	110,000	110,000	190,000	170,000	160,000
Other countries . . .	1,940,000	2,300,000	2,340,000	2,170,000	2,100,000	1,700,000	1,610,000	1,830,000	1,670,000	1,760,000
State of residence										
Total.	8,460,000	10,490,000	11,310,000	11,780,000	11,600,000	10,750,000	10,790,000	11,590,000	11,510,000	11,430,000
California.	2,510,000	2,770,000	2,790,000	2,840,000	2,850,000	2,600,000	2,570,000	2,910,000	2,830,000	2,820,000
Texas	1,090,000	1,360,000	1,620,000	1,710,000	1,680,000	1,680,000	1,770,000	1,780,000	1,790,000	1,830,000
Florida.	800,000	850,000	960,000	960,000	840,000	720,000	760,000	730,000	740,000	730,000
New York	540,000	560,000	510,000	640,000	640,000	550,000	460,000	690,000	630,000	580,000
Illinois	440,000	520,000	530,000	560,000	550,000	540,000	490,000	550,000	550,000	540,000
New Jersey	350,000	380,000	420,000	470,000	400,000	360,000	370,000	440,000	420,000	430,000
Georgia	220,000	470,000	490,000	490,000	460,000	480,000	460,000	430,000	440,000	400,000
North Carolina	260,000	360,000	360,000	380,000	380,000	370,000	390,000	390,000	400,000	360,000
Arizona	330,000	480,000	490,000	530,000	560,000	460,000	470,000	350,000	360,000	350,000
Washington	170,000	240,000	280,000	260,000	260,000	230,000	200,000	260,000	260,000	270,000
Other states	1,750,000	2,510,000	2,860,000	2,940,000	2,980,000	2,760,000	2,840,000	3,040,000	3,100,000	3,110,000

*Revised as noted in the 1/1/2007 unauthorized estimates report published in September 2008.

**Revised to be consistent with estimates derived from the 2010 Census.

Detail may not sum to totals because of rounding.

Source: U.S. Department of Homeland Security.

REFERENCES

Ahmed, Bashir and J. Gregory Robinson, 1994. “Estimates of Emigration of the Foreign-Born Population: 1980-1990,” Technical Working Paper No. 9, U.S. Bureau of the Census, http://www.census.gov/population/www/documentation/twps0009/twps0009.html

Arias, Elizabeth and Lester R. Curtin, Rong Wei and Robert N. Anderson, 2008. “U.S. Decennial Life Tables for 1999-2001, United States Life Tables,” *National Vital Statistics Report* 57 (1), National Center for Health Statistics, Centers for Disease Control. http://www.cdc.gov/nchs/data/nvsr/nvsr57/nvsr57_01.pdf

Hoefer, Michael, Nancy Rytina and Bryan C. Baker, 2012. “Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2010,” Office of Immigration Statistics, Policy Directorate, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/statistics/publications/ois_ill_pe_2011.pdf

Hoefer, Michael, Nancy Rytina and Bryan C. Baker, 2011. “Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2010,” Office of Immigration Statistics, Policy Directorate, U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/statistics/publications/ois_ill_pe_2010.pdf

Passel, Jeffrey S. and D’Vera Cohn, 2011. “Unauthorized Immigrant Population: National and State Trends, 2010,” Pew Hispanic Center, http://pewhispanic.org/files/reports/133.pdf

Passel, Jeffrey S. and D’Vera Cohn, 2012a. “U.S. Foreign-Born Population: How Much Change from 2009 to 2010?” Pew Hispanic Center, http://www.pewhispanic.org/files/2012/01/Foreign-Born-Population.pdf

Passel, Jeffrey S. and D’Vera Cohn, 2012b. “Unauthorized Immigrants: 11.1 Million in 2011,” Pew Hispanic Center, http://www.pewhispanic.org/2012/12/06/unauthorized-immigrants-11-1-million-in-2011/

U.S. Census Bureau, 2011. “Changes in Population Controls,” American Community Survey Research Note, http://www.census.gov/acs/www/Downloads/comparing_acs_data/2010_Change_Population_Controls.pdf

U.S. Department of Homeland Security, 2003. “Estimates of the Unauthorized Immigrant Population Residing in the United States: 1990 to 2000,” http://www.dhs.gov/xlibrary/assets/statistics/publications/Ill_Report_1211.pdf

Warren, Robert and Jeffrey S. Passel, 1987. “A Count of the Uncountable: Estimates of Undocumented Aliens Counted in the 1980 United States Census,” *Demography* 24:375-393.

Homeland Security

DHS Sensitive Systems Policy Directive 4300A

Version 12.01
February 12, 2016

This Policy implements DHS Management Directive 140-01
"Information Technology System Security," July 31, 2007

Protecting the Information that Secures the Homeland

This page intentionally left blank

FOREWORD

The Department of Homeland Security (DHS) 4300 series of information security publications are the official documents that articulate Departmental policies, standards, and guidelines in accordance with DHS Management Directive 140-01 *Information Technology System Security*.

Comments concerning DHS Information Security publications are welcomed and should be submitted to the DHS Director of IT Security Policy and Remediation at infosecpolicy@hq.dhs.gov or addressed to:

DHS Director of IT Security Policy and Remediation
OCIO CISO Stop 0182
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0182

Jeffrey Eisensmith
Chief Information Security Officer
Department of Homeland Security

This page intentionally left blank

TABLE OF CONTENTS

1.0 INTRODUCTION

This document articulates the Department of Homeland Security (DHS) Information Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook*. This Policy Directive and the *Handbook* serve as the foundation on which Components are to develop and implement their own information security programs. The Baseline Security Requirements (BLSR) included in the Handbook must be addressed when developing and maintaining information security documents.

1.1 Information Security Program

The DHS Information Security Program provides a baseline of policies, procedures, standards, and guidelines for DHS Components. This Policy Directive provides direction to managers and senior executives for managing and protecting sensitive systems. It also defines policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation in DHS information system infrastructure and operations. The policy elements expressed in this Policy Directive are designed to be broad in scope to accommodate the diverse DHS operating environments. Each Component or Office is responsible for identifying, developing, and implementing any additional policies needed to meet their specific requirements. Implementation information can often be found in specific National Institute of Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Rev 4, “Security and Privacy Controls for Federal Information Systems and Organizations.”

This Policy Directive pertains to DHS Sensitive Systems, as distinct from DHS National Security Systems (NSS), which are governed by DHS National Security Systems Policy Directive 4300B series, available on the DHS Chief Information Security Officer (CISO) Web site. The 4300B series applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS, and users of DHS NSS that collect, generate, process, store, display, transmit, or receive Confidential, Secret, or Top Secret classified national security information.

Policy elements are effective when issued. Failure to implement any policy element within 135 days shall be considered a weakness, and either a system or program Plan of Action and Milestones (POA&M) must be generated by the Component for the identified weaknesses. When this Policy Directive is changed, the DHS Chief Information Security Officer (CISO) will ensure that appropriate tool changes are made available to the Department within 90 days of the changes.

1.2 Authorities

The following are authoritative references for the DHS Sensitive Information Security Program. Additional references are located in Appendix C to this Policy Directive.

- E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 44 U.S.C. 101
- Federal Information SecurityModernization Act of 2014 (FISMA), Public Law 113-283; 128 Stat 3073
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Transmittal Memorandum 4, 2010
- DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- NIST Special Publication (SP) 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, with updates as of January 22, 2015
- NIST SP 800-37, Rev 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010

1.3 Policy Overview

DHS information security policies define the security management structure and foundation needed to ensure adequate control over DHS sensitive information and systems. Policies in this document are organized in three sections:

- **Management Controls –** These controls focus on managing both system information security controls and system risk. These controls consist of risk mitigation techniques normally used by management.
- **Operational Controls –** These controls focus on mechanisms primarily implemented and executed by the people responsible for use of the system. Operational controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.
- **Technical Controls –** These are the security controls executed by the information systems. Technical controls provide automated protection from unauthorized access or misuse; facilitate detection of security violations; and support security requirements for applications and data.

DHS privacy controls have been added to DHS information security policy documents to comply with the publication of NIST SP 800-53, Rev.4, Appendix J: "Privacy Control Catalog." The privacy controls focus on ensuring information privacy, distinct from, but closely related to information security. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of Personally Identifiable Information (PII).

1.4 Definitions

The definitions in this section apply to the policies and procedures discussed in this document. In general, the sources for the definitions given in this Section are relevant NIST documents. Other definitions may be found in Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance Glossary," 26 April 2010. Definitions bearing on Privacy are sourced from *Privacy Incident Handling Guidance* and the *Privacy Compliance* documentation issued by the DHS Privacy Office.

1.4.1 Classified National Security Information

Information that has been determined, pursuant to Executive Order 13526, "Classified National Security Information," to require protection against unauthorized disclosure and is marked to indicate its classified status. [Source: Executive Order 13526]

1.4.2 Component

A DHS *Component* is any organization which reports directly to the Office of the Secretary (including the Secretary, the Deputy Secretary, the Chief of Staff's, Counselors, and staff, when approved as such by the Secretary), including both Operational Components and Support Components (also known as Headquarters Components). [Source *DHS Lexicon* and DHS Management Directive 112-01]

1.4.3 Continuity of Operations

Internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies, through plans and procedures that:

- Delineate essential functions and supporting information systems
- Specify succession of office and the emergency delegation of authority
- Provide for the safekeeping of vital records and databases
- Identify alternate operating facilities, if necessary
- Provide for interoperable communications
- Validate the capability to recover through tests, training, and exercises

1.4.4 Continuity of Operations Plan (COOP)

A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. [Source NIST SP 800-34]

1.4.5 DHS System

A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on behalf of DHS. DHS systems include *general support systems* and *major applications*.

1.4.6 Essential Functions

Essential functions are those that enable Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain industrial capability and the national economy base during an emergency.

1.4.7 Federal Information Security Modernization Act (FISMA)

FISMA requires each agency to develop, document, and implement an agency-wide information security program that will provide a high level of security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA requires that the Chief Information Officer (CIO) designate a senior agency information security official who shall develop and maintain a Department-wide information security program. The designee’s responsibilities include:

- Developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements
- Training and overseeing personnel with significant information security responsibilities
- Assisting senior Department officials with respect to their responsibilities under the statute
- Ensuring that the Department has sufficient trained personnel to ensure the Department’s compliance with the statute and related policies, procedures, standards, and guidelines
- Ensuring that the Department CIO, in coordination with other senior Department officials, reports annually to the Secretary on the effectiveness of the Department’s information security program, including the progress of remedial actions

1.4.8 Foreign Intelligence Information

This type of information relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but does not include counterintelligence (CI) except for information on international terrorist activities.

1.4.9 General Support System

A *general support system* (GSS) is an interconnected set of information resources that share common functionality and are under the same direct management control. A GSS normally includes hardware, software, information, applications, communications, data and users. Examples of GSSs include local area networks (LAN), including smart terminals that support a branch office, Department-wide backbones, communications networks, and Departmental data processing centers including their operating systems and utilities.

Security for GSSs in use at DHS Headquarters shall be under the oversight of the DHS Office of the Chief Information Officer (OCIO), with support from the DHS Security Operations Center (SOC). All other GSSs shall be under the direct oversight of respective Component CISOs, with support from the Component's SOC. Every GSS must have an Information Systems Security Officer (ISSO) assigned.

1.4.10 Information Technology

Division E of the Clinger-Cohen Actof 1996 (Public Law 104-106) defines Information Technology (IT) as:

> "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information"

For purposes of the preceding definition, "equipment" refers to that used by any DHS office, Component, or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a product in support of DHS.

The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

The term *information system* as used in this policy document, is equivalent to the term *information technology system*.

1.4.11 Major Application

A *major application* (MA) is an automated information system (AIS) that OMB Circular A-130 defines as requiring "…special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."

All Federal applications require some level of protection. Certain applications, because of the information they contain, however, require special management oversight and should be classified as MAs. An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications. Each MA must be under the direct oversight of a Component CISO or Information System Security Manager (ISSM), and must have an ISSO assigned.

1.4.12 National Intelligence Information

The Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, 118 Stat. 3662) amended the National Security Act of 1947 (50 U.S.C. 401a) to provide the following definition:

> ''(5) The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—
> (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and

(B) that involves—
(i) threats to the United States, its people, property, or interests;
(ii) the development, proliferation, or use of weapons of mass destruction; or
(iii) any other matter bearing on United States national or homeland security.''.

1.4.13 Operational Data

Operational data is information used in any DHS mission activity.

1.4.14 Personally Identifiable Information

Personally Identifiable Information (PII)" means information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. [see also Sensitive Personally Identifiable Information (SPII)]

1.4.15 Privacy Sensitive System

A *Privacy Sensitive System* is any system that collects, uses, disseminates, or maintains PII or Sensitive PII.

1.4.16 Privileged User

A *privileged user* is a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Source: NISTIR 7298 rev 2.0

1.4.17 Public Information

Public information can be disclosed to the public without restriction, but requires protection against erroneous manipulation or alteration (e.g., public websites).

1.4.18 Sensitive Information

Sensitive Information is any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy.

Sensitive Information includes:

- Chemical-terrorism Vulnerability Information (CVI)
- Protected Critical Infrastructure Information (PCII)
- Sensitive Security Information (SSI)
- Personally Identifiable Information (PII)

1.4.19 Sensitive Personally Identifiable Information (SPII)

Sensitive Personally Identifiable Information (SPII) is a subset of PII [see definition above], which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements..

1.4.20 Sensitive System

A *sensitive system* is any combination of facilities, equipment, personnel, procedures, and communications that is integrated for a specific purpose, and that may be vulnerable to an adversarial attack by an adversary seeking to violate or disrupt the system's confidentiality, integrity, or availability.

1.4.21 Strong Authentication

Strong authentication is a method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have). Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. [See the discussion of Level 4 assurance in NIST SP 800-63-2, "Electronic Authentication Guideline," (August 2013)]

1.4.22 Trust Zone

A *Trust Zone* consists of any combination of people, information resources, IT systems, and networks that are subject to a shared security policy (a set of rules governing access to data and services). For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.

1.4.23 Two-Factor Authentication

The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication:

- *Something you know* (for example, a password or Personal Identification Number (PIN)
- *Something you have* (for example, an ID badge or a cryptographic key)
- *Something you are* (for example, a fingerprint or other biometric data)

The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor." A requirement for two of the three factors listed above constitutes two factor authentication.

1.4.24 Visitor

A guest or temporary employee who presents themselves or is presented by a sponsor, for entry for less than 6 months to a secured facility that is not their primary work location. (Source: DHS Lexicon)

The visitor is placed in one of two categorizes, either ***escort required*** or ***no escort required***. ***Escort required*** visitors are escorted at all times. ***No escort required*** visitors are granted limited general access to the facility without an escort. Escort procedures for classified areas are indicated in Management Directive 11051 "SCIF Escort Procedures." (Source: DHS Lexicon)

1.4.25 Vital Records

Vital records are electronic and hardcopy documents, references, databases, and information systems needed to support essential functions under the full spectrum of emergencies. Categories of vital records may include:

- Emergency operating records: emergency plans and directive(s); orders of succession; delegations of authority; staffing assignments; selected program records needed to continue the most critical agency operations; and related policy or procedural records.
- Legal and financial rights records: records that protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records.
- Records used to perform national security preparedness functions and activities in accordance with Executive Order (EO).

1.5 Waivers

When a Component is unable to fully comply with any portion of this Policy Directive, it may request a waiver. Waiver requests should be routed through the Component's ISSO for the system, to the Component's CISO or ISSM, and then to the DHS CISO. All submitters shall coordinate with the Authorizing Official (AO) prior to submission.

If a material weakness is reported in an audit report, and the weakness is not scheduled for remediation within 12 months, the Component must submit a waiver request to the DHS CISO. If the material weakness exists in a financial system, the Component Chief Financial Officer (CFO) must also approve the waiver request before sending to the DHS CISO. If the material weakness exists in a system processing PII, the Component Privacy Officer or Privacy Point of Contact (PPOC) and DHS Chief Privacy Officer must also approve the waiver request before sending to the DHS CISO.

An approved waiver does not bring the system into compliance with policy; it is an acknowledgement by the DHS CISO of the system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided and compensating controls have been implemented.

In all cases, waivers shall be requested for an appropriate period based on a reasonable remediation strategy.

1.5.1 Waiver Requests

The Waiver Request Form found in Attachment B of the *DHS 4300A Sensitive Systems Handbook* shall be used.

Component ISSOs, audit liaisons, and others may develop the waiver request, but the System Owner shall submit the request through the Component's CISO/ISSM. All submitters shall coordinate with the Authorizing Official (AO) prior to submission

Waiver requests shall include documentation of mission impact as operational justification; mission impact; risk acceptance; risk mitigation measures; and a current POA&M for bringing the system control weakness into compliance.

Additionally, any waiver requests for financial systems must be submitted to and approved by the Component's CFO prior to submission to the DHS CISO. Any waiver request for sensitive systems with PII information must be submitted to and approved by the Component's Privacy Officer or senior PPOC prior to being submitted to the DHS CISO.

Any waiver for compliance with privacy controls must be submitted to and approved by the DHS Chief Privacy Officer.

Policy ID	DHS Policy Statements	Relevant Controls
1.5.1.a	This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).	SA-3
1.5.1.b	Systems not yet authorized to operate when this policy is issued shall comply with all of its policy statements or obtain appropriate waivers. Systems with an Authority to Operate (ATO) shall comply within 135 days of the date of this Policy is issued or obtain appropriate waivers. (A new ATO is only required for significant changes.)	PL-1
1.5.1.c	Components shall request a waiver whenever they are unable to comply fully with any portion of this policy.	CA-2
1.5.1.d	The Component CISO/ISSM shall approve all waiver requests prior to submitting them to the DHS CISO.	CA-6
1.5.1.e	The Component CIO shall approve any waiver request that results in a total waiver time exceeding (12 months before sending the request to the DHS CISO.	---
1.5.1.f	The Component CFO shall approve all requests for waivers for financial systems prior to their submission to the DHS CISO.	CA-6
1.5.1.g	The Component's Privacy Officer or Senior PPOC shall approve all requests for waivers for sensitive systems processing PII or SPII prior to their submission to the DHS CISO.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.5.1.h	The DHS Chief Privacy Officer shall approve all requests for waivers for compliance with any privacy control in Appendix J of NIST SP 800-53 prior to their submission to the DHS CISO.	---

1.5.2 Requests for Exception to U.S. Citizenship Requirement

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS). For further information regarding the citizenship exception process, contact the DHS OCSO at *foreign.visitors@hq.dhs.gov*.

Policy ID	DHS Policy Statements	Relevant Controls
1.5.2.a	Any Person of dual-citizenship (one being a US citizenship) and any Legal Permanent Resident who requires access to DHS systems as a validated representative of foreign power shall be processed as indicated in Section 1.5.2.	---
1.5.2.b	Exceptions to the U.S. Citizenship requirement shall be requested by submitting a completed Foreign National Visitor Access Request form to the DHS Office of the OCSO for each foreign national requiring access to DHS systems and networks.	PS-3
1.5.2.c	Component CISOs shall select a Foreign Access Coordinator to be the point of contact to the DHS OCSO for processing requests for exception to the U.S. Citizenship policy requirement (4.1.1.e). The Component shall notify OCSO of the selected Foreign Access Coordinator.	--
1.5.2.d	Foreign Access Coordinators shall, in coordination with the DHS OCSO, conduct an assessment of the risk of granting access to DHS systems by the Foreign National-specified and provide a recommendation to the Component CISO regarding the approval or disapproval of the request.	--

1.6 Digital and Other Electronic Signatures

Pursuant to Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), OMB Memorandum M-00-10, "Procedures and Guidance on Implementing of the Government Paperwork Elimination Act" requires executive agencies to provide the option for electronic maintenance, submission, and disclosure of information when practicable as a substitute for paper, and to use and accept electronic signatures.

Electronic signatures are essential in the Department's business processes and IT environments; reducing reliance on paper transactions improves information sharing, strengthens information security, and streamlines business processes, while reducing both cost and environmental impact.

Please refer to the "DHS Electronic Signature Policy Guidance" document for guidance on electronic signature policy

1.6.1 Digital Signatures and Other Electronic Signature Methods

The following DHS Policy Statements are applicable to both digital signatures and other electronic signature methods.

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.a	Digital signatures or other electronic signature methods shall be used whenever practical, except where handwritten signatures are required by law, regulation, Executive Order, or other agency requirement. Digital signature or other electronic signature methods, when properly executed, shall be accepted to the maximum extent practicable.	---
1.6.1.b	Electronic signatures, including digital signatures, shall be implemented by applications with the necessary security controls and practices such that: 1) the signer cannot successfully repudiate that he/she intended to sign, or that he/she applied the electronic signature; and 2) the integrity of the signed content cannot be successfully challenged.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.c	When a signature is required on electronic documents, transactions, communications, etc. for use within DHS, or for use for intra-governmental transactions, communications, etc., where all potential signers possess a Personal Identity Verification (PIV) card, Department of Defense (DOD)-issued Common Access Card (CAC), or PIV-I card (and the associated card readers, software, and verification processes are in place), the signing process shall employ a digital signature created by a properly identified signer through the use of their PIV card, CAC issued by DOD, or PIV-I card, whenever possible. Signers may use their software-based digital signature certificate that meets the requirements specified in Section 1.6.2.a below for signing when their PIV card, DOD-issued CAC, or PIV-I card cannot be used. Other electronic signature methods may be used when it is determined that it is not possible for the signer to use his/her PIV card, DOD-issued CAC, PIV-I card, or software-based digital signature certificate that meets the requirements specified in Section 1.6.2.a below. For legally binding signatures, the determination of what other electronic signature method shall be used must be based on a risk assessment of the likelihood of a successful challenge to the enforceability of the signature, and the monetary loss, or other adverse impact of an unenforceable signature.	---
1.6.1.d	The following requirements shall be met when implementing legally binding signatures using Digital Signature or an Other Electronic Signature Method: 1) The Signer must use an acceptable electronic form of signature; 2) The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record; 3) The electronic form of signature must be attached to or associated with the electronic record being signed; 4) There must be a means to identify and authenticate a particular person as the signer; and 5) There must be a means to preserve the integrity of the signed record.	---
1.6.1.e	When implementing one or more legally binding Digital Signatures in an electronic document, transaction, communication, etc., and the intent to sign for each signature is not evidenced by the context of the content being signed, a clear and conspicuous notice shall be incorporated into that electronic document, transaction, communication, etc., just prior to the location each signature, that indicates: 1) That an electronic signature is being created, and what constitutes the execution of the signature, 2) The reason for signing (for that specific signature), and 3) That when completed, it will constitute the Signer’s legally binding signature.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.f	When implementing legally binding electronic signatures for a specific use, where Other Electronic Signature Methods will be used, the risk assessment process, described in the "DHS Electronic Signature Policy Guidance" document, Section I.G. "Determining Which Electronic Signature Method to Use - Risk Assessment and Cost-Benefit Analysis", shall be used to determine the overall level of risk, and the specific approaches to be implemented to meet each of the following five requirements for legally binding signatures: 1) The Signer must use an acceptable electronic form of signature; 2) The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record; 3) The electronic form of signature must be attached to or associated with the electronic record being signed; 4) There must be a means to identify and authenticate a particular person as the signer; 5) There must be a means to preserve the integrity of the signed record.	---
1.6.1.g	The date and time a legally binding signature is executed, using Digital Signature or an Other Electronic Signature Method, shall be captured and incorporated as part of the record of the signature. The captured date and time must be accurate and trustworthy. Within DHS, legally binding signatures using a digital signature or other electronic signature method shall be executed on systems whose system clocks have been synchronized via Network Time Protocol (NTP) with DHS networks, and are managed to prevent unauthorized changes to the system clock. When the signature is executed, the date and time from the system clock shall be captured and incorporated as part of the record of the signature. When a legally binding signature must be executed on a system whose system clock is not synchronized via NTP and not managed to prevent unauthorized changes to the system clock, the signer is responsible for ensuring that the date and time incorporated as part of the record of the signature is accurate.	---
1.6.1.h	The visual context of an electronic signature implemented using digital signature or other electronic signature method, shall be maintained. The Relying Parties for the electronically signed document, transaction, communication, etc. must be able to view the exact format and content of the document, transaction, communication, etc. that the Signer saw when he or she signed it.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.1.i	Where a DHS entity is the Relying Party for an electronic signature executed on a non-DHS system by an external signer, using a digital signature or other electronic signature method, the DHS entity shall determine whether the asserted signing date and time is sufficiently accurate and trustworthy to be acceptable for the intended use of the signature.	---
1.6.1.j	Electronically signed records shall be maintained based on operational needs, perception of risks, and historical value, as formalized through corresponding Records Disposition Schedules approved by the National Archives and Records Administration (NARA). Operational needs shall be determined on the basis of the approach taken to ensure the availability, accessibility, and trustworthiness of electronically signed records over time.	---
1.6.1. k	The Component CISO shall approve the design, development, resources and infrastructure for implementations of electronic signatures using Digital Signatures or Other Electronic Signature Methods. The adoption and integration of legally binding electronic signature capabilities into workflows, business processes, specific document types, etc., shall be reviewed and approved by the Component General Counsel and by the Component Chief Records Officer. Additional review/endorsement by other cognizant officials (e.g., Privacy Officer; Chief Financial Officer; Forms Management Officer; etc.) shall be obtained when appropriate.	---
1.6.1.l	All implementations of digital signatures or other electronic signature methods in DHS shall comply with the requirements of DHS Sensitive Systems Policy Directive 4300A. Existing (legacy) implementations of electronic signatures shall be brought into compliance with DHS Sensitive Systems Policy Directive 4300A as soon as is practical, but in no case later than 12 months, or a waiver must be obtained. The waiver shall be requested in writing and submitted to the DHS CISO.	---

1.6.2 Digital Signatures

The following policy statements are applicable only to digital signatures.

<table>
<tr><th>Policy ID</th><th>DHS Policy Statements</th><th>Relevant Controls</th></tr>
<tr><td>1.6.2.a</td><td>
<p>Digital signatures shall not be accepted unless the following conditions are met:</p>
<p>1) Standard Path Development and Validation (PDVAL) software verifies the validity of the signer’s signature verification certificate as of the time the signature was executed; and</p>
<p>2) The certificate is authorized for signature use (i.e., has the digital signature and non-repudiation key usage bits set in the keyUsage extension); and</p>
<p>3) The certificate was;</p>
<p>i) Issued by DHS Principal Certification Authority (CA) (DHS CA4) under one of the following U.S. Common Policy Framework certificate policies,</p>
<table>
<tr><th>Policy</th><th>Policy Object Identifier</th></tr>
<tr><td><i>id-fpki-common-policy</i></td><td>::= {2 16 840 1 101 3 2 1 3 6}</td></tr>
<tr><td><i>id-fpki-common-hardware</i></td><td>::= {2 16 840 1 101 3 2 1 3 7}</td></tr>
<tr><td><i>id-fpki-common-High</i></td><td>::= {2 16 840 1 101 3 2 1 3 16}</td></tr>
</table>
<p>as indicated by the Policy Object Identifier (OID) entered in the <i>Certificate Policies</i> extension in the certificate; or</p>
<p>ii) Issued by another U.S. Federal Government (CA that is subordinate to the U.S. Common Root CA under one of the following U.S. Common Policy Framework certificate policies,</p>
<table>
<tr><th>Policy</th><th>Policy Object Identifier</th></tr>
<tr><td><i>id-fpki-common-policy</i></td><td>::= {2 16 840 1 101 3 2 1 3 6}</td></tr>
<tr><td><i>id-fpki-common-hardware</i></td><td>::= {2 16 840 1 101 3 2 1 3 7}</td></tr>
<tr><td><i>id-fpki-common-High</i></td><td>::= {2 16 840 1 101 3 2 1 3 16}</td></tr>
</table>
<p>as indicated by the Policy OID entered in the <i>Certificate Policies</i> extension in the certificate; or</p>
<p>iii) Issued by a CA from another PKI cross-certified with the Federal Bridge Certification Authority (FBCA), where the certificate is issued under a certificate policy that maps to one of the following FBCA certificate policies,</p>
</td><td>---</td></tr>
</table>

<table>
<tr><th>Policy ID</th><th>DHS Policy Statements</th><th>Relevant Controls</th></tr>
<tr><td></td><td>
<table>
<tr><th>Policy</th><th>Policy Object Identifier</th></tr>
<tr><td><i>id-fpki-certpcy-mediumAssurance</i></td><td>::= { 2 16 840 1 101 3 2 1 3 3 }</td></tr>
<tr><td><i>id-fpki-certpcy-mediumHardware</i></td><td>::= { 2 16 840 1 101 3 2 1 3 12 }</td></tr>
<tr><td><i>id-fpki-certpcy-highAssurance</i></td><td>::= { 2 16 840 1 101 3 2 1 3 4 }</td></tr>
<tr><td><i>id-fpki-certpcy-pivi-hardware</i></td><td>::= { 2 16 840 1 101 3 2 1 3 18 }</td></tr>
</table>
as indicated by the <i>PolicyMappings</i> extension in the cross-certificate issued by the FBCA to the Root CA for the Signer’s PKI, mapping an appropriate FBCA policy OID from the table above to the policy OID in the <i>Certificate Policies</i> extension from the Signer’s certificate.
</td><td></td></tr>
<tr><td>1.6.2.b</td><td>If a digital signature is time stamped by a Trusted Timestamp Authority approved by the DHS CISO, DHS relying parties for the signature shall accept the time stamp as a trustworthy indicator that the digital signature was executed prior to that time.</td><td>---</td></tr>
<tr><td>1.6.2.c</td><td>For electronic documents, transactions, communications, etc. containing legally binding digital signatures, a visible signature block containing information about the signer and the signature shall be embedded for each signature, when possible. The visible signature block for each signature shall be located in proximity to, but after the statement in the document, transaction, communications, etc. indicating the intent of that signature.
The visible signature block shall be formatted to clearly indicate that it is a block of information about the signature, and shall contain:
1) The name of the signer (mandatory)
2) The Role of the signer (mandatory)
3) The date and time the signature was executed (mandatory)
4) A graphical depiction or image of the signer’s handwritten signature (recommended)
5) Additional information as appropriate (optional)
The presence of a visual signature block shall not be used to indicate that a digital signature has been validated. A relying party must validate a digital signature using standard Path Development and Validation (PDVAL) protocols each time they make a determination to trust on not trust the digital signature.</td><td>---</td></tr>
<tr><td>1.6.2.d</td><td>Since any change to a digitally signed record will prevent validation of the digital signature, the use of stable file formats, with broad product support for</td><td>---</td></tr>
</table>

Policy ID	DHS Policy Statements	Relevant Controls
	backwards compatibility is essential to maintaining digitally signed records. Electronic documents, transactions, communications, etc. to be digitally signed shall be limited to file formats that will be stable over the retention period of the signed record. Suggested stable standard file formats include, but are not limited to: 1) American Standard Code for Information Exchange (ASCII)(.txt) 2) Portable Document Format (.pdf), ISO 3200 3) Open Office Extended Markup Language (XML) File Formats, ECMA-376, ISO/IEC 29500 i) XML Document Format (.docx) ii) XML Workbook Format (.xlxs) iii) XML Presentation Format (.pptx)	
1.6.2.e	Using a combination of digital signatures and handwritten signatures on a single document, transaction, message, etc. shall be avoided whenever possible, to ensure that a single record can be created where all of the signatures are part of the record and can be validated by Relying Parties.	---
1.6.2.f	In order to facilitate interoperability, DHS implementations of digital signatures shall comply with the PDF Advanced Electronic Signature (PAdES) standard or XML Advanced Electronic Signature (XAdES) standard for digital signature formats.	---
1.6.2.g	For DHS electronic records that are digitally signed, the digital signatures shall be verifiable by relying parties for the entire retention period of the record. The digital signatures shall be verifiable using standard PDVAL protocols (http://www.idmanagement.gov/path-discovery-and-validation).	---
1.6.2.h	When a digital signature is applied to an email by a DHS entity, it shall be for security purposes only, i.e., to enable the recipient or a third party to determine the source of the email and its integrity. Email may be used as a transport mechanism to send documents, transactions, messages, etc., that include legally binding digital signatures, as attachments to an email. If an email is received containing a digital signature that is intended to be legally binding, the source of the email shall be contacted and asked to re-submit the relevant content signed with the legally binding signature as an email attachment, or via another acceptable means.	---
1.6.2.i	A public-private key pair is only valid for the uses specified in the public key's certificate. Only private keys with an associated public key certificate that asserts both the digital signature and non-repudiation bits in the keyUsage	---

Policy ID	DHS Policy Statements	Relevant Controls
	extension shall be used to execute legally binding digital signatures. Digital signatures executed with a private key with associated public key certificate that does not assert both the digital signature and non-repudiation bits in the keyUsage extension shall be rejected (not accepted). Key pairs with associated public key certificates intended for authentication or encryption use shall not be used to execute digital signatures, and digital signatures generated with them shall not be accepted. Authentication certificates, such as the PIV Authentication Certificate and PIV Card Authentication Key certificate, do not assert the non-repudiation key usage bit, and shall not be used to execute digital signatures. Encryption certificates do not assert the digital signature bit or the non-repudiation bit and shall not be used to execute digital signatures. The three certificate types issued by DHS Principal Certificate Authority (CA) (DHS CA4) that are authorized for use for traditional human subscriber digital signatures are: 1) The PIV Digital Signature Certificate, 2) The Non-PIV Human Software Digital Signature Certificate, and 3) The Non-PIV Human Hardware Digital Signature Certificate. The following algorithms are currently authorized for digital signature use: 1) RSA 2048 with SHA-1 and PKCS #1 v1.5 padding 2) RSA 2048 with SHA-256 and PKCS #1 v1.5 padding 3) RSA 2048 with SHA-256 and PSS padding 4) ECDSA P-256 with SHA-256 ecdsa-with-SHA256 5) ECDSA P-384 with SHA-384 ecdsa-with-SHA384 The use of SHA-1 shall be abandoned in favor of SHA-256, as soon as possible.	
1.6.2.j	Digital signatures performed from a mobile device shall only be executed using the Signer's signature key on their PIV or PIV Derived Credential, in accordance with NIST Special Publication 800-157. Implementations of digital signatures to be performed from a mobile device, which are executed using the Signer's signature key from a software-based token and its associated public key certificate issued by DHS Principal CA (DHS CA4), must be authorized by the DHS CISO.	---
1.6.2.k	Public Key Infrastructure (PKI) artifacts (e.g., trust path Certification Authority Certificates, Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP) Responses) are stapled to a digital signature (i.e., incorporated into the signature data) to ensure that it can be validated in the future. OCSP Responses shall be used instead of CRLs whenever possible, to limit the size of digitally signed electronic records.	---

Policy ID	DHS Policy Statements	Relevant Controls
1.6.2.l	PIN caching shall not be used with legally binding digital signatures. In a session where the user is required to execute multiple legally binding digital signatures, the user shall be required to authenticate himself/herself immediately prior to the execution of each legally binding digital signature.	---
1.6.2.m	The key pairs and associated public key certificates issued to Non Person Entities (NPE) (such as devices, systems, and applications) by the DHS Principal CA (DHS CA4) or acquired from authorized commercial vendors, shall not be used to generate legally binding digital signatures. Certificates issued to NPEs by DHS Internal Use NPE CAs shall only be used for authentication and shall not be used for digital signature.	---

Implementations of digital signatures should adhere, where possible, to the guidance provided in the current versions of the following documents, developed by the DHS Enterprise Digital Signature Capability Integrated Project Team and maintained by the DHS PKI Management Authority:

1) “Using the PIV Card to Digitally Sign Outlook Emails”
2) “Using the PIV Card to Digitally Sign Adobe Acrobat Documents”
3) “Using the PIV Card to Digitally Sign Microsoft Office Documents”

These documents are available for download from the Enterprise Digital Signature folder in the DHS PKI SharePoint site.

1.7 Information Sharing

The DHS Security Operations Center (SOC) exchanges information with Component SOCs, Network Operations Centers (NOC), the Homeland Secure Data Network (HSDN) SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from information obtained from “raw” fault, Configuration Management (CM), accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

The DHS SOC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to Component SOCs, Component CISOs/ISSMs and other identified Component points of contact.

The DHS SOC portal implements role-based user profiles that allow Components to use the website’s incident database capabilities. Users assigned to Component groups shall be able to perform actions such as:

- Entering incident information into the DHS SOC incident database
- Generating preformatted incident reports
- Initiating queries of the incident database
- Viewing FISMA incident reporting numbers
- Automating portions of the Information Security Vulnerability Management (ISVM) program
- Automating portions of the vulnerability assessment program

1.8 Threats

Emphasis on e-Government has added the general public to the class of Government computer users and has transferred the repository for official records from paper to electronic media.

Information systems are often connected to different parts of an organization; interconnected with other organizations' systems; and with the Internet. Remote access for telecommuting and building management services (e.g., badge systems; heating, ventilating, and air-conditioning (HVAC); and entry) may require additional connections, all of which introduce additional risks.

Wireless mobile systems such as cell phones and pagers, allow personnel to stay in touch with their offices and wireless local area networks (WLAN) permit connection from various locations throughout a building. While these technologies provide greater flexibility and convenience, they also introduce additional risks.

As technologies continue to converge, (cell phones with Internet access, walkie-talkie communications, and video; low cost Voice over Internet Protocol [VoIP]; copiers that allow network printing; printing over the Internet; and facsimile [fax] functions) operating costs are reduced, making their implementation tempting;, but each of these technology advancements contains inherent security risks and presents challenges to security professionals.

1.8.1 Insider Threats

Managers are generally aware of natural and physical threats, such as earthquakes, tornadoes, fires, floods, electric outages, and plumbing disasters, but may not have the same level of awareness regarding threats originating from within their organizations. The threat from DHS users should not be underestimated. Sensitive information can be lost, corrupted, or compromised through malicious or careless acts. A malicious user can intentionally cause harm to the Department's reputation and data. Uninformed or careless users can inflict similar damage.

Converging technologies combine the vulnerabilities of the individual technologies, so care must be taken to ensure that systems are designed with no single points of failure (for example, if the building HVAC were connected to the data network it would become necessary to ensure that an outage or attack on the HVAC would not also cause a network outage).

1.8.2 Criminal Threats

Malicious code continues to be a threat to DHS systems. Malware and those who employ it have become very sophisticated. Malicious code can be tailored to the recipient. This code can be transferred to an unsuspecting user's machine by various means, including email, visiting infected websites, or across a network. These capabilities may be used to steal, alter, or destroy data; export malicious code to other systems; add backdoors that would permit access to data or network resources; or prevent the legitimate use of the individual computer or network service.

Instructions for exploiting hardware or software vulnerabilities are often available on hacker sites within hours of discovery. Skilled hackers routinely target e-commerce sites to obtain credit card numbers. Persons with hacking skills are often hired to perform espionage activities.

1.8.3 Foreign Threats

Foreign Governments routinely conduct espionage activities to obtain information that will be useful to their own industrial/government base and operations. They also have the resources to disrupt Internet communications and have launched successful cyber-attacks.

Eavesdropping on wireless communications with commercially available equipment is common; it is relatively easy to detect and exploit wireless access points. Employees overseas should assume that their wireless communications (BlackBerry, cell phone, etc.) are being monitored.

Many software manufacturers outsource software code development, which raises concerns about whether or not malicious code has been inserted. Indeed, it is becoming increasingly difficult to determine the actual provenance of an organization's information systems because code and equipment are assembled from so many sources.

1.8.4 Lost or Stolen Equipment

Lost or stolen equipment also poses a threat. Data on portable computing devices (laptops, smart phones, etc.) or storage media (Universal Serial Bus (USB) drives, compact disks (CD), etc.) can reveal sensitive information, such as changes to legislation, investigations, or economic analyses. Thefts from offices, airports, automobiles, and hotel rooms occur regularly.

1.8.5 Supply Chain Threats

A *supply chain threat* is a man-made threat achieved through exploitation of the system's supply chain or acquisition process.

A system's *supply chain* is composed of the organizations, people, activities, information, resources, and facilities for designing, creating and moving a product or service from suppliers through to the integrated system (including its sub-Components), and into service by the original acquirer.

1.9 Changes to Policy

Procedures and guidance for implementing this policy are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook* and its attachments. The Handbook serves as a foundation for Components to use in developing and implementing their information security programs.

For interpretation or clarification of DHS information security policies found in this policy document and of the procedures and guidance found in the *DHS 4300A Sensitive Systems Handbook*, contact the Director of IT Security Policy and Remediation at infosecpolicy@hq.dhs.gov.

Changes to this policy and to the Handbook may be requested by the form included in *DHS 4300A Sensitive Systems Handbook*, Attachment P, "Document Change Requests."

Policy ID	DHS Policy Statements	Relevant Controls
1.9.a	The DHS CISO shall be the authority for interpretation, clarification, and modification of the *DHS Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook* (inclusive of all Attachments and appendices).	PL-1
1.9.b	The DHS CISO shall update the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* at least annually.	PL-1

2.0 ROLES AND RESPONSIBILITIES

Security is inherently a Government responsibility. Contractors, others working on behalf of the Department of Homeland Security (DHS), and other sources may assist in the performance of security functions, but a DHS employee must always be designated as the responsible agent for all security requirements and functions. This section outlines the roles and responsibilities for implementing these requirements.

2.1 Information Security Program Roles

Designated personnel play a major role in the planning and implementation of information security requirements. Roles directly responsible for information system security are described in the subsections that follow.

2.1.1 DHS Senior Agency Information Security Officer

Policy ID	DHS Policy Statements	Relevant Controls
2.1.1.a	The DHS Chief Information Security Officer (CISO) shall perform the duties and responsibilities of the DHS Senior Agency Information Security Officer (SAISO).	PL-1, PM-2

2.1.2 DHS Chief Information Security Officer

The DHS CISO shall implement and manage the DHS Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations.

The DHS CISO reports directly to the DHS Chief Information Officer (CIO) and is the principal advisor on information security matters.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.2.a	The DHS CISO shall implement and manage the DHS-wide Information Security Program.	PL-1, PM-2
2.1.2.b	The DHS CISO will serve as the CIO's primary liaison with the organization's Authorizing Officials (AO), information System Owners (SO) and Information Systems Security Officers (ISSO).	---

The DHS CISO:

- Implements and manages the Department-wide Information Security Program and ensures compliance with the Federal Information Security Modernization Act of 2014 (FISMA), Office of Management and Budget (OMB) directives, and other Federal requirements.
- Issues Department-wide information security policy, guidance, and architecture requirements for all DHS systems, networks, and IS-related supply chains. Security policies shall incorporate National Institute of Standards and Technology (NIST) guidance, as well as all applicable OMB memorandums and circulars.
- Facilitates development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.
- Serves as the principal Departmental liaison with organizations outside DHS in matters relating to information security.
- Establishes and institutionalizes contact with selected groups and associations within the security community:

a. To facilitate ongoing security education and training for organizational personnel;

b. To maintain currency with recommended security practices, techniques, and technologies; and

c. To share current security-related information including threats, vulnerabilities, and incidents.

- Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: (1) are developed and maintained; and (2) continue to be executed in a timely manner.

- Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
- Implements a threat awareness program that includes a cross-organization information-sharing capability.
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and authorizing DHS systems, and for reporting and managing systems-level FISMA data. This responsibility includes reviews and approval of Security Control Assessment plans, Contingency Plans, and security risk assessments.
- Consults with the DHS Chief Security Officer (CSO) on matters pertaining to physical security, personnel security, information security, investigations, and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure.
- Develops and implements procedures for detecting, reporting, and responding to information security incidents.
- Chairs the CISO Council. The Council is composed of all Component CISOs, and is the Department's primary coordination body for any issues associated with information security policy, management, and operations. Component CISOs and Information Systems Security Managers (ISSM) will be invited to CISO Council meetings as required.
- Maintains a comprehensive inventory of all general support systems (GSS) and major applications (MA) in use within the Department:
  - Security management for every GSS shall be under the direct oversight of either the DHS CISO (for enterprise systems) or a Component CISO/ISSM (for Component-specific GSSs).
  - MAs must be under the direct control of either a Component CISO or Component ISSM.
- Maintains a repository for all Information Assurance (IA) security authorization process documentation and modifications.
- Performs security reviews for all planned information systems acquisitions over $2.5 million and for additional selected cases.
- Provides oversight of all security operations functions within the Department.
- Maintains classified threat assessment capability in support of security operations.
- Performs annual program assessments for each of the Components.
- Performs periodic compliance reviews for selected systems and applications
- Publishes monthly Compliance Scorecards.
- Delegates specific authorities and assigns responsibilities to Component CISOs and ISSMs as appropriate for maintaining a high degree of compliance.

- Reports annually to the Secretary on the effectiveness of the Department information security program, including progress of remedial actions. The CISO's annual report provides the primary basis for the Secretary's annual report to both OMB and to the United States Congress that is required by FISMA.
- Assists senior Department officials concerning their responsibilities under FISMA.
- Heads an office with the mission and resources to assist in ensuring Department compliance with information security requirements.
- Appoints a DHS employee to serve as the Headquarters CISO.
- Appoints a DHS employee to serve as the Office of Intelligence and Analysis (I&A) CISO.
- Provides operational direction to the DHS Security Operations Center (SOC).

2.1.3 Component Chief Information Security Officer

The Component CISO implements and manages all aspects of the Component Information Security Program to ensure compliance with DHS policy and guidance implementing FISMA, other laws, and Executive Orders. The Component CISO shall report directly to the Component CIO on matters relating to the security of Component information systems. In order to ensure continuity of operations and effective devolution, large Components should ensure the designation of a Deputy CISO with full authorities, to include the roles of Risk Executive and Security Control Assessor upon the absence of the CISO.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.3.a	Component CISOs shall develop and maintain a Component-wide information security program in accordance with the DHS security program.	PL-1, PM-2 PM-6
2.1.3.b	All Components shall be accountable to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO.	---

The following Components shall have a fulltime CISO:

- Customs and Border Protection (CBP)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- United States Secret Service (USSS)
- United States Coast Guard (USCG)
- Federal Emergency Management Agency (FEMA)
- United States Citizenship and Immigration Services (USCIS)
- Federal Law Enforcement Training Center (FLETC)

- Headquarters, Department of Homeland Security
- Office of Intelligence and Analysis (I&A)
- National Protection and Programs Directorate (NPPD)
- Science and Technology (S&T)

Component CISOs shall:

- Serve as principal advisor on information security matters
- Report directly to the Component CIO on matters relating to the security of Component information systems
- Oversee the Component information security program
- Ensure that information security-related decisions and information, including updates to the 4300 series of information security publications, are distributed to the ISSOs and other appropriate persons within their Component
- Approve and/or validate all Component information system security reporting
- Consult with the Component Privacy Officer or Privacy Point of Contact (PPOC) for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Review and approve the security of hardware and software prior to implementation into the Component SOC
- Provide operational direction to the Component SOC
- Periodically test the security of implemented systems
- Implement and manage a Plan of Action and Milestones (POA&M) process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each information system managed at the Component level, and review and approve ISSO appointments
- Ensure that weekly incident reports are submitted to the DHS SOC
- Acknowledge receipt of Information System Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers
- Manage Component firewall rule sets
- Ensure that Interconnection Security Agreements (ISA) are maintained for all connections between systems that do not have the same security policy
- Ensure adherence to the DHS Secure Baseline Configuration Guides (*DHS 4300A Sensitive Systems Handbook*)

- Ensure reporting of vulnerability scanning activities to the DHS SOC, in accordance with *DHS 4300A Sensitive Systems Handbook* Attachment O, "Vulnerability Management Program."
- Develop and maintain a Component-wide information security program in accordance with Department policies and guidance
- Implement Department information security policies, procedures, and control techniques to ensure that all applicable requirements are met
- Ensure training and oversight of personnel with significant responsibilities for information security
- Oversee the Component's Security Authorization process for GSSs and MAs
- Maintain an independent Component-wide assessment program to ensure that there is a consistent approach to controls effectiveness testing
- Ensure that an appropriate SOC performs an independent network assessment as part of the assessment process for each authorized application
- Ensure that enterprise security tools are utilized
- Oversee all Component security operations functions, including the Component SOCs
- Ensure that external providers who operate information systems on behalf of the Component meet the same security requirements as required for government information and information systems.
- Ensure an acceptable level of trust for each external service, either by accepting risk or by using compensating controls to reduce risk to an acceptable level
- Ensure that systems engineering lifecycle activities implement processes that include software assurance and supply chain risk management
- Issue a Component Supply Chain Risk Management (SCRM) Plan that defines how Component programs and systems shall develop and execute their individual SCRM plans or adopt SCRM into Security Plans

Component CISO qualifications include:

- Training, experience, and professional skills required to discharge the responsibilities and functions of the position
- Ability to maintain a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance
- Ability to perform information security duties as primary duty
- Ability to participate in the DHS CISO Council
- Ability to head an office with the mission and resources to ensure the Component's compliance with this Policy Directive
- Ability to coordinate, develop, implement, and maintain an organization-wide information security program

- Ability to serve as the Component Risk Executive

2.1.4 Component Information Systems Security Manager

Components that are not required to have a fulltime CISO shall have a fulltime ISSM. The ISSM is designated in writing by the Component CIO, with the concurrence of the DHS CISO.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.4.a	Component ISSMs shall serve as the principal interface between the HQ CISO, Component ISSOs and other security practitioners.	---
2.1.4.b	The Component ISSM shall work directly with the HQ CISO.	---

The ISSM plays a critical role in ensuring that the DHS Information Security Program is implemented and maintained throughout the Component.

Component ISSMs shall:

- Oversee the Component information security program
- Ensure that the Component CIO and DHS CISO are kept informed of all matters pertaining to the security of information systems
- Ensure that all communications and publications pertaining to information security, including updates to the 4300 Policies and Handbooks, are distributed to the ISSOs and other appropriate persons within their Component
- Validate all Component information system security reporting
- Consult with the Component Privacy Officer or PPOC for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Test the security of the Component’s information systems periodically
- Implement and manage a POA&M process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each Component-managed information system
- Ensure that weekly incident reports are forwarded to the HQ CISO
- Acknowledge receipt of ISVM messages, report compliance with requirements, or notify applicants of the granting of waivers
- Ensure adherence to the DHS Secure Baseline Configuration Guides (*DHS 4300A Sensitive Systems Handbook*)

- Develop and publish procedures for implementation of DHS information security policy within the Component
- Implement Department information security policies, procedures, and control techniques to address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
- Oversee the Security Authorization process for the Component's MAs
- Maintain an independent Component-wide security control assessment program to ensure a consistent approach to controls effectiveness testing
- Ensure that an appropriate SOC performs an independent network assessment as part of the security control assessment process for each authorized application
- Ensure that enterprise security tools are used
- Ensure that ISSOs monitor and manage the information security aspects of supply chain risks
- Ensure that ISSOs adopt software assurance principles and tools

2.1.5 Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. In keeping with its organizational structure, DHS has two levels of Risk Executive: Departmental and Component. The risk executive provides a holistic view of risk beyond that associated with the operation and use of individual information systems. Risk Executive observations and analyses are documented and become part of the security authorization decision.

DHS Departmental and Component Risk Executives shall:

- Ensure that management of security risks related to information systems is consistent throughout the organization; reflects organizational risk tolerance; and is performed as part of an organization-wide process that considers other organizational risks affecting mission and business success
- Ensure that information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization
- Provide visibility into the decisions of AOs and a holistic view of risk to the organization beyond the risk associated with the operation and use of individual information systems, including those associated with the supply chain
- Facilitate the sharing of security-related and risk-related information among AOs and other senior leaders in the organization in order to help those officials consider all types of risks that could affect mission and business success and the overall interests of the organization at large

- Ensure that System Owners, ISSOs and AOs monitor and manage supply chain risks, as part of the overall Component risk management strategy.

The DHS Risk Executive develops information security policy, establishes the standards for system security risk, oversees risk management and monitoring, and approves all waivers to DHS policy.

Component Risk Executives may establish system security risk standards more stringent than DHS standards. Risk Executives implement the system security risk management and monitoring program and submit requests for higher-risk deviations from the enterprise standard.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.5.a	The DHS CIO shall be the DHS Risk Executive. The DHS CIO has delegated this authority to the DHS CISO.	PL-1, PM-9
2.1.5.b	Each Component CIO shall be the Risk Executive for his or her Component. The Component CIO may delegate this authority to the Component CISO.	PL-1, PM-9
2.1.5.c	The Risk Executive shall perform duties in accordance with NIST Special Publication (SP) 800-37.	---

2.1.6 Authorizing Official

The AO formally assumes responsibility for operating an information system at an acceptable level of risk. He or she shall be a senior management official and a Federal employee or member of the U.S. military. The AO shall assign the Security Control Assessor for the system.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.a	The DHS CIO shall act as the AO for enterprise information systems, excluding financial systems, or shall designate an AO in writing for DHS mission systems and for multi-Component systems without a designated AO.	CA-6
2.1.6.b	The Component CIO shall act as the AO for Component information systems, excluding financial systems, or shall designate an AO in writing all systems without a designated AO.	CA-6
2.1.6.c	Every system shall have a designated AO. (An AO may be responsible for more than one system.)	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.d	The AO shall be responsible for review and approval of any individual requiring administrator privileges. The AO may delegate the performance of this duty to the appropriate system owner or Program Manager.	AC-2
2.1.6.e	The AO shall be responsible for acceptance of remaining risk to organizational operations and assets, individuals, other organizations, and the Nation.	CA-6
2.1.6.f	The AO shall periodically review security status for all systems under his or her purview to determine if risk remains acceptable.	CA-6
2.1.6.g	The AO shall perform additional duties in accordance with NIST SP 800-37.	CA-6

2.1.7 Security Control Assessor

The Security Control Assessor is a senior management official whose responsibilities include certifying the results of the security control assessment. A Security Control Assessor is assigned in writing to each information system by the Component CISO. The Security Control Assessor and the team conducting a certification must be impartial. They must be free from any perceived or actual conflicts of interest with respect to the developmental, operational, and or management chains of command associated with the information system; or with respect to the determination of security control effectiveness.

For systems with low impact, a Security Control Assessor and/or certifying team does not need to be independent so long as assessment results are carefully reviewed and analyzed by an independent team of experts to validate their completeness, consistency, and truthfulness.

The AO decides the required level of assessor independence based on:

- The criticality and sensitivity of the information system
- The ultimate risk to organizational operations, organizational assets, and individuals
- The level of assessor independence required for confidence that the assessment results are sound and valid for making credible risk-based decisions

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7.a	The Component CISO shall serve as Security Control Assessor when no other person has been officially designated.	CA-2
2.1.7.b	A Security Control Assessor may be responsible for more than one system.	CA-2
2.1.7.c	The Security Control Assessor may take the lead for any or all remedial actions.	CA-7

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7d	The Security Control Assessor provides an assessment of the severity of weaknesses or deficiencies in the information systems, and prepares the final security control assessment report containing the results and findings from the assessment but not making a risk determination.	CA-7

2.1.8 Information Systems Security Officer

An ISSO performs security actions for an information system. Only one ISSO is assigned to a system, but multiple Alternate ISSOs may be designated to assist the ISSO.

While the ISSO performs security functions, responsibility for information system security always rests with the System Owner.

See *DHS 4300A Sensitive Systems Handbook,* Attachment C, "Information Systems Security Officer (ISSO) Designation Letter."

Policy ID	DHS Policy Statements	Relevant Controls
2.1.8.a	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
2.1.8.b	An ISSO shall ensure the implementation and maintenance of security controls in accordance with the Security Plan (SP) and DHS policies.	PL-1
2.1.8.c	ISSOs shall be federal or contractor employees whose background investigations have been completed in accordance with Section 4 of this Policy.	PL-1
2.1.8.d	An ISSO may be assigned to more than one system.	PL-1
2.1.8.e	ISSO duties shall not be assigned as collateral duties unless approved by the Component CISO.	PL-1
2.1.8.f	The ISSO shall have been granted a clearance and access greater than or equal to the highest level of information contained on the system. It is strongly encouraged that ISSOs be cleared to the Secret level in order to facilitate intelligence sharing among information security professionals.	---
2.1.8.g	The ISSO shall ensure that timely responses are provided to Infrastructure Change Control Board (ICCB) change request packages.	---

2.1.9 Ongoing Authorization Manager and Operational Risk Management Board

Each Component shall have an Ongoing Authorization (OA) Manager responsible for evaluating and tracking security events for systems operating under the DHS OA Program. Component OA Managers:

- Account for Component risk threshold
- Ensure that Component Risk Executives[see Sec. 2.1.5] are made aware of new risks and security issues
- Facilitate collaboration of the Component IT Security Subject Matter Experts (SME) that serve on the Operational Risk Management Board (ORMB). Component ORMBs determine the criticality of security triggers and the impact of triggers on the security posture of Component systems that are in OA. The ORMB determines the level of each trigger's visibility and recommends to the Component CISO and AO as adjudicators the actions required to mitigate the risks introduced. Refer to the *DHS Ongoing Authorization Methodology* for more information regarding the ORMB.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.9.a	An OA Manager shall be designated for every Component by the Component CISO and serve as the Point of Contact (POC) for all ongoing risk management for all Component systems enrolled in the OA Program.	PL-1
2.1.9.b	OA Manager duties may be assigned as collateral duties for personnel with existing security responsibilities.	PL-1
2.1.9.c	The OA Manager shall have been granted a security clearance and access greater than or equal to the highest level of information contained in Component systems.	---
2.1.9.d	The OA Manager shall ensure that timely analysis (as outlined by the DHS OA Methodology) of identified security events or triggers is provided to the Component ORMB in support of an accountable environment between the ORMB and the OA Manager.	---
2.1.9.e	The Component CISO shall appoint the Chair of the Component ORMB.	---
2.1.9.f	The OA Manager or designee shall be responsible for tracking security events in the monthly Trigger Accountability Log (TRAL), communicating and recording recommendations for Component CISO consumption, and ensuring at least quarterly communication with the AO on system risks.	---

2.1.10 DHS Security Operations Center

The DHS Enterprise SOC (DHS SOC) is charged to act as a single point for DHS enterprise-wide cyber situational awareness. As such, DHS Enterprise SOC provides incident management oversight for all incidents detected and reported from all sources. DHS Enterprise SOC also provides the first line of active defense against all cyber threats by monitoring all perimeter network gateways. Lastly, DHS Enterprise SOC oversees the department-wide vulnerability management program.

The DHS SOC has functional, advisory, and reporting responsibilities that include the following:

- Review all reported incidents and verify that all pertinent information is recorded, confirmed, and that closure occurs only after all remediation and reporting activities have occurred in accordance with this Policy Directive.
- Focus 24x7 monitoring efforts on shared DHS infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Points (PEP), Email Security Gateway (EMSG), Demilitarized Zones (DMZ), Virtual Private Networks (VPN) and other devices as required by DHS CISOs to identify security events of interest that require confirmation, escalation, or declaration as false positive.
- Create Security Event Notifications (SEN) based on monitoring and analysis activities when events of interest are identified that require further investigation.
- Provide oversight on investigational activities and review SENs prior to escalation. SENs will be escalated when Components have sufficiently demonstrated that adequate investigation has been performed and that the event is a verified incident. The Component must provide necessary information regarding the event in accordance with the escalation criteria outlined in Appendix F3, “Response Guidelines”.
- Review all SENs for closure and close SENs after all reasonable investigational activities have been completed.
- Conduct operations and maintenance and approve changes on all security monitoring devices associated with shared DHS infrastructure (such as Intrusion Detection System (IDS), Data Loss Prevention (DLP).
- Provide oversight and guidance for all incidents to ensure adherence to DHS Sensitive Systems Policy Directive 4300A.
- Serve as the primary clearinghouse and collection point for information related to incidents involving DHS systems or networks.
- Coordinate privacy and security incident handling activities with DHS entities such as the DHS Office of Security and the DHS Privacy Office.
- Ensure that remediation and all necessary coordination activities are completed before incident closure.
- Analyze incidents, identifying and notifying other stakeholders and DHS Components and Data Center SOCs that may be affected.

- Provide technical and investigative assistance to Components and Data Center SOCS as needed.
- Provide accurate and timely reports to the DHS CISO on significant incidents and on the status of DHS enterprise computer security.
- Develop and maintain an incident database that contains information on all discovered and reported incidents.
- Provide automated incident notification and reporting to senior DHS and Component leadership and stakeholders such as the DHS Privacy Office and the DHS Office of Security, as well as external reporting entities such as the United States Computer Emergency Readiness Team (US-CERT).
- Update US-CERT on incident status as required.
- Facilitate communications between DHS Components and Data Center SOCS (when applicable) for those incidents involving more than one Component (i.e., Master incidents).
- Provide ad hoc incident trending reports as requested by the DHS CISO.

2.1.11 DHS Component Security Operations Centers

Component SOCs have functional, advisory, and reporting responsibilities in incident response that include the following:

- Focus security monitoring efforts on the Component network.
- Compile and maintain a list of mission-critical systems, financial systems, and applications. The list will assist in determining the classification of the Component's systems, and in prioritization of security incidents.
- Component SOCs shall develop and publish internal computer security incident response plans and incident handling procedures, with copies provided to the DHS Enterprise SOC upon request.
- Investigate SENS and Incidents created by the DHS Enterprise SOC and comply with reporting timelines and escalation criteria outlined in *DHS 4300A Sensitive Systems Handbook* Attachment F, "Incident Response," Appendix F3, "Response Guidelines" to either escalate the SEN or close it.
- Monitor internal network enclave traffic such as firewall logs and Network IDS) and host-based security events (e.g. audit logs and Host-based Intrusion Prevention Systems (IPS) and IDS). This includes workstation activity, internal server enclaves, Component-managed externally accessible applications and networks (e.g. DMZ, VPN), and applications hosted by third parties external to DHS.
- Request SEN escalation by the DHS Enterprise SOC, within the reporting timeframes and meeting the escalation criteria outlined in *DHS 4300A Sensitive Systems Handbook* Attachment F, "Incident Response," Appendix F3, "Response Guidelines."
- Conduct SEN and incident investigation including traceback to the host.

- Request closure when a SEN has been identified as inconclusive or as a false positive after providing adequate explanation of investigational activities via the Enterprise Operations Center Portal (EOConline).
- Respond to DHS ENTERPRISE SOC on SEN investigation activities based on the escalation criteria in *DHS 4300A Sensitive Systems Handbook* Attachment F, “Incident Response,” Appendix F3, “Response Guidelines.”
- Ensure 24x7 incident handling function exists for the Component.
- Lead the Component’s incident handling and response activities, including identification, investigation, containment, eradication, and recovery. Coordinate incident response, investigation, and reporting to the DHS Enterprise SOC. Reporting should include all significant data, such as the who, what, when, where, why, and how of a given incident. Coordinate incident handling activities with internal Component entities such as the Component Office of Security, Component Privacy Office, and Internal Affairs.
- Coordinate Component-level remediation efforts as mandated by DHS security policies and communicate remediation activity to DHS Enterprise SOC through EOConline log entries.
- Share applicable information Department-wide or Component-wide, for example by providing network and host-based indicators for malicious logic incidents; such indicators will facilitate implementation of proactive measures to prevent future incidents.
- Provide updates to the DHS Enterprise SOC for significant incidents whenever additional information becomes available.
- Request closure of incidents when Component remediation and mitigation actions have concluded.
- Assist other Components with technical or investigation assistance as requested by the DHS Enterprise SOC.
- Use security automation tools and technologies that facilitate efficient machine and human data exchange with the DHS SOC, with the National Cybersecurity and Communications Integration Center (NCCIC), and with peer SOCs to the maximum extent possible.

2.2 Other Roles

Roles related to but not directly responsible for information system security are described in the subsections that follow.

2.2.1 Secretary of Homeland Security

The Secretary of Homeland Security is responsible for fulfilling the Department’s mission, which includes ensuring that DHS information systems and their data are protected in accordance with Congressional and Presidential directives. The Secretary’s role with respect to information system security is to allocate adequate resources.

To that end, the Secretary:

- Ensures that DHS implements its Information Security Program throughout the life cycle of each DHS system
- Submits the following to the Director, OMB:
  - The DHS CIO's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance
  - The results of an annual independent information security program evaluation performed by the DHS Office of Inspector General (OIG)
  - The Senior Agency Official for Privacy's (SAOP) annual assessment of the Department's privacy policies, procedures, and practices
- Provides information security protection commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Department, and on information systems used or operated by the Department, or by a contractor or other organization on behalf of the Department
- Ensures that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the Department's operations
- Ensures that information security processes are integrated with strategic and operational planning processes to secure the Department's mission
- Ensures that the Department's senior officials have the necessary authority to secure the operations and assets under their control
- Delegates authority to the CIO to ensure compliance with applicable information security requirements

2.2.2 Under Secretaries and Heads of DHS Components

The Under Secretaries and Heads of DHS Components are responsible for oversight of their Components' information security program, including the appointment of CIOs. Undersecretaries and Heads of Components allocate adequate resources to information systems for information system security.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.2.a	The Under Secretaries of Homeland Security and Heads of Components shall ensure that information systems and their data are sufficiently protected.	PL-1

Under Secretaries and the Heads of DHS Components:

- Appoint CIOs
- Ensure that an Information Security Program is established and managed in accordance with DHS policy and implementation directives
- Ensure that the security of information systems is an integral part of the life cycle management process for all information systems developed and maintained within their Components
- Ensure that adequate funding for information security is provided for Component information systems and that adequate funding requirements are included for all information systems budgets
- Ensure that information system data are entered into the appropriate DHS Security Management Tools to support DHS information security oversight and FISMA reporting requirements
- Ensure that the requirements for an information security performance metrics program are implemented and the resulting data maintained and reported

2.2.3 DHS Chief Information Officer

The DHS CIO is the senior agency executive responsible for all DHS information systems and their security as well as for ensuring FISMA compliance.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.3.a	The DHS CIO shall develop and maintain the DHS Information Security Program.	PL-1, PM-7, PM-8
2.2.3.b	The DHS CIO designates the DHS CISO.	PL-1

The DHS CIO:

- Heads the office with the mission and resources to assist in ensuring Component compliance with the DHS Information Security Program
- Oversees the development and maintenance of a Department-wide information security program
- Appoints in writing a DHS employee to serve as the DHS CISO
- As appropriate, serves as or appoints in writing the AO for DHS enterprise information systems.
- Ensures the development of DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide security program

- Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensures that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes
- Ensures that System Owners understand and appropriately address risks, including supply chain risk and risks arising from interconnectivity with other programs and systems outside their control
- Reviews and evaluates the DHS Information Security Program annually
- Ensures that an information security performance metrics program is developed, implemented, and funded
- Reports to the DHS Under Secretary for Management on matters relating to the security of DHS systems
- Ensures compliance with applicable information security requirements
- Implements firewall changes as requested by DHS and Component CISOs
- Coordinates and advocates resources for enterprise security solutions
- Leads the DHS Contingency Planning program

2.2.4 Component Chief Information Officer

The Component CIO is responsible for Component information systems and their security as well as for ensuring FISMA compliance within the Component.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.4.a	The Component CIO shall develop and maintain the Component Information Security Program.	PL-1, PM-1

Component CIOs:

- Establish and oversee their Component information security programs
- Direct a review of the Component information security program plan be performed with a frequency depending on risk, but no less than annually
- Ensure that an AO has been appointed for every Component information system; serves as the AO for any information system for which no AO has been appointed or where a vacancy exists

- Ensure that information security concerns are addressed by Component Configuration Control Boards, Enterprise Architecture Board (EAB), Acquisition Review Board (ARB), and Investment Review Board (IRB)
- Ensure that an accurate information systems inventory is established and maintained
- Ensure that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensure that System Owners understand and appropriately address risks, including supply chain risk and risks arising from interconnectivity with other programs and systems outside their control
- Ensure that an information security performance metrics program is developed, implemented, and funded
- Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or the possibility of public concern
- Ensure that incidents are reported to the DHS SOC within the timeframes defined in Attachment F, “Incident Response” of the *DHS 4300A Sensitive Systems Handbook*
- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.
- Ensure compliance with DHS information systems security policy
- Coordinate and advocate resources for information security enterprise solutions

CIOs of the following Components shall appoint a CISO that reports directly to the Component CIO and shall ensure that the CISO has resources to assist with Component compliance with policy. CISOs shall be DHS employees.

- CBP
- FEMA
- FLETC
- ICE
- TSA
- USCIS
- USCG
- USSS

CIOs of all other Components shall:

- Ensure that Component ISSMs have been appointed
- Provide the resources and qualified personnel to ensure Component compliance with DHS security policy

2.2.5 DHS Chief Security Officer

The DHS CSO implements and manages the DHS Security Program for DHS facilities and personnel.

The CSO is a senior agency official who reports directly to the Deputy Secretary on all matters pertaining to facility and personnel security within the DHS.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.5.a	DHS information systems that control physical access shall be approved by the DHS CSO to operate in accordance with this policy document, whether they connect to other DHS information systems or not.	CA-1
2.2.5.b	The DHS CSO shall be the AO for all systems automating or supporting physical access controls or shall appoint an AO for each of those systems.	CA-6

2.2.6 DHS Chief Privacy Officer

The DHS Chief Privacy Officer is the head of the DHS Privacy Office and is responsible for establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy. The DHS Chief Privacy Officer ensures that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of Personally Identifiable Information (PII). The responsibilities of the DHS Chief Privacy Officer include oversight of all privacy activities within the Department, and ensuring compliance with privacy laws, regulations, and policies.

The DHS Chief Privacy Officer coordinates with the CIO and the CISO to provide guidance regarding information technology and technology-related programs and to develop and implement policies and procedures to safegaurd PII used or maintained by the Department in accordance with federal law and policy.

The DHS Chief Privacy Officer coordinates with Component Privacy Officers and Privacy PPOC with policy compliance at the Component level.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.6.a	The DHS Chief Privacy Officer shall review all Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.	AR-2, PL-1,

Policy ID	DHS Policy Statements	Relevant Controls
2.2.6.b	The DHS Chief Privacy Officer shall lead and oversee the implementation of and compliance with the NIST SP 800-53 Appendix J, "*Privacy Control Catalog.*" Implementation of Appendix J controls is in coordination with the CIO, CISO, program officials, legal counsel, and others as appropriate. No Authority to Operate (ATO) shall be issued without the DHS Chief Privacy Officer's approval signifying that a system is in compliance with NIST SP 800-53 Appendix J.	AR-1
2.2.6.c	The DHS Chief Privacy Officer shall establish and chairs a Data Integrity Board to review all Computer Matching Agreements (CMA).	DI-2
2.2.6.d	The DHS Chief Privacy Officer shall ensure that the public has access to information about DHS privacy activities and is able to communicate with DHS Privacy Officials; and shall ensure that privacy practices are publicly available through DHS' public facing website.	TR-3
2.2.6.e	The DHS Chief Privacy Officer monitors and audits privacy controls and internal privacy policy during the privacy compliance process to ensure effective implementation.	AR-4
2.2.6.f	The DHS Chief Privacy Officer implements a process for receiving and responding to complaints, concerns, or questions from individuals about DHS' privacy practices.	IP-4

The DHS Chief Privacy Officer, as the SAOP:

- Develops, implements, and maintains a Department-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems
- Monitors federal privacy laws and policy for changes that affect the privacy program
- Allocates sufficient resources to implement and operate the Department-wide privacy program
- Develops a strategic Department privacy plan for implementing applicable privacy controls, policies, and procedures
- Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII
- Updates privacy plans, policies, and procedures biennially

- Oversees privacy incident management, to include providing guidance to Components, and where appropriate coordination with Components responding to suspected or confirmed privacy incidents
- Coordinates with the DHS CIO, DHS CISO, the DHS SOC, and senior management regarding privacy incidents
- Convenes and chairs incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG)
- Reviews and approves all Department Privacy Compliance Documentation, including PTAs, PIAs, and SORNs
- Designates Privacy Sensitive Systems as part of the Risk Management Framework based on approved PTAs. Privacy Sensitive Systems are those that maintain PII
- Ensures that the Department meets all reporting requirements mandated by Congress or OMB regarding DHS activities that involve PII or otherwise impact privacy
- Provides department-wide annual and refresher privacy training

2.2.7 DHS Chief Financial Officer

The DHS Chief Financial Officer (CFO) implements and manages the DHS Financial Program, including oversight of DHS financial systems. The DHS CFO designates financial systems and oversees security control definitions for financial systems.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.a	The DHS CFO, or their designee, shall be the AO for applicable financial systems or mixed financial systems and oversee security control definitions for those systems.	CA-6
2.2.7.b	The DHS CFO has directed that the Component CFO shall be the AO for all applicable financial mission applications managed at the Component level.	CA-6
2.2.7.c	The DHS CFO shall designate the financial systems that fall under the DHS CFO-mandated policy statements.	CA-6
2.2.7.d	The DHS CFO shall publish a comprehensive list of designated financial systems during the fourth quarter of every fiscal year. (This list shall be referred to as the CFO Designated Systems List.)	CA-6

All systems on the CFO Designated Systems List are required to comply with the policies defined in Sections 3.5.1 and 3.15.

2.2.8 Program Managers

Program Managers ensure compliance with applicable Federal laws and DHS policy directives governing the security, operation, maintenance, and privacy protection of information systems, information, projects, and programs under their control.

Program Managers are responsible for program-level POA&Ms that may impact one or more systems.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.8.a	Program Managers shall ensure that program POA&Ms are prepared and maintained.	CA-5, PM-4
2.2.8.b	Program Managers shall prioritize security weaknesses for mitigation.	CA-5
2.2.8.c	Program Managers shall provide copies of program POA&Ms to affected System Owners.	CA-5, PM-4
2.2.8.d	Program Managers shall ensure that POA&Ms address the following: ▪ known vulnerabilities in the information system ▪ the security categorization of the information system ▪ the specific weaknesses or deficiencies in the information system security controls ▪ the importance of the identified security control weakness or deficiencies ▪ the Component's proposed risk mitigation approach, while addressing the identified weaknesses or deficiencies in the security controls and the rationale for accepting certain weaknesses or deficiencies in the security controls	CA-5 PM-4
2.2.8.e	Program Managers shall determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.	AP-1
2.2.8.f	Program Managers shall ensure compliance with SCRM Plans and consider supply chain risks, as identified by the System Owner, when prioritizing security weaknesses for mitigation.	---

2.2.9 System Owners

System Owners use Information Technology (IT) to help achieve the mission needs within their program area of responsibility. They are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. For proper administration of security, an shall be designated in writing for each system by the AO.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.9.a	System Owners shall ensure that each of their systems is deployed and operated in accordance with this policy document.	PL-1
2.2.9.b	System Owners shall ensure that an ISSO is designated in writing for each information system under their purview.	PL-1
2.2.9.c	There shall be only one System Owner designated for each DHS system.	PL-1
2.2.9.d	The System Owner shall ensure information security compliance, development and maintenance of security plans, user security training, notifying officials of the need for security authorization and need to resource.	CA-2
2.2.9.e	System Owners shall ensure development of a POA&M to address weaknesses and deficiencies in the information system and its operating environment.	CA-2
2.2.9.f	The DHS CIO shall designate a System Owner in writing for DHS mission systems and for multi-Component systems.	---
2.2.9.g	The Component CIO shall designate an AO in writing for Component systems.	---
2.2.9.h	Where systems or programs provide common controls, the System Owners shall ensure that a security control assessment is completed in the Information Assurance Compliance System (IACS) for those common controls.	---
2.2.9.i	System Owners shall ensure that risk management activities include addressing supply chain risks for the system’s current and all subsequent lifecycle phases and documenting this activity in the SCRM Plan.	---

2.2.10 Common Control Provider

The Common Control Provider is an organizational official responsible for planning, development, implementation, assessment, authorization, and maintenance of common controls.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.10.a	The Common Control Provider shall document all common controls and submit them to the AO.	PM-1
2.2.10.b	The Common Control Provider ensures that required assessments of common controls are carried out by qualified assessors with the appropriate level of independence.	PM-1

2.2.10.c	The Common Control Provider documents assessment findings in a Security Assessment Report (SAR).	PM-1
2.2.10.d	The Common Control Provider ensures that POA&Ms are developed for all controls having weaknesses or deficiencies.	PM-4
2.2.10.e	The Common Control Provider shall make available security plans, SARs, and POA&Ms for common controls to information System Owners inheriting those controls after the information is reviewed and approved by a senior official.	PM-1, PM-4

2.2.11 DHS Employees, Contractors, and Others Working on Behalf of DHS

DHS employees, contractors, and others working on behalf of the DHS or its agencies shall follow the appropriate set(s) of rules of behavior.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.11.a	DHS users shall follow prescribed rules of behavior. (See *DHS 4300A Sensitive Systems Handbook*, Attachment G, “Rules of Behavior.”	PL-4

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

Basic security management principles must be followed in order to ensure the security of Department of Homeland Security (DHS) information resources. These principles are applicable throughout the Department and form the cornerstone of the DHS Information Security Program.

Component Chief Information Security Officers (CISO) and Information Systems Security Managers (ISSM) shall submit all security reports concerning DHS systems to the Component senior official or designated representative. Component CISOs/ISSMs shall interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. Component CISOs/ISSMs shall also answer data queries from the DHS CISO and develop and manage information security guidance and procedures unique to Component requirements.

Information Systems Security Officers (ISSO) are the primary points of contact for the information systems assigned to them. They develop and maintain Security Plans (SP) and are responsible for overall system security.

Policy ID	DHS Policy Statements	Relevant Controls
3.1.a	Every DHS computing resource (desktop, laptop, server, wireless mobile device, etc.) shall be individually accounted for as part of a FISMA[1]-Inventoried information system.	CM-8
3.1.b	The Component Chief Information Officer (CIO), in cooperation with each of the Component's senior officials, shall ensure that every DHS computing resource is identified as an information system or as a part of an information system, either as an Major Application (MA) or as a General Support System (GSS).	CM-8
3.1.c	The System Owner or designee shall develop and maintain a Security Plan (SP) for each information system. Component Authorizing Officials (AO) shall review and approve SPs.	PL-2
3.1.d	An ISSO shall be designated for every information system and serve as the Point of Contact (POC) for all security matters related to that system.	PL-1
3.1.e	Component information security programs shall be structured to support DHS and applicable FISMA, Office of Management and Budget (OMB), and other Federal requirements.	PL-1

[1] *FISMA: Federal Information Security Modernization Act of 2014, Public Law 113-283*

Policy ID	DHS Policy Statements	Relevant Controls
3.1.f	Information security reports regarding DHS systems shall be submitted to the Senior Component official or designated representative.	---
3.1.g	Component CISOs/ISSMs shall ensure that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference Model (TRM) and Security Architecture (SA) or, for deviations, maintain a waiver approved by the DHS CIO or CISO.	PL-1, PM-1 SA-1
3.1.h	The DHS CISO shall issue department-wide information security policy, guidance, and information security architecture requirements for all DHS systems.	CM-2, CM-6
3.1.i	Component CISOs shall implement DHS information security policies, procedures, and control techniques to meet all applicable requirements.	PL-1, PM-1
3.1.j	Component CISOs shall develop and manage information security guidance and procedures unique to Component requirements.	PL-1, PM-1
3.1.k	Security-relevant management processes and tools shall comply with applicable NIST-standard protocols and conventions as described in NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP)*, including the Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposures (CVE)	RA-5, SI-2, CM-6

3.2 Capital Planning and Investment Control

Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved, to the maximum extent possible, in all aspects of the acquisition process, including drafting contracts, and procurement documents. DHS Management Directive (MD) 102-01 Rev. 2, *Acquisition Management Directive* and DHS MD 4200.1, *IT Capital Planning and Investment Control (CPIC) and Portfolio Management* provide additional information on these requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.2.a	System Owners shall include information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.	PM-3, PM-11, SA-1
3.2.b	System Owners or AOs shall ensure that information security requirements and Plans of Action and Milestones (POA&M) are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.	PM-3, PM-4, SA-2

Policy ID	DHS Policy Statements	Relevant Controls
3.2.c	Component Investment Review Boards (IRB) and Acquisition Review Boards (ARB) shall not approve any capital investment in which the information security requirements, including those that address supply chain threats, are not adequately defined and funded.	PM-3, SA-2
3.2.d	The DHS CISO shall perform security reviews for planned information system acquisitions over $2.5 million, and in selected additional cases.	SA-1
3.2.e	Components shall ensure that information security requirements as described in this Policy Directive are met in the acquisition of all DHS systems and services used to input, process, store, display, or transmit sensitive information.	SA-4
3.2.f	Procurement authorities throughout the Department shall enforce the provisions of the Homeland Security Acquisition Regulation (HSAR).	SA-1, SA-4
3.2.g	Procurements for services and products involving facility or system access control shall be in accordance with DHS guidance regarding Homeland Security Presidential Directive 12 (HSPD-12) implementation.	---

3.3 Contractors and Outsourced Operations

Policy ID	DHS Policy Statements	Relevant Controls
3.3.a	All Statements of Work (SOW) and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.	SA-4
3.3.b	Contractor information system services and operations shall adhere to all applicable DHS information security policies.	SA-9
3.3.c	Requirements shall address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements shall also include requirements for personnel background investigations and clearances, and facility security.	SA-9
3.3.d	SOWs and contracts shall include a provision stating that, when the contract ends, the contractor shall return all information and information resources provided during the life of the contract and certify that all DHS information has been purged from any contractor-owned system(s) that have been used to process DHS information.	SA-4

Policy ID	DHS Policy Statements	Relevant Controls
3.3.e	Components shall conduct reviews to ensure that information security requirements and provisions to address supply chain risk are included in contract language and that the requirements and provisions are met throughout the life of the contract.	SA-1
3.3.f	Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.	SA-9, PM-4
3.3.g	Components shall require contractors to apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27, *Engineering Principles for Information Technology Security*.	SA-8
3.3.h	For systems with high or moderate impact for any of the Federal Information Processing Standard 199 (FIPS 199) security objectives, Components shall require developers of an information system, system Components, or information system services to: a. Perform Configuration Management (CM) during system, system Component, or service development and implementation b. Document, manage, and control the integrity of changes to items under CM c. Implement only organization-approved changes to the system, system Component, or service d. Document approved changes to the system, system Component, or service and the potential security impacts of such changes e. Track security flaws and flaw resolution within the system, system Component, or service and report findings to the DHS SOC.	SA-10
3.3.i	For systems with high or moderate impact for any of the FIPS 199 security objectives, Components shall require developer of information systems, system Components, or information system services to: a. Create and implement a security assessment plan b. Perform: unit; integration; system; regression testing/evaluation commensurate with the volume and complexity of modifications and the impact to the system risk made by those modifications c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation d. Implement a verifiable flaw remediation process e. Correct flaws identified during security testing/evaluation.	SA-11

Policy ID	DHS Policy Statements	Relevant Controls
3.3.j	All SOW, contract vehicles, and other acquisition-related documents shall include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and service providers.	AR-3

3.4 Performance Measures and Metrics

Policy ID	DHS Policy Statements	Relevant Controls
3.4.a	The DHS CISO shall define performance measures to evaluate the effectiveness of the DHS information security program.	---
3.4.b	Components shall provide OMB FISMA data at least monthly to the DHS Compliance Officer.	---
3.4.c	The DHS CISO shall report annually to the Secretary on the effectiveness of the DHS information security program, including the progress of remedial actions.	---
3.4.d	Components shall use the automated tool specified by the DHS CISO for Performance Plan reporting.	---
3.4.e	The DHS CISO shall collect OMB FISMA data from Components at least quarterly and provide FISMA reports to OMB.	AR-6

3.5 Continuity Planning for Critical DHS Assets

The Continuity Planning for Critical DHS Assets Program is vital to the success of the DHS Information Security Program. The Business Impact Assessment (BIA) is essential in the identification of critical DHS assets. Once critical systems are identified, continuity planning shall address the following two different but complementary elements:

- Continuity of Operations Planning (COOP)
- Contingency Planning (CP)

3.5.1 Continuity of Operations Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.a	When available, a DHS-wide process for continuity of operations planning shall be used in order to ensure continuity of operations under all circumstances.	CP-2
3.5.1.b	Components shall develop, test, implement, and maintain comprehensive COOPs to ensure the recovery and continuity of essential DHS functionalities.	CP-2, CP-4
3.5.1.c	All CISOs/ISSMs shall ensure that all COOPs under their purview are tested and exercised annually.	CP-4
3.5.1.d	All Chief Financial Officer (CFO) Designated Systems requiring high availability shall be identified in COOP plans and exercises.	CP-1
3.5.1.e	All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.	AT-3, CP-3
3.5.1.f	To ensure that accounts can be created in the absence of the usual account approval authority, systems that are part of the Critical DHS Assets Program shall have provisions to allow a Component CISO/ISSM or Component CIO to approve new user accounts as part of a COOP scenario.	AC-2
3.5.1.g	Each Component shall compile and maintain a list of mission essential information systems in support of COOP.	CM-8, CP-1
3.5.1.h	The DHS and Component CISOs/ISSMs shall ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.	CP-1
3.5.1.i	DHS information systems that are part of the DHS Continuity Planning for Critical DHS Assets Program shall be provided requirements for system-level contingency planning by a Component Contingency Planning Program Office or by a DHS Contingency Planning Program Office.	---

3.5.2 Contingency Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.a	The DHS CIO shall provide guidance, direction, and authority for a standard DHS-wide process for contingency planning for information systems.	CP-1

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.b	System Owners shall develop and document information system Contingency Plans (CPs) for their information systems, manage plan changes, and distribute copies of the plan to key contingency personnel. Component CIOs shall review and approve Component-level information system CPs.	CP-1, CP-2
3.5.2.c	Components shall ensure implementation of backup policy and procedures for every Component information system.	CP-9
3.5.2.d	The DHS CIO shall ensure that each DHS system has contingency capabilities commensurate with the ***availability*** security objective. The minimum contingency capabilities for each impact level are as follows: **High impact** – System functions and information have a high priority for recovery after a short period of loss. **Moderate impact** – System functions and information have a moderate priority for recovery after a moderate period of loss. **Low impact** – System functions and information have a low priority for recovery after prolonged loss.	CP-1
3.5.2.e	CPs shall be developed and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the **availability** security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	CP-1, CP-2
3.5.2.f	The DHS CIO shall ensure that CP testing is performed in accordance with the **availability** security objective. The minimum contingency testing for each impact level follows: **High impact** – System recovery roles, responsibilities, procedures, and logistics in the CP shall be tested within a year prior to authorization to recover from a simulated contingency event at the alternate processing site. The system recovery procedures in the CP shall be exercised at least annually to simulate system recovery in a test facility. **Moderate impact** – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This may be achieved by performing a walk-through/tabletop exercise. **Low impact** – CP contact information shall be verified at least annually.	CP-4, CP-7

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.g	The DHS CIO shall ensure that contingency training is performed in accordance with the **availability** security objective. The minimum contingency planning for each impact level follows: **High impact** – All personnel involved in contingency planning efforts shall be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, and logistics. This training shall incorporate simulated events. Refresher training shall be provided at least annually. **Moderate impact** – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually. **Low impact** – There is no training requirement.	CP-3
3.5.2.h	Components shall coordinate CP testing and/or exercises as appropriate, using COOP-related plans for systems with moderate and high availability FIPS 199 categorization.	CP-4

3.6 Systems Engineering Life Cycle

The DHS Systems Engineering Life Cycle (SELC) is detailed in MD 102-01, "Acquisition Management Directive," Rev.2, Appendix B.

Policy ID	DHS Policy Statements	Relevant Controls
3.6.a	Components shall ensure that system security is integrated into all phases of SELC.	SA-3
3.6.b	Components shall ensure that security requirements for sensitive information systems are incorporated into life-cycle documentation.	SA-3
3.6.c	The Program Manager shall review, approve, and sign all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority in writing to another DHS employee. The authority shall not be delegated to contractor personnel.	RA-5

3.7 Configuration Management

Configuration Management (CM) includes management of all hardware and software elements of information systems and networks. CM within DHS consists of a multi-layered structure – policy, procedures, processes, and compliance monitoring. Each Component shall use an appropriate level of CM.

CM applies to all systems, subsystems, and components of the DHS infrastructure, and ensures implementation and continuing life-cycle maintenance. CM begins with baselining of requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline applies to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. A CM Process ensures that documentation associated with an approved change to a DHS system is updated to reflect the appropriate baseline, including an analysis of any potential security implications. The initial configuration must be documented in detail and all subsequent changes must be controlled through a complete and robust CM process.

CM has security implications in three areas:

- Ensuring that the configuration of subordinate information system elements is consistent with the Security Authorization Process requirements of the parent system
- Ensuring that any subsequent changes (including an analysis of any potential security implications) are approved
- Ensuring that all recommended and approved security patches are properly installed

The *DHS 4300A Sensitive Systems Handbook* includes the DHS Secure Baseline Configuration Guides.

Policy ID	DHS Policy Statements	Relevant Controls
3.7.a	Components shall develop and maintain a Configuration Management Plan (CMP) for each information system as part of its system Security Plan (SP). All DHS systems shall be under the oversight of the officer responsible for CM.	CM-1, CM-9
3.7.b	Components shall establish, implement, and enforce CM controls on all information systems and networks and address significant deficiencies as part of a POA&M.	CA-5, CM-3, PM-4
3.7.c	Information security patches shall be installed in accordance with CM plans and within the timeframe or direction stated in the Information Security Vulnerability Management (ISVM) message published by the DHS Security Operations Center (SOC).	SI-2
3.7.d	System Owners shall document initial system configuration in detail and shall control all subsequent changes in accordance with the CM process.	CM-2, CM-3, CM-9

Policy ID	DHS Policy Statements	Relevant Controls
3.7.e	Workstations shall be configured in accordance with DHS guidance on the U.S Government Configuration Baseline (USGCB) (formerly known as the Federal Desktop Core Configuration [FDCC]). Configuration shall include installation of the DHS Common Policy Object identifier (OID), Common Policy Framework Root CA certificate, and the DHS Principal CA certificate.	CM-2, CM-6, CM-9
3.7.f	Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a (NIST)-validated SCAP tool.	---
3.7.g	The System Owner shall request a waiver for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in the DHS Secure Baseline Configuration Guides included in the *DHS 4300A Sensitive Systems Handbook*. Requests shall include a proposed alternative secure configuration.	CM-2, CM-6
3.7.h	Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.	CM-4
3.7.i	Users shall report known or suspected implementations of unauthorized IT changes to DHS Enterprise Configuration Management (ICCB.Services@hq.dhs.gov). For more information regarding how unauthorized changes are addressed, refer to the DHS ICCB Unauthorized Change Tracking Process.	---

3.8 Risk Management

Risk management is a process that allows System Owners to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the information systems and data that support their organization’s missions.

Policy ID	DHS Policy Statements	Relevant Controls
3.8.a	Components shall establish a risk management program in accordance with NIST Special Publication (SP) 800-30 Rev 1, “Guide for Conducting Risk Assessments,” and with other applicable Federal guidelines.	RA-1

Policy ID	DHS Policy Statements	Relevant Controls
3.8.b	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever major modifications that have the potential to significantly impact risk are made to sensitive information systems, or to their physical environments, interfaces, or user community. The risk assessment shall consider the effects of the modifications on the operational risk profile of the information system. SPs shall be updated and re-certifications conducted if warranted by the results of the risk assessment.	RA-3
3.8.c	Each Component CISO/ISSM shall establish an independent Component-wide Security Authorization program to ensure a consistent approach to testing the effectiveness of controls.	RA-1
3.8.d	Risk Executives shall review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and appropriate CIO.	RA-3
3.8.e	Component SOCs shall deploy a Component-wide network scanning program.	RA-5
3.8.f	Special rules apply to CFO-designated systems. See Section 3.15 for additional information.	---

3.9 Security Authorization and Security Control Assessments

DHS periodically assesses the selection of security controls to determine their continued effectiveness in providing an appropriate level of protection.

It is recommended that Components pursue Type Security Authorization for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments.

Type Security Authorization shall consist of a master security authorization package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.

The DHS *Security Authorization Process Guide* describes detailed processes governing security authorizations.

Detailed information for creating and managing POA&Ms is published in *DHS 4300A Sensitive Systems Handbook*, Attachment H, “Plan of Action and Milestones (POA&M) Process Guide.”

Policy ID	DHS Policy Statements	Relevant Controls
3.9.a	Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-53 and NIST SP 800-161 controls as tailored specifically to the security objective and impact level determined as described in Attachment M to *DHS 4300A, Sensitive Systems Handbook*, "Tailoring the NIST SP 800-53 Security Controls."	PM-10, RA-2
3.9.b	Components shall implement NIST SP 800-53 and NIST SP 800-161 security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	---
3.9.c	It is recommended that Components pursue Type Security Authorization for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. Type Security Authorization shall consist of a master Security Authorization package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	---
3.9.d	The AO for a system shall be identified in the Information Assurance Compliance System (IACS). The Component CIO shall serve as the AO whenever the System Owner or an appropriate program official has not been named as the AO.	---
3.9.e	Component CISOs shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.	CA-2, PM-10
3.9.f	As part of the authorization process, a supporting assessment shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.	PM-10
3.9.g	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever modifications are made to sensitive information systems, networks, or their physical environments, interfaces, or user community. SPs shall be updated and systems re-authorized if warranted.	PM-9, RA-3
3.9.h	Components shall authorize systems at Initial Operating Capability (IOC) and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first. An Authority to Operate (ATO) of six (6) months or less shall receive an ATO authorization period waiver from the DHS CISO before submission to the AO for a final authorization decision.	CA-6, PM-10

Policy ID	DHS Policy Statements	Relevant Controls
3.9.i	AOs may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system shall be assessed and authorized in an ATO letter prior to passing the Acquisition Decision Event 2C milestone in the SELC. IATOs shall not be used for operational systems. The AO may grant an IATO for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension. Systems under an IATO shall not process sensitive information but may attach to system networks for testing.	PL-1, PM-10
3.9.j	If the system is not fully authorized and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.	PL-1, PM-10
3.9.k	Components shall request concurrence from the DHS CISO for all authorizations for 6 (six) months or less.	---
3.9.l	The DHS CISO shall specify tools, techniques, and methodologies used to assess and authorize DHS information systems, report and manage FISMA data, and document and maintain POA&Ms.	CA-1, PM-4
3.9.m	Currently, all DHS systems shall be authorized using the automated IACS tools that have been approved by the DHS CISO.	CA-1, CA-2, PM-10
3.9.n	The DHS CISO shall maintain a repository for all Security Authorization Process documentation and modifications.	CA-1
3.9.o	Component CISOs shall establish processes to ensure that the Security Authorization Process is used consistently for all Component systems.	CA-1, PM-10
3.9.p	System Owners shall use the POA&M process to document the control deficiencies or vulnerabilities, and shall use the plans to correct the deficiencies and vulnerabilities.	CA-5, PM-4
3.9.q	The AO shall formally assume responsibility for operating an information system at an acceptable level of risk. Operating any system with sensitive information is prohibited without an ATO.	CA-6, PM-10
3.9.r	ATOs shall only be provided for systems that fully comply with policy or have been granted appropriate waivers.	CA-6, PM-10
3.9.s	Artifacts in support of *new* ATOs shall not be older than 13 months. Older artifacts remain valid during the life of a current ATO.	---
3.9.t	The DHS CIO may revoke the ATO of any DHS information system.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
3.9.u	The Component CIO may revoke the ATO of any Component-level information system.	CA-6
3.9.v	Components shall assign a common control provider to share controls between systems (e.g., at hosting centers). The authorization package of those common controls must be shared with those operating under the controls.	---
3.9.w	DHS enterprise services shall be required to provide a catalog of common controls that have been assessed and authorized by the AO of that service.	---
3.9.x	An Enterprise System Security Agreement (ESSA) shall be developed for all enterprise services.	---

3.9.1 Ongoing Authorization

The DHS Ongoing Authorization (OA) Program builds upon an information system’s existing Security Authorization. The purpose of the OA Program is continuous evaluation of security controls, based on system-specific information, and timely action in response to changes to information systems and risk posture.

OA enhances the information assurance life cycle process by replacing the periodic three-year assessment cycle with ongoing security assessments that are driven by risk as opposed to time.

The *DHS Ongoing Authorization Methodology* describes detailed processes governing the OA Program’s requirements and entrance criteria for a Component and for a Component’s systems. The OA Methodology defines the deliverables and templates required for maintaining compliance with OA as well as required and recommended internal procedures.

Policy ID	DHS Policy Statements	Relevant Controls
3.9.1.a	Components shall be accepted into the DHS OA Program only with concurrence of the DHS CISO and the Component’s AO and/or CIO. All submissions will be considered by DHS CISO using objective eligibility requirements as outlined in the *DHS OA Methodology*.	---
3.9.1.b	Eligible Components may submit requests for systems to join the DHS OA Program. Systems submitted must have a valid ATO at least 60 days from expiration at date of submission (further details are found in the latest version of the *DHS Ongoing Authorization Methodology*).	CA-6, PM-10

Policy ID	DHS Policy Statements	Relevant Controls
3.9.1.c	The DHS CISO shall specify requirements, tools, techniques, and methodologies used to assess and authorize DHS information systems within a Component OA Program.	CA-1, PM-4
3.9.1.d	All DHS systems within the OA Program shall be monitored using the automated Information Assurance Compliance System tools currently in use and approved by the DHS CISO.	CA-1, CA-2, PM-10
3.9.1.e	The DHS OCISO shall maintain a repository for all OA Process documentation and modifications and will communicate changes through the Component CISOs.	CA-1
3.9.1.f	Components shall adhere to established processes and requirements outlined in the *DHS Ongoing Authorization Methodology* to ensure that the OA process is consistent across all DHS Component systems.	CA-1, PM-10
3.9.1.g	The DHS CISO shall review monthly OA deliverables for Component IT systems security compliance for quality and for deficiencies periodically in order to allow continued participation in the DHS OA Program. The DHS CISO may require information systems to revert to previous steps of the NIST Risk Management Framework (RMF), RMF Steps 1-6, in response to OA and/or general information security deficiencies found during periodic quality assurance reviews. Components found unable to sustain OA requirements, or maintain sound security practices (as specified in the Component OA eligibility details of the *DHS OA Methodology*), shall be required to have all or some of their information systems revert to previous steps of the NIST RMF in order to mitigate or compensate for deficiencies found during periodic quality assurance reviews.	CA-6
3.9.1.h	The Component Authorizing Official shall require any of their information systems participating in the DHS OA Program to revert to previous steps of the NIST RMF in order to mitigate or compensate for deficiencies found during periodic quality assurance reviews, in response to system Triggers, changes in supply chain risk, or due to other circumstances which supplies the Component CIO with knowledge of risk to the system or the Component.	CA-6

Policy ID	DHS Policy Statements	Relevant Controls
3.9.1.i	Component CISOs shall designate qualified personnel to fulfill the function of the Operational Risk Management Board (ORMB). The ORMB shall be considered a board of experts representing technical and operational expertise as it relates to Information Security and the Component's information systems, data, and networks. Ideal ORMB roles are detailed in the *DHS OA Methodology*.	---

3.10 Information Security Review and Assistance

Policy ID	DHS Policy Statements	Relevant Controls
3.10.a	Components shall submit their information security policies to the DHS CISO for review.	PL-1
3.10.b	Each Component shall establish an information system security review and assistance program within its respective security organization in order to provide System Owners with expert review of programs; to assist in identifying deficiencies; and to provide recommendations for bringing systems into compliance.	CA-7, PL-1, PM-10
3.10.c	Components shall conduct their information systems security reviews in accordance with both FIPS 200 and NIST SP 800-53, for specification of security controls. NIST SP 800-53A shall be used for assessing the effectiveness of security controls and for quarterly and annual FISMA reporting.	CA-7, PL-1
3.10.d	The DHS CISO shall conduct information security reviews and assistance visits across the Department in order to monitor the effectiveness of Component security programs.	CA-2

3.11 Security Working Groups and Forums

Working groups and other forums representing various functional security areas convene on a regular basis.

3.11.1 CISO Council

The CISO Council and ISSMs constitute the management team responsible for ensuring the development and implementation of the DHS Information Security Program. The Council is responsible for implementing a security program that meets DHS mission requirements, and also for reviewing specific topic areas assigned by the DHS CIO or the DHS CISO.

The CISO Council is also responsible for establishing and implementing significant security responsibilities; promoting communications between security programs; implementing information systems security acquisition requirements; and for developing security best practices in all enterprise and Component information security programs.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.1.a	Component CISOs shall actively participate in the CISO Council.	PL-1, PM-11
3.11.1.b	Members of the CISO Council shall ensure that the DHS CISO is kept apprised of all matters pertinent to the security of information systems.	PL-1, PM-11
3.11.1.c	Members of the CISO Council shall ensure that security-related decisions and information, including updates to the 4300 series of security publications, are distributed to the ISSOs and other appropriate persons.	PL-1, PM-11

Note: Periodically, the CISO Council shall be convened to include Component ISSMs.

3.11.2 DHS Information Security Training Working Group

The DHS Information Security Training Working Group is established to promote collaboration on information security training efforts throughout the Department and to share information on Component-developed training activities, methods, and tools, thereby reducing costs and avoiding duplication of effort. The Information Security Training Working Group is chaired by the DHS Program Director for Information Security Training.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.2.a	Each Component shall appoint a representative to the DHS Information Security Training Working Group.	---
3.11.2.b	Component representatives shall actively participate in the DHS Information Security Training Working Group.	---
3.11.2.c	Components shall abide by the security training requirements listed in the Information Security Awareness, Training, and Education section of this policy.	---

3.11.3 DHS Security Policy Working Group

The OCISO Director responsible for Policy shall chair or appoint the chair for the Security Policy Working Group. The DHS Security Policy Working Group is established to promote collaboration between the Components and Headquarters in the maintenance of DHS information security policy.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.3.a	Each Component CISO shall appoint a representative to the DHS Security Policy Working Group.	---
3.11.3.b	The DHS Security Policy Working Group chair shall ensure that a report on representative attendance is made available to Component and Department CISOs.	---

3.11.4 DHS Enterprise Services Security Working Group

The DHS Enterprise Services Security Working Group (ESSWG) ensures the development, review and vetting of proposed security documents for current and proposed enterprise service solutions and service offerings. It also provides recommendations to the CISO Council for review and approval. The ESSWG is chaired by the DHS CISO, the DHS Headquarters CISO, and Executive Director of Enterprise Systems Development Office or their delegates.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.4.a	Each Component CISO shall appoint a representative to the DHS ESSWG.	---
3.11.4.b	Component representatives shall actively participate in the DHS ESSWG.	---

3.12 Information Security Policy Violation and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. Component Heads are responsible for taking corrective actions whenever security incidents or violations occur and for holding personnel accountable for intentional violations. Each Component must determine how to best address each individual case.

Policy ID	DHS Policy Statements	Relevant Controls
3.12.a	Violations related to information security are addressed in *Standards of Ethical Conduct for Employees of the Executive Branch*; DHS employees may be subject to disciplinary action for failure to comply with DHS security policy whether or not the failure results in criminal prosecution.	PS-8
3.12.b	Non-DHS Federal employees, contractors, or others working on behalf of DHS who fail to comply with Department security policies are subject to termination of their access to DHS systems and facilities whether or not the failure results in criminal prosecution.	PS-8
3.12.c	Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.	PS-8

3.13 Required Reporting

FISMA requires that the status of the DHS Information Security Program be reported to OMB on a recurring basis.

Policy ID	DHS Policy Statements	Relevant Controls
3.13.a	Components shall collect and submit quarterly and annual information security program status data as required by FISMA.	CA-2 AR-6
3.13.b	Components shall use the automated tool approved by the DHS CISO for the systems authorization process and report generation.	CA-2 AR-6

3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Departmental information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to Personally Identifiable Information (PII) and to privacy-sensitive programs, systems, or initiatives. Questions from Components concerning privacy-related policy should be directed to the Component Privacy Office or Privacy Point of Contact (PPOC). If the Component does not have a Privacy Office or PPOC, then please contact the DHS Privacy Office (privacy@dhs.gov; 202-343-1717) or refer to the DHS Privacy Office Web page at www.dhs.gov/privacy for additional information.

The privacy controls in NIST SP 800-53 Rev 4, Appendix J are primarily for use by an organization's Senior Agency Official for Privacy (SAOP) and Chief Privacy Officer when working with program managers, mission and business owners, information owners and stewards, Chief Information Officers, Chief Information Security Officers, information system developers and integrators, and risk executives to incorporate effective privacy protections and practices (i.e., privacy controls) within organizational programs and information systems and the environments in which they operate. The privacy controls facilitate DHS efforts to comply with privacy requirements affecting those department-wide and Component programs and systems that collect, use, maintain, share, or dispose of PII or other activities that raise privacy risks. Unlike the security controls in NIST SP 800-53 Rev 4, Appendix F, which are allocated to the low, moderate, and high baselines given in Appendix D, the privacy controls in Appendix J are selected and implemented based on DHS privacy requirements and the need to protect the PII collected and maintained by DHS information systems and programs, in accordance with Federal privacy legislation, policies, directives, regulations, guidelines, and best practices.

3.14.1 Personally Identifiable Information

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether or not the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or Department employee or contractor.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, Alien Registration Numbers (A-number), medical information, and criminal history. The sensitivity of this data requires that stricter handling guidelines be applied. For more information on handling Sensitive PII see: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security.*

Consistent with the DHS *Fair Information Practice Principles (FIPPS)*, PII collected and maintained by DHS should be accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices. In addition, DHS adheres to data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. Programs will retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a record retention schedule approved by National Archives and Records Administration (NARA).

Policy ID	DHS Policy Statements	Relevant Controls
3.14.1.a	When collecting PII, programs shall: a. Confirm to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collect PII directly from the individual to the greatest extent practicable; and c. Check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems through the Privacy Threshold Analysis (PTA) process.	DI-1
3.14.1.b	DHS shall issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	DI-1
3.14.1.c	Prior to the collection of PII, all programs shall: a. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; and b. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.	DM-1
3.14.1.d	DHS shall conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings through the privacy compliance process. The objective of this evaluation is to ensure that only PII that is identified in privacy compliance documentation and other public notices is collected and retained, and that the PII continues to be necessary for accomplishment of a legally authorized purpose.	DM-1
3.14.1.e	Programs and systems that maintain PII shall: a. Retain each collection of PII for the minimum amount of time necessary to fulfill the purpose(s) identified in the notice or as required by law; b. Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Ensure secure deletion or destruction of PII (including originals, copies, and archived records).	DM-2
3.14.1.f	DHS shall develop policies and procedures that protect and minimize the use of any PII used for testing, training, and research,	DM-3

Additional PII and Sensitive PII-related guidance is included in the following sections of the *DHS 4300A Sensitive Systems Handbook.*

- Section 3.9, Security Authorization Process, and Security Control Assessments – For Privacy Sensitive Systems, the confidentiality security objective shall be assigned an impact level of at least moderate.
- Section 4.8.2, Laptop Computers and Other Mobile Computing Devices – All information stored on any laptop computer or other mobile computing device is to be encrypted using mechanisms that comply with Section 5.5, Encryption, of this policy.
- Section 5.2.2, Automatic Session Termination – Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after twenty (20) minutes of inactivity.
- Section 5.3, Auditing – DHS defines computer-readable data extracts as “any Federal record or collection of records containing sensitive PII that is retrieved from a DHS-owned database, through a query, reporting tool, extract generation tool, or other means that is then saved into removable media and/or a separate computer-readable device or application such as another database, a spreadsheet, or a text file." (Attachment S1, *DHS 4300A Sensitive Systems Handbook*).
- Section 5.4.1, Remote Access and Dial-in – Remote access of PII must be approved by the AO. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Restrictions are placed on the downloading and remote storage of PII accessed remotely, as noted below in this document.
- Attachment S, “Compliance Framework for Privacy Systems.”

The DHS Privacy Office works with Component Privacy Officers, PPOCs, Program Managers, System Owners, and information systems security personnel to ensure that sound privacy practices and controls are integrated into the Department’s operations. The DHS Privacy Office implements three types of documents for managing privacy practices and controls for information systems:

- A Privacy Threshold Analysis (PTA) provides a high level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether or not a PIA and/or SORN are required.
- A Privacy Impact Assessment (PIA) is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared.
- A System of Records Notice (SORN) describes the categories of records within a system of records and describes the routine uses of the data and how individuals can gain access to records and correct errors.

To promote privacy compliance within the Department, the Office has published official Department guidance regarding the requirements and content for PTAs, PIAs, and SORNs.

Privacy Compliance Guidance can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

3.14.2 Privacy Threshold Analyses

The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new information system is being developed or an existing system is significantly modified. System Owners and Program Managers are responsible for writing the PTA as part of the SELC process. The Component Privacy Officer or PPOC reviews the PTA and forwards it to the DHS Privacy Office, who determines whether a PIA and/or SORN are required. PTA artifacts expire after three (3) years. DHS Instruction 047-01-001 defines the PTA requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.2.a	A PTA shall be conducted as part of new information system development or whenever an existing system is significantly modified. PTA artifacts expire after three years and a new PTA must be submitted.	AR-2
3.14.2.b	A PTA shall be conducted whenever an information system undergoes security authorization.	---
3.14.2.c	The DHS Chief Privacy Officer shall evaluate the PTA and determine if it is a Privacy Sensitive System and if the system requires a PIA and SORN.	AR-2
3.14.2.d	Information systems shall not be designated operational until the DHS Privacy Office approves the PTA.	AR-2
3.14.2.e	For Privacy Sensitive Systems, the **confidentiality** security objective shall be assigned an impact level of moderate or higher.	RA-2
3.14.2.f	The PTA process shall be used to maintain a current inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.	SE-1
3.14.2.g	The PTA process shall be used to ensure that DHS designs information systems to support privacy by automating privacy controls, to the greatest extent feasible.	AR-7

3.14.3 Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared. PIAs are required (as determined by the PTA) whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the Program Manager as part of the SELC process. OMB Memorandum M-03-22, DHS MD 0470.1, and the *Official DHS Privacy Impact Assessment Guidance* discuss the requirements for conducting PIAs at DHS.

Policy ID	**DHS Policy Statements**	**Relevant Controls**
3.14.3.a	PIAs are required (as determined by the PTA) as part of new information system development or whenever an existing system is significantly modified.	AR-2
3.14.3.b	Information systems for which the DHS Privacy Office requires a PIA (as determined by the PTA) shall not be designated operational until the DHS Privacy Office approves the PIA for that system.	AR-2
3.14.3.c	Programs shall use the PIA process to document the means (where feasible and appropriate) for individuals to: 1. Authorize the collection, use, maintaining, and sharing of PII prior to its collection; 2. Understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; 3. Provide consent prior to any new uses or disclosure of previously collected PII; and 4. Consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.	IP-1
3.14.3.d	Programs shall provide effective notice to the public and to individuals regarding: 1. Activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; 2. Authority for collecting PII; 3. The choices, if any, individuals may have regarding how the program uses PII and the consequences of exercising or not exercising those choices; and 4. The ability to access and have PII amended or corrected if necessary.	TR-1

3.14.3.e	Through effective public notice, programs shall describe: 1. The PII the program collects and the purpose(s) for which it collects that information; 2. How the program uses PII internally; 3. Whether the program shares PII with external entities, the categories of those entities, and the purposes for such sharing; 4. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; 5. How individuals may obtain access to PII; and 6. How the PII will be protected.	TR-1
3.14.3.f	Programs shall revise all public notices to reflect changes in practice or policy that affect PII or changes in their activities that impact privacy, before or as soon as practicable after any change.	TR-1

PIAs are one tool that DHS uses to convey public notice of information practices and the privacy impact of Department programs and activities. The Department also uses web privacy policies, System of Records Notices (SORN), and Privacy Act Statements to provide effective public notice of program privacy practices. PIAs also document how DHS makes individuals active participants in the decision-making process regarding the collection and use of their PII.

3.14.4 System of Records Notices

The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is "*a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual*"[2]. The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term "system of records" is not synonymous with "information system" and can include paper as well as electronic records. SORNs can be written to cover the records in a single group of records or a single information system or they can be written to cover multiple groups of records or multiple information systems.

Information systems that are considered a system of record may not be designated operational until a SORN has been published in the *Federal Register* for thirty days. OMB has issued the benchmark references for development of SORNs: *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975; and Appendix I, "Federal Agency Responsibilities for Maintaining

[2] *5 U.S.C. §552a(a)(5) Italics added.*

Records About Individuals" to Circular A-130. DHS has published MD 047-01-001, "Privacy Policy and Compliance," October 6, 2005; and *Official DHS Guidance on System of Records and System of Records Notices.* Information systems that are considered a System of Records must keep an accurate accounting of disclosures of information shared outside of the system.

OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. This process is called the Biennial SORN Review Process. The DHS Privacy Office works with Components to ensure that SORN reviews are conducted every two years following publication in the Federal Register.

Policy ID	**DHS Policy Statements**	**Relevant Controls**
3.14.4.a	A SORN is required when PII is maintained by a Federal agency in a system of records where information about an individual is retrieved by a unique personal identifier. SORNs are published in the Federal Register.	TR-2
3.14.4.b	Information systems containing PII shall not be designated operational until a SORN has been published in the Federal Register for 30 days.	CA-6
3.14.4.c	Components shall review and republish SORNs every two years as required by OMB Circular A-130.	TR-2
3.14.4.d	Components shall in their privacy notices, including SORNS, describe the purpose(s) for which PII is collected, used, maintained, and shared.	AP-2
3.14.4.e	Components shall include Privacy Act Statements on all forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.	TR-2
3.14.4.f	Programs shall provide individuals the ability to have access to their PII maintained in its system(s) of records.	IP-2
3.14.4.g	DHS publishes rules and regulations governing how individuals may request access to records maintained in a System of Records.	IP-2
3.14.4.h	Programs shall publish access procedures in SORNs.	IP-2
3.14.4.i	DHS shall adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	IP-2
3.14.4.j	DHS shall provide a process for individuals to have inaccurate PII maintained by the Department corrected or amended, as appropriate.	IP-3
3.14.4.k	Components shall establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII (such as external information-sharing partners) and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.	IP-3

Policy ID	DHS Policy Statements	Relevant Controls
3.14.4.j	Components shall: 1. Keep an accurate accounting of disclosures of information held in each system of records under its control, including; a. Date, nature, and purpose of each disclosure of a record; and b. Name and address of person or agency to which the disclosure was made; 2. Retain the accounting of disclosures for the life of the record or five years after the disclosure, whichever is longer; and 3. Make the accounting of disclosures available to the person named in the record upon request.	AR-8

3.14.5 Protecting Privacy Sensitive Systems

OMB M-06-16, *Protection of Sensitive Agency Information* requires that agencies protect PII that is physically removed from Department locations or is accessed remotely. Physical removal includes both removable media and media in mobile devices (e.g., laptop hard drives). Refer to the following documents for additional information and policies on protecting PII and Sensitive PII at DHS:

- *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*
- *DHS 4300A Sensitive System Handbook*, Attachment S: "Compliance Framework for Privacy Sensitive Systems"
- *DHS 4300A Sensitive Systems Handbook*, Attachment S1: "Managing Computer-Readable Extracts Containing Sensitive PII."

In addition, see Section 5.3 of this Policy Directive for PII auditing requirements and Section 5.4.1 for remote access requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.5.a	PII and Sensitive PII removed from a DHS facility on removable media, equipment or mobile devices shall be encrypted unless the information is being sent to an individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.	MP-5 SC-13
3.14.5.b	If PII and Sensitive PII can be physically removed from an information system (e.g., printouts, CDs), the Security Plan (SP) shall document the specific procedures, training, and accountability measures in place to ensure that remote use of the data does not bypass the protections provided by the encryption.	MP-5

Policy ID	DHS Policy Statements	Relevant Controls
3.14.5.c	Systems that as part of routine business remove Sensitive PII in the form of a Computer-Readable Extract (CRE), for example routine system-to-system transmissions of data (routine CREs) shall address associated risks in the system SP.	MP-5
3.14.5.d	Sensitive PII contained within a non-routine or ad hoc CRE (e.g., CREs not included within the boundaries of a source system's SP) shall not be removed, physically or otherwise, from a DHS facility without written authorization from the Data Owner responsible for ensuring that disclosure of the CRE data is lawful and in compliance with this Policy Directive and with applicable DHS privacy and security policies.	---
3.14.5.e	All ad hoc CREs must be documented, tracked, and validated every 90 days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased.	---
3.14.5.f	Ad hoc CREs shall be destroyed or erased within 90 days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or Privacy Point of Contact (PPOC).	---

3.14.6 Privacy Incident Reporting

The DHS Privacy Office is responsible for implementing the Department's privacy incident response program based on requirements outlined in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. Through close collaboration, the DHS Chief Privacy Officer, the DHS CIO, the DHS CISO, the DHS SOC, and Components must ensure that all DHS privacy and computer security incidents are identified, reported, and appropriately responded to, in order to mitigate harm to DHS-maintained assets, information, and personnel. Incidents involving (or that may involve) PII are subject to strict reporting standards and timelines.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.6.a	Any Component discovering a suspected or confirmed privacy incident shall immediately coordinate with the Component Privacy Officer or PPOC and Component CISO/ISSM to evaluate and subsequently report the incident to the DHS SOC upon discovery. The DHS SOC will then transmit the report to the United States Computer Emergency Readiness Team (US-CERT) within one (1) hour.	IR-4

Policy ID	DHS Policy Statements	Relevant Controls
3.14.6.b	The Component Privacy Officer or PPOC, in cooperation with the Component CISO/ISSM, shall jointly evaluate the incident, but the Component CISO/ISSM is responsible for reporting the incident to the Component SOC, or directly to the DHS SOC if the Component does not have its own SOC.	IR-4
3.14.6.c	For Components without Privacy Officers or PPOCs, the Component CISO/ISSM shall report *all* types of privacy incidents, whether or not they involve information resources. This unitary reporting process shall remain in effect until each Component has a Privacy Officer or PPOC who can fulfill the reporting duties.	IR-6
3.14.6.d	DHS personnel shall also report suspected or confirmed privacy incidents to their Program Manager immediately upon discovery/detection, regardless of the manner in which it might have occurred.	IR-6
3.14.6.e	Components shall follow the DHS Privacy Incident Handling Guidance.	---

3.14.7 E-Authentication

Identity verification or authentication (e-authentication) is needed to ensure that online Government services are secure and that individual privacy is protected. Each DHS system must be evaluated to determine whether e-authentication requirements apply. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access Management's (ICAM) Trust Framework Provider Adoption Process (TFPAP) should be used. Components should see www.IDmanagement.gov for details regarding the Federal Identity, Credentialing, and Access Management (FICAM) initiative.

E-authentication guidance is provided in the following:

- OMB M-04-04, *E-Authentication Guidance for Federal Agencies*
- NIST SP 800-63, *Electronic Authentication Guideline*

Policy ID	DHS Policy Statements	Relevant Controls
3.14.7.a	For systems that allow online transactions, Components shall determine whether e-authentication requirements apply.	IA-2
3.14.7.b	Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.	IA-2
3.14.7.c	Components shall implement the technical requirements described in NIST SP 800-63, *Electronic Authentication Guideline*, at the appropriate assurance level for those systems with e-authentication requirements.	IA-2

Policy ID	DHS Policy Statements	Relevant Controls
3.14.7.d	Components shall ensure that each SP reflects the e-authentication status of the respective system.	IA-2, PL-2
3.14.7.e	Programs considering the use of e-authentication are required to consult their Privacy Officer to determine whether a change is significant enough to warrant a new or updated PTA, thus initiating the review of privacy risks and how they will be mitigated.	AR-2
3.14.7.f	Existing physical and logical access control systems shall be upgraded to use Personal Identification Verification (PIV) credentials, in accordance with NIST and DHS guidelines.	---
3.14.7.g	All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational.	---
3.14.7.h	All new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials.	---
3.14.7.i	For systems with high or moderate impact for any of the FIPS 199 security objectives information systems shall uniquely identify and authenticate network devices before establishing a network connection.	IA-3

3.14.8 Use Limitation and External Information Sharing

Programs may use PII either as specified in public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Any PII shared outside the Department MUST be for a purpose compatible with the purpose for which the PII was collected.

DHS uses PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act or in other public notices. The DHS Chief Privacy Officer and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing privacy compliance documentation such as PIAs and SORNs or other public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act or specified in a notice, the Chief Privacy Officer evaluates whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, program owners review, update, and republish their PIAs, SORNs, website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.

DHS programs that engage in Computer Matching Agreements (CMA) must follow established DHS guidance for ensuring that controls are in place to maintain both the quality and integrity of data shared under CMAs. See DHS MD 262-01 *Computer Matching Agreement and the Data Integrity Board*.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.8.a	Programs use PII *within DHS* only for the authorized purpose(s) identified in the Privacy Act or in public notices such as PIAs and SORNs.	UL-1
3.14.8.b	Programs share PII *outside of DHS* only for the authorized purposes identified in the Privacy Act or described in PUBLIC notice(s) such as PIAs and SORNs or for a purpose that is compatible with those purposes.	UL-2
3.14.8.c	Components, where appropriate, enter into Memorandums of Understanding, Memorandums of Agreement, Letters of Intent, CCMAs, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.	UL-2
3.14.8.d	Component Privacy Officers monitor, audit, and train their staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.	UL-2
3.14.8.e	Component Privacy Officers evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether new or updated public notice is required.	UL-2
3.14.8.f	All Computer Matching Agreements shall be reviewed by the Data Integrity Board, chaired by the DHS Chief Privacy Officer.	DI-2

3.15 DHS CFO Designated Systems

DHS CFO-designated systems are systems that require additional management accountability to ensure effective internal control exists over financial reporting. The DHS CFO publishes the approved list of CFO-designated systems annually. This section provides additional requirements for these systems based on Appendix A to OMB Circular A-123, *Management's Responsibility for Internal Control*. Controls required to be assessed annually for CFO Designated Systems may be found documented in Attachment R, "Compliance Framework for CFO Designated Financial Systems" to the *DHS 4300A Sensitive Systems Handbook*. Attachment R is limited to the controls that must be reviewed annually (and does not contain the requirements of OMB Circular 123).

These requirements are in addition to both the other security requirements established in this Policy Directive and to other system Line of Business requirements developed by the CFO.

Wherever there is a conflict between this section and other sections of this Policy Directive regarding requirements for CFO-designated systems, this section shall take precedence.

These additional requirements provide a strengthened assessment process and form the basis for management's assurance of internal control over financial reporting. The strengthened process requires management to document the design and test the operating effectiveness of controls for CFO-designated systems. The System Owner is responsible for ensuring that all requirements, including security requirements, are implemented on DHS systems. Component CISOs/ISSMs must coordinate with their CFO organization to ensure that these requirements are implemented.

Policy ID	DHS Policy Statements	Relevant Controls
3.15.a	System Owners are responsible for ensuring that security control assessments of key security controls (i.e., Security Control Assessment and Security Assessment Report [SAR]) for CFO-designated systems are completed annually in IACS. This includes updating the security control assessment and SAR annually.	CA-2, CA-7
3.15.b	The DHS CFO shall designate the systems that must comply with additional internal controls and the Office of the CFO shall review and publish the CFO Designated System List annually.	CA-2
3.15.c	Component CISOs/ISSMs shall ensure that vulnerability assessments and verification of critical patch installations are conducted on all CFO-designated systems. **Vulnerability assessment**s shall be performed at least annually.	RA-5
3.15.d	All CFO-designated systems shall be assigned a minimum impact level of “moderate” for confidentiality, integrity, and availability. If warranted by a risk based assessment, the integrity objective shall be elevated to “high.”	RA-2
3.15.e	All Component security authorizations for CFO-designated systems shall be approved and signed by the Component CFO.	CA-6
3.15.f	System Owners shall ensure that Contingency plans are created for *all* CFO Designated Systems requiring moderate availability and that Disaster Recovery Plans are created for *all* CFO-designated systems requiring high availability and that each plan is tested annually, and results with lessons learned annually.	CP-2, CP-4
3.15.g	Component CISOs/ISSMs shall ensure that weekly incident response tracking is performed for all of their respective CFO-designated systems.	IR-5
3.15.h	Component CISOs/ISSMs shall ensure that incidents related to their respective CFO-designated systems are reported to the Component CFO.	IR-4, IR-6
3.15.i	The SP shall be updated for CFO-designated systems at least annually. Key controls prescribed in Attachment R, *Compliance Framework for CFO-designated systems* shall be identified in the SP.	PL-2
3.15.j	Component CISOs/ISSMs must request a waiver from the DHS CISO if a key control weakness is identified for a CFO-designated System and not remediated within 12 months.	CA-5, CA-7

Policy ID	DHS Policy Statements	Relevant Controls
3.15.k	Component CFOs shall ensure that a full time dedicated ISSO is assigned to each CFO-designated System. CFO-designated System ISSOs may be assigned to more than one CFO Designated System.	---
3.15.l	CFO Designated System ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.	CA-1, CA-6
3.15.m	Component CFOs shall work with their Component CISOs/ISSMs to approve any major system changes to CFO-designated systems identified in the DHS inventory.	CA-1, CM-8

3.16 Social Media

Due to the high threat of malware, Social Media host sites have been blocked at the Trusted Internet Connection (TIC). Social Media hosts are public content sharing websites that allow individual users to upload, view, and share content such as video clips, press releases, opinions and other information. The DHS Office of Public Affairs (OPA) will publish Terms of Service (TOS) and guidelines for posting to these sites. In some cases the Department will develop its own TOS, and in other cases it will endorse those of other Federal agencies such as the General Services Administration (GSA) or Office of Personnel Management (OPM).

Policy ID	DHS Policy Statements	Relevant Controls
3.16.a	Only OPA-designated Content Managers (Department level and Component level) may post content on behalf of DHS or representing DHS, and only those individuals designated by OPA for this purpose shall be granted access on a continuing basis.	CM-10
3.16.b	Posted content shall be in alignment with the Department's Terms of Service (TOS) and guidelines for a given social media host (e.g., YouTube, Twitter). This condition is also met if the Department endorses another appropriate Federal agency's guidance or TOS (e.g., GSA, OPM).	---
3.16.c	Under no circumstances shall sensitive information be posted to social media sites.	--
3.16.d	Content shall not be posted to any social media site for which the Department has not approved and published *both* final posting guidelines *and* TOS.	CM-10
3.16.e	Content Managers shall review and understand the appropriate Department-level TOS for the appropriate social media host.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.16.f	Content Managers shall make a risk decision prior to posting any information and shall recognize that social medial hosts are not DHS information systems and therefore subject only to the DHS TOS and not to DHS policy. Once released, information is no longer under DHS control.	---

3.17 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[3] addresses the privacy of individuals' health information by establishing a Federal privacy standard for health information and how it can be used and disclosed.

HIPAA prohibits the use or disclosure without the authorization of the individual or as part of an exception contained in HIPAA of Protected Health Information (PHI), electronic or otherwise, for any purpose other than treatment, payment, or health care operations for that individual.

Because of the diverse mission of DHS, it may be necessary for some Components to collect PHI as part of a larger mission requirement (for example detainee processing, disaster relief, etc.). This section applies to all Components and personnel who collect, process, or store PHI (refer to NIST SP 800-66 Rev 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, for further information).

Policy ID	DHS Policy Statements	Relevant Controls
3.17.a	Components whose systems collect, process, or store Protected Health Information (PHI) shall ensure that the stored information is appropriately protected in compliance with HIPAA and that access or disclosure is limited to the minimum required.	---
3.17.b	Affected Components shall work with the DHS Privacy Office, Component Privacy Office, or PPOC to ensure that privacy and disclosure policies comply with HIPAA and privacy requirements.	---
3.17.c	Affected Components shall ensure that employees with access to DHS systems that collect, process, or store PHI are trained in HIPAA requirements.	---

[3] *Public Law 104-191*

Policy ID	DHS Policy Statements	Relevant Controls
3.17.d	Affected Components shall establish administrative processes for responding to complaints; requesting corrections to health information; and tracking of PHI disclosures.	---
3.17.e	When collecting PHI, Components shall issue a privacy notice to individuals concerning the use and disclosure of their PHI.	---

3.18 Cloud Services

Cloud computing technologies allow DHS to address demands for better information services; conserve resources; consolidate systems; and improve security. The essential characteristics of cloud computing (on-demand provisioning, resource pooling, elasticity, network access, and measured services) provide the potential for DHS to reduce procurement and operating costs and increase service efficiency.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save cost, time, and staff required to conduct redundant agency security assessments. The Federal CIO Memorandum "Security Authorization of Information Systems in Cloud Computing Environments," issued on December 8, 2011, established FedRAMP to provide a cost-effective risk-based approach for the adoption and use of cloud services.

The purposes of FedRAMP are:

- To improve the consistency and quality of information security in the cloud
- To ensure trustworthy and re-usable documentation and assessment of security controls
- To provide ongoing assurance and risk assessment of select cloud services. Cloud services are discussed on the FedRAMP Web site at http://www.gsa.gov/portal/category/102371 .
- To enable rapid and cost-effective procurement of information systems and services for Federal agencies.

DHS is a key participant in FedRAMP. Other major participants are:

- Federal agency customers
- Cloud Service Providers (CSP)
- Joint Authorization Board (JAB)
- Third Party Assessors (3PAO)
- FedRAMP Program Management Office (PMO)
- National Institute of Standards and Technology (NIST)

NIST SP 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." All uses of cloud computing by DHS will follow DHS security authorization processes and procedures to include a completed security authorization package and an ATO signed by the appropriate Authorizing Official. Those cloud systems and services which are not exempt from FedRAMP requirements will use the FedRAMP process as required by OMB. Organizations should also review Section 3.14 for applicability in cloud environments if they are dealing with privacy data.

Policy ID	DHS Policy Statements	Relevant Controls
3.18.a	Components shall leverage cloud services with FedRAMP Provisional Authority to Operate (P-ATO) whenever available when authorizing cloud systems or services. When a P-ATO is not available, Components shall leverage FedRAMP compliant Agency ATO packages whenever available to the fullest extent possible.	---
3.18.b	All DHS cloud services of FIPS Moderate categorization or higher, consumed by or intended to be consumed by multiple government organizations outside of DHS, shall submit to FedRAMP for JAB Provisional Authorization.	---
3.18.c	The use of cloud systems and services shall follow existing DHS security authorization processes and procedures to include a completed security authorization package and an ATO signed by the Component or DHS-designated Authorizing Official.	---
3.18.d	All DHS cloud systems and services not exempt from FedRAMP shall use appropriate FedRAMP documentation templates, be assessed using the JAB-approved security-control baselines and additional DHS requirements, and be categorized in the FISMA inventory as either a General Support System or a Major Application. DHS cloud systems and services shall not be categorized as External Information Systems (EIS).	---
3.18.e	All DHS cloud systems and services not exempt from FedRAMP shall use the FedRAMP process and security authorization requirements when initiating, reviewing, granting and revoking risk assessments and security authorizations.	---

4.0 OPERATIONAL POLICIES

4.1 Personnel

Department of Homeland Security (DHS) systems face threats from a myriad of sources. The intentional and unintentional actions of system users can potentially harm or disrupt DHS systems and facilities and could result in destruction or modification of the data being processed, denial of service, and unauthorized disclosure of data. It is thus highly important that stringent safeguards be in place to reduce the risk associated with these types of threats.

4.1.1 Citizenship, Personnel Screening, and Position Categorization

Policy ID	DHS Policy Statements	Relevant Controls
4.1.1.a	Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.	PS-2, PS-3, PS-7
4.1.1.b	Components shall ensure that the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.	PS-2, PS-3, PS-7
4.1.1.c	Components shall ensure any Federal employee granted access to any DHS system has a favorably adjudicated Tier 2 Investigation (formerly Moderate Risk Background Investigation [MBI]) as defined in DHS Instruction 121-01-007, *Personnel Suitability and Security Program*, Chapter 2, Federal Employee/Applicant Suitability Requirements. In cases where non-DHS Federal employees have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 2, paragraph G). Active duty United States Coast Guard (USCG) and other personnel subject to the Uniform Code of Military Justice (UCMJ) shall be exempt from this requirement.	PS-3
4.1.1.d	Components shall ensure that no contractor personnel are granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in Department of Homeland Security Acquisition Regulation (HSAR) and the DHS Instruction 121-01-007, *Personnel Suitability and Security Program*, Chapter 3, Excepted Service Federal Employee and Contractor Employee Fitness Requirements. In cases where contractor personnel have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 3, paragraph G).	PS-3
4.1.1.e	Components shall ensure that only U.S. Citizens are granted access to DHS systems and networks. Exceptions to the U.S. Citizenship requirement may be requested by submitting a completed Foreign National Visitor Access Request form for each foreign national to the DHS Office of the Chief Security Officer (OCSO), in accordance with Section 1.5.2, of this policy, "Requests for Exception to U.S. Citizenship Requirement."	PS-3
4.1.1.f	Components shall ensure that no temporary employee is granted access to any DHS system without having met the review and investigation standard defined in DHS Instruction 121-01-007, "Personnel Suitability and Security Program," Chapter 2: "Federal Employee/Applicant Suitability Requirements."	--

4.1.2 Rules of Behavior

Policy ID	DHS Policy Statements	Relevant Controls
4.1.2.a	Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a "Consent to Monitor" provision) and that disciplinary actions may result from violations.	PL-4
4.1.2.b	Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.	AT-1, AT-2, PL-4

4.1.3 Access to Sensitive Information

Policy ID	DHS Policy Statements	Relevant Controls
4.1.3.a	System Owners shall ensure that users of the information systems supporting their programs have a valid requirement to access these systems.	AC-2

4.1.4 Segregation of Duties and Least Privilege

Segregation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process.

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.a	Components shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility of any one individual having the necessary authority or system access to be able to engage in fraudulent or criminal activity.	AC-2, AC-5
4.1.4.b	All individuals requiring administrator privileges shall be reviewed and approved by the appropriate Authorizing Official (AO). The AO may delegate this duty to the appropriate System Owner or Program Manager.	AC-2
4.1.4.c	Individuals requiring administrator privileges shall be assigned administrator accounts separate from their normal user accounts.	AC-6

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.d	Administrator accounts shall be used only for performing required administrator duties. Individuals shall use their regular user accounts to perform all other functions not directly tied to administrator duties (checking email, accessing the Internet).	AC-6

4.1.5 Information Security and Privacy Awareness, Training, and Education

Policy ID	DHS Policy Statements	Relevant Controls
4.1.5.a	Components shall establish an information security training program for users of DHS information systems.	AT-1
4.1.5.b	DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) accessing DHS systems shall receive initial training and annual refresher training in security awareness and accepted security practices. Personnel shall complete security awareness training within 24 hours of being granted a user account. If a user fails to meet this training requirement, user access shall be suspended.	AT-1, AT-4
4.1.5.c	DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) with significant security responsibilities (e.g., Information Systems Security Officers (ISSO), system administrators) shall receive initial specialized training and thereafter annual refresher training specific to their security responsibilities.	AT-3
4.1.5.d	Components shall maintain awareness training records to include: Component name, name of trainee, training course title, type of training received, and completion date of training.	AT-4
4.1.5.e	Components shall maintain role-based training records to include Component name, name of trainee, security role of trainee, training course title, type of training received, completion date of training, and cost of training.	AT-4
4.1.5.f	User accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training, unless a waiver is granted by the Component’s Chief Information Security Officer (CISO) or Information Systems Security Manager (ISSM).	AT-1
4.1.5.g	Components shall prepare and submit an annual security awareness and role-based training plan, as specified by the DHS Information Security Training Program Office.	AT-1

Policy ID	DHS Policy Statements	Relevant Controls
4.1.5.h	Components shall prepare and submit information security awareness reports with content, frequency, format, and distribution at the request of the DHS CISO.	AT-1
4.1.5.i	Components shall at the request of the DHS Information Security Training Program Office provide evidence of training by submitting copies of training schedules, training rosters, and training reports.	AT-4
4.1.5.j	The DHS CISO shall review Component information security awareness and role-based training programs annually.	AT-1
4.1.5.k	Components shall submit a roster during the first month and during the seventh month of each fiscal year identifying all significant information security personnel, including full name, security role, employment status (federal employee, military, contractor), and work location (state). At a minimum, the roster will include all standard information security roles: Chief Information Officer, Chief Information Security Officer, Authorizing Official, Program Manager, System Owner, Information System Security Officer, Security Operations Center Manager, System Administrator (Windows-based), and Contracting Officer/Contracting Officer Representative.	AT-3
4.1.5.l	The annual security awareness training shall include incident response training to information system users consistent with assigned roles and responsibilities. (Initial training shall be completed within twenty-four (24) hours of assuming an incident response role or responsibility. Out of cycle refresher training shall be conducted as required due to information system changes)	IR-2
4.1.5.m	Components shall develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.	AR-5
4.1.5.n	Components shall administer basic privacy training annually and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII annually.	AR-5
4.1.5.o	Components shall ensure that personnel annually certify (manually or electronically) acceptance of responsibilities for privacy requirements.	AR-5

4.1.6 Separation from Duty

Policy ID	DHS Policy Statements	Relevant Controls
4.1.6.a	Components shall implement procedures to ensure that system access is revoked for DHS employees, contractors, or others working on behalf of DHS who leave the Component, are reassigned to other duties, or no longer require access.	AC-2, PS-5
4.1.6.b	Components shall establish procedures to ensure that all DHS property and assets related to information systems are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual.	PS-4
4.1.6.c	Accounts for personnel on extended absences shall be temporarily suspended.	AC-2
4.1.6.d	System Owners shall review information system accounts supporting their programs at least annually.	AC-2
4.1.6.e	Components shall develop and document access agreements for information systems and ensure that individuals requiring access to information and information systems sign appropriate access agreements prior to being granted access, and re-sign whenever access agreements have been updated. Access agreements shall be reviewed at least annually,	PS-6

4.2 Physical Security

4.2.1 General Physical Access

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.a	Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.	PE-2
4.2.1.b	Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	PE-3
4.2.1.c	Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.d	Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.	PE-2, PE-3, PE-6, PE-8
4.2.1.e	These requirements shall extend to DHS assets located at non-DHS facilities or non-DHS assets and equipment that host DHS data.	---
4.2.1.f	Components shall control physical access to transmission medium that transmits unencrypted data within Component facilities using DHS SOC-approved safeguards.	PE-4
4.2.1.g	Components shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	PE-5
4.2.1.h	Components shall: a. Protect power equipment and power cabling for the information systems from damage and destruction b. Provide capability to shut off power to the information system or individual system Components in emergency situations c. Place emergency shutoff switches or devices to facilitate safe and easy access for personnel d. Protect emergency power shutoff capability from unauthorized activation e. Provide a short-term uninterruptible power supply to facilitate either an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss.	PE-9, PE-10, PE-11

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.i	Components shall: a. Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility b. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source c. Maintain and monitor temperature and humidity levels within the facility where information systems reside d. Protect information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	PE-12, PE-13, PE-14, PE-15
4.2.1.j	Components shall authorize, monitor, control and maintain records of the delivery and removal of hardware and software that enters and exits a facility.	PE-16
4.2.1.k	Components shall: a. Employ security at an alternate work site that is commensurate with the security categorization level of the information processed and that supports an organizational risk assessment b. Assess as feasible, the effectiveness of security controls at alternate work sites c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.	PE-17

4.2.2 Sensitive Facility

Policy ID	DHS Policy Statements	Relevant Controls
4.2.2.a	Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk shall be determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9

4.3 Media Controls

4.3.1 Media Protection

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.a	Components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as Universal Serial Bus (USB) drives, are stored when not in use in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or in other storage that prohibits access by unauthorized persons).	MP-2, MP-4, PE-1
4.3.1.b	Components shall ensure that all offsite backup media are protected as per guidance in this section.	CP-6
4.3.1.c	DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government-issued removable media (such as USB drives) and from connecting them to DHS equipment or networks or using them to store DHS sensitive information.	MP-2
4.3.1.d	All USB drives shall use encryption in compliance with Section 5.5.1 of this Policy Directive.	IA-7, SC-13
4.3.1.e	DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM). (The respective CISO is the CISO with that system in his or her inventory.)	AC-20, MP-2, PM-9
4.3.1.f	Components shall follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.	MP-1
4.3.1.g	Users shall ensure proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.	SI-12
4.3.1.h	Components shall follow the procedures established by DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, for the transportation or mailing of sensitive media.	MP-5

4.3.2 Media Marking and Transport

Policy ID	DHS Policy Statements	Relevant Controls
4.3.2.a	Media determined by the information owner to contain sensitive information shall be appropriately marked in accordance with DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.	MP-3
4.3.2.b	Components shall control the transport of information system media containing sensitive information, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel.	MP-5

4.3.3 Media Sanitization and Disposal

Policy ID	DHS Policy Statements	Relevant Controls
4.3.3.a	Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.	MP-6
4.3.3.b	Components shall maintain records of the sanitization and disposition of information systems storage media.	MP-6
4.3.3.c	Components shall periodically test degaussing equipment to verify that the equipment is functioning properly.	MP-6

4.3.4 Production, Input/Output Controls

Policy ID	DHS Policy Statements	Relevant Controls
4.3.4.a	Components shall follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.	SI-12
4.3.4.b	These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.	SI-12

4.4 Voice Communications Security

4.4.1 Private Branch Exchange

Policy ID	DHS Policy Statements	Relevant Controls
4.4.1.a	Components shall provide adequate physical and information security for all DHS-owned Private Branch Exchanges (PBX). (Refer to NIST Special Publication (SP) 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)	--

4.4.2 Telephone Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.4.2.a	Components shall develop guidance for discussing sensitive information over the telephone. Guidance shall be approved by a senior Component official and is subject to review and approval by the DHS CISO. Under no circumstances shall classified national security information be discussed over unsecured telephones.	PL-4

4.4.3 Voice Mail

Policy ID	DHS Policy Statements	Relevant Controls
4.4.3.a	Sensitive information shall not be communicated over nor stored in voice mail.	PL-4

4.5 Data Communications

4.5.1 Telecommunications Protection Techniques

Policy ID	DHS Policy Statements	Relevant Controls
4.5.1.a	Components shall carefully select the telecommunications protection techniques that meet their information security needs in the most cost-effective manner, consistent with Departmental and Component information system security policies. Approved protected network services (PNS) may be used as	CM-2

Policy ID	DHS Policy Statements	Relevant Controls
	cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.	
4.5.1.b	In cases with high impact and moderate impact for any of the FIPS 199 security objectives, Components shall establish alternate telecommunications services including necessary agreements to permit the resumption of specified operations for essential missions and business functions within a Component-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	CP-8

4.5.2 Facsimiles

Policy ID	DHS Policy Statements	Relevant Controls
4.5.2.a	Components shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.	SC-1, SC-7, SC-8
4.5.2.b	Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.	AC-4

4.5.3 Video Teleconferencing

Policy ID	DHS Policy Statements	Relevant Controls
4.5.3.a	Components shall implement controls to ensure that only authorized individuals are able to participate in each video conference.	AC-3, PE-3
4.5.3.b	Components shall ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.	SC-8
4.5.3.c	Video teleconferencing equipment and software shall be disabled when not in use.	AC-3, PE-3

4.5.4 Voice over Data Networks

Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over Frame Relay, Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Line (refer to National Institute of Standards and Technology (NIST) SP 800-58 for further information).

Policy ID	DHS Policy Statements	Relevant Controls
4.5.4.a	Prior to implementing voice over data network technology, Components shall conduct rigorous risk assessments and security testing and provide a business justification for its use. Any systems that employ this technology shall be authorized for this purpose with residual risks clearly identified.	SC-19, PM-9
4.5.4.b	Voice over data network implementations shall have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.	SC-19
4.5.4.c	Components shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every element of their voice over data networks.	SC-19
4.5.4.d	Components shall ensure that physical access to voice over data network elements is restricted to authorized personnel.	SC-19

4.6 Wireless Network Communications

Wireless network communications technologies include the following:

- Wireless systems (e.g., Wireless Local Area Networks [WLAN], Wireless Wide Area Networks [WWAN], Wireless Personal Area Networks [WPAN], peer-to-peer wireless networks, information systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols
- Wireless mobile devices capable of storing, processing, or transmitting sensitive information (e.g., Personal Digital Assistants [PDA], smart telephones, two-way pagers, handheld radios, cellular telephones, Personal Communications Services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices)
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, technical investigative communications systems)

- Radio Frequency Identification (RFID)

Policy ID	DHS Policy Statements	Relevant Controls
4.6.a	Components shall not introduce new wireless network communications technologies into the enterprise unless the appropriate AO specifically approves a technology and application.	AC-18
4.6.b	Components using Public Key Infrastructure (PKI)-based encryption on any wireless device shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.	IA-5, SC-12

4.6.1 Wireless Systems

Wireless system policy and procedures are described more completely in Attachment Q1 (*Wireless Systems*) to the *DHS 4300A Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.1.a	Annual information security assessments shall be conducted on all approved wireless systems. Wireless information security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	CA-2, PM-9
4.6.1.b	Plans of Action and Milestones (POA&M) shall be developed to address wireless information security vulnerabilities. Plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.	CA-5, PM-4, PM-9
4.6.1.c	Components shall identify countermeasures to denial-of-service attacks and complete a risk based evaluation prior to approving the use of any non-GFE wireless device.	AC-19, PM-9, SC-5
4.6.1.d	SPs shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure that information security solutions and secure connections to external interfaces are consistently enforced.	SI-3
4.6.1.e	A Migration Plan shall be implemented for legacy wireless systems that are not compliant with DHS information security policy. The migration plan shall outline the provisions, procedures, and restrictions for transitioning the legacy systems to DHS-compliant security architectures. Operation of these noncompliant systems before and during the migration requires an approved waiver to policy from the DHS CISO.	CA-5

Policy ID	DHS Policy Statements	Relevant Controls
4.6.1.f	Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO annually.	AC-18, PM-5
4.6.1.g	Component CISOs shall (1) establish usage restrictions and implementation guidance for wireless technologies; and (2) authorize, monitor, and control wireless access to DHS information systems.	AC-18

4.6.2 Wireless Mobile Devices

Wireless mobile devices include any wireless clients capable of storing, processing, or transmitting sensitive information.

Biometrics may be harvested and are not a secret (in cryptographic terms). For this reason, biometrics should not be utililzed as a single-factor authentication mechanism for *sensitive information*. Component AO's and CISO's should carefully assess the residual risks when authorizing biometric use in mobile device operations.

Guidance applicable to wireless mobile devices is detailed in *DHS 4300A Sensitive Systems Handbook* Attachment Q2, "Mobile Devices."

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.a	Components shall ensure that neither personally-owned wireless mobile devices nor Government-owned wireless mobile devices are permitted in conference rooms or secure facilities where classified information is discussed. Wireless mobile devices and accessories are prohibited in areas where unclassified, sensitive information is discussed, maintained, or distributed unless specifically authorized in writing by the AO(s) for the system(s) used in the area.	AC-19, PL-4; PE-18
4.6.2.b	Wireless mobile devices shall not be tethered or otherwise physically or wirelessly connected to the DHS-wired core network without written consent from the AO.	AC-18, AC-19

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.c	Wireless mobile devices that store, process, or transmit sensitive information shall implement full-disk encryption using NIST FIPS 140-2 Validated encryption modules[4] and strong complex passwords prior to receiving sensitive information. A strong complex password shall be required to decrypt after any power cycling or restart.	AC-19, IA-5, IA-7
4.6.2.d	The AO shall approve the use of wireless mobile devices or software applications used to process, store, or transmit sensitive information from the NSA Commercial Solutions for Classified (CSFC) Program components list[5]; FIPS 201 Approved Products List (APL)[6]; or the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) product list[7]. Mobile devices approved by the AO must be posted in the DHS Enterprise Architecture (EA) Approved Products List (APL) of the Technical Reference Model (TRM).	AC-19, CA-6, IA-7, SC-8, SC-9, SC-13
4.6.2.e	Device mobile code will be downloaded and installed only as approved by the AO. Mobile code approved by the AO must be posted in the DHS Enterprise Architecture (EA) Approved Products List (APL) of the Technical Reference Model (TRM).	SC-18
4.6.2.f	Wireless mobile device operation is permitted only when Component CISO -approved anti-malware software and software patches are current. Anti-malware and software patch versions approved by the Component CISO must be posted in the DHS Enterprise Architecture (EA) Approved Products List (APL) of the Technical Reference Model (TRM).	SI-3
4.6.2.g	The AO will approve appropriate cost-effective countermeasures against denial-of-service attacks prior to wireless device operation.	SC-5 SC-7
4.6.2.h	Components shall maintain a current inventory of all approved wireless mobile devices in operation. The inventory must be posted in the DHS inventory management system.	PM-5

[4] *A list of FIPS 140-2 validated encryption is located at* http://csrc.nist.gov/groups/STM/cmvp/validation.html

[5] *A list of NSA CSFC Program components is located at* *https://www.nsa.gov/ia/programs/csfc_program/component_list.shtml.*

[6] *The FIPS-201 Approved Products List is located at* http://www.idmanagement.gov/approved-products-list

[7] *A list of NIAP-CCEVS products is located at* *https://www.niap-ccevs.org/CCEVS_Products*

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.i	Wireless mobile devices shall be sanitized of all information before being reused by another individual, office, or Component within DHS or before they are retired. Wireless mobile devices that are disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using procedures approved by the AO using NSA-approved media destruction methods as appropriate[8].	MP-6
4.6.2.j	Wireless mobile devices not compliant with DHS information security policy require a migration plan outlining the provisions, procedures, and plans for transitioning these wireless mobile devices to meet 4300A requirements. Operation of these non-compliant systems requires an approved waiver from the DHS CISO.	CA-5 CA-6
4.6.2.k	AOs may authorize use of Biometric tokens as an authentication factor when the mobile device implements physical isolation of secure memory for storage of biometric data and trusted execution environment for reading and processing biometrics	
4.6.2.l	If authorized for use, fingerprint sensors must be touch-based (vs. swipe-based) and must read and process data in a trusted execution environment separated from access by other processes	
4.6.2.m	The use of add-on devices, such as cameras and video/voice recorders, is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via audio, video, Infrared (IR), or Radio Frequency (RF) shall be disabled or powered off in areas where sensitive information is discussed.	AC-19, CM-7, PE-18, SC-7
4.6.2.n	When Biometric fingerprint technology is used as a subsequent unlock method on a mobile device; it shall be configured to allow no more than five (5) consecutive failed fingerprint attempts and upon failure of these attempts require entering the complex password.	AC-19, IA-7, SC-8, SC-9, SC-13
4.6.2.o	Mobile devices shall be configured to lock after a maximum of 10 minutes idle.	
4.6.2.p	Mobile devices shall be configured to lock after a maximum of 10 sequential unsuccessful attempts to gain access.	

[8] *The NSA Media Destruction guidance is located at https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml*

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.q	Components shall ensure that use of a device's native biometric fingerprint authentication technology is permitted by and in compliance with the published DHS Configuration Guide for the device.	
4.6.2.r	When derived PIV credentials are utilized and stored in a FIPS 140-2 validated (a) native device hardware keystore or (b) Mobile Device Manager's (MDMs) software-based keystore; the credential shall be activated by either a knowledge-based or biometric token.	

4.6.2.1 Cellular Phones

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.1.a	Components shall develop guidance for discussing sensitive information on cellular phones. Guidance shall be approved by a senior Component official and is subject to review by the DHS CISO. Under no circumstances shall classified information be discussed on cellular phones.	PL-4

4.6.2.2 Pagers

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.2.a	Pagers shall not be used to transmit sensitive information.	PL-4

4.6.2.3 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional (cell phones, pagers, and radios can surf the Internet, retrieve email, take and transmit pictures). Most of these functions do not have sufficient security.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.3.a	Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.	AC-19, SC-8, SC-12
4.6.2.3.b	Functions that transmit or receive video, IR, or RF signals shall be disabled in areas where sensitive information is discussed.	AC-19, PE-18
4.6.2.3.c	Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used to process, store, or transmit sensitive information, and shall be disabled whenever possible.	---

4.6.2.4 Bluetooth

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.4.a	Bluetooth functionality shall be disabled when not in use.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.b	Master devices (those that have unidirectional control over one or more other devices, such as a smartphone and headset combination) shall include link activity status indicators such as icons or LEDs.	AC-18 CM-6 SC-8 SC-13

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.4.c	Pairing shall be performed as infrequently as possible.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.d	Devices shall use low power to minimize the range of communication.	AC-4 PE-3 PE-18 PE-19
4.6.2.4.e	Devices shall be configured for manual pairing and shall prompt the user to authorize any incoming connection requests; auto pairing shall not be used.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.f	Devices shall be maintained in non-discoverable mode except during device pairing.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.g	Multiple or split communication paths shall not be used on devices.	AC-3 AC-18
4.6.2.4.h	Pairings shall only be made between approved devices. Devices may be paired to receivers in personally owned vehicles for voice communication as approved by the AO.	AC-18 AC-19 AC-20
4.6.2.4.i	Profiles shall be deleted for devices no longer in service.	AC-18 CM-6 SC-8 SC-13
4.6.2.4.j	Devices shall be transported and stored securely at all times.	---

For additional information, please refer to “Bluetooth Security,” Attachment Q 6 to *DHS 4300A Sensitive Systems Handbook.*

4.6.3 Wireless Tactical Systems

Wireless tactical systems include LMR subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures. To ensure secure tactical communications, Components must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

Wireless tactical system policy and procedures are described more completely in Attachment Q3, “Wireless Tactical Systems” to the *DHS 4300A Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.3.a	AOs shall be immediately notified whenever any security feature is disabled in response to time-sensitive, mission-critical incidents.	CM-3
4.6.3.b	Wireless tactical systems shall implement strong identification, authentication, and encryption.	IA-2, IA-7, SC-8
4.6.3.c	Cost-effective countermeasures to denial-of-service attacks shall be identified and implemented prior to a wireless tactical system being approved for use.	SC-5
4.6.3.d	Components shall maintain a current inventory of all approved wireless tactical systems in operation.	PM-5
4.6.3.e	A Migration Plan shall be implemented for legacy tactical wireless systems that are not compliant with DHS information security policy. The migration plan will outline the provisions, procedures, and restrictions for transitioning the legacy systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver from the DHS CISO, as appropriate.	---
4.6.3.f	The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	SC-12
4.6.3.g	All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	CM-2

4.6.4 Radio Frequency Identification

Radio Frequency Identification (RFID) enables wireless identification of objects over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication, that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive information.

RFID procedures are described in "Sensitive RFID Systems," Attachment Q4 to *DHS 4300A Sensitive Systems Handbook.*

Policy ID	DHS Policy Statements	Relevant Controls
4.6.4.a	Components implementing RFID systems shall assess hazards of	PE-18

Policy ID	DHS Policy Statements	Relevant Controls
	electromagnetic radiation to fuel, ordnance, and personnel before deployment of the RFID technology.	
4.6.4.b	Components shall limit data stored on RFID tags to the greatest extent possible, recording information beyond an identifier only when required for the application mission. When data beyond an identifier is stored on a tag, the tag's memory shall be protected by access control.	AR-2, AC-6
4.6.4.c	Components shall develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.	---
4.6.4.d	Components shall identify and implement appropriate operational and technical controls to limit unauthorized tracking or targeting of RFID-tagged items when these items are expected to travel outside the Component's physical perimeter.	AC-14
4.6.4.e	When an RFID system is connected to a DHS data network, Components shall implement network security controls to segregate RFID network elements such as RFID readers, middleware, and databases from other non-RFID network hosts.	CM-6
4.6.4.f	Components implementing RFID technology shall determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.	IA-7, PM-9, RA-3

4.7 Overseas Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.7.a	Where required or appropriate, all communications outside of the United States and its territories shall be in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.	---

4.8 Equipment

4.8.1 Workstations

Policy ID	DHS Policy Statements	Relevant Controls
4.8.1.a	Components shall configure workstations to either log off, or activate a password-protected lock, or password-protected screensaver after 15 minutes of user inactivity.	AC-11, CM-6
4.8.1.b	Components shall ensure that workstations are protected from theft.	PE-3
4.8.1.c	Users shall either log off or lock their workstations when unattended.	---

4.8.2 Laptop Computers and Other Mobile Computing Devices

Policy ID	DHS Policy Statements	Relevant Controls
4.8.2.a	Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption in accordance with Section 5.5.1, Encryption, for data at rest and in motion. Passwords, tokens and Smart Cards shall not be stored on or with the laptop or other mobile computing device.	AC-19, IA-2, SC-12, SC-28
4.8.2.b	Laptop computers shall be powered down when not in use (due to volatile memory vulnerabilities).	AC-19, PL-4
4.8.2.c	When unattended, laptop computers and other mobile computing devices shall be secured using one of the following methods: • a locked office • a locking cable • a locked cabinet • a locked desk	AC-19, PE-3, PL-4
4.8.2.d	Users shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device outside of the United States or its territories.	AC-19, PL-4

4.8.3 Personally Owned Equipment and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.a	Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the AO.	CM-10, CM-11

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.b	Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component CISO/ISSM.	SA-9
4.8.3.c	Any device that has been obtained through civil or criminal asset forfeiture shall not be used as part of a DHS information system nor used to process DHS data.	AC-20

4.8.4 Hardware and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.a	Components shall ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications published by the DHS CISO. *DHS 4300A Sensitive Systems Handbook* includes the DHS Secure Baseline Configuration Guides.	CM-2, CM-6
4.8.4.b	Components shall limit access to system software and hardware to authorized personnel.	AC-3, CM-5
4.8.4.c	Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their CM Plan.	CM-2, CM-3
4.8.4.d	Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services. When the technology is available, Components shall ensure that their systems are protected against pass-the-hash and lateral movement vulnerabilities.	CM-3, RA-5
4.8.4.e	Components shall ensure that maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.	MA-1
4.8.4.f	System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.4.g	Components shall develop maintenance policy and procedures.	MA-1
4.8.4.h	If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. Components shall take all possible steps to ensure that trusted maintenance personnel are available.	MA-5
4.8.4.i	Maintenance using a different user's identity may be performed only when the user is present. The *user* shall log in and observe the maintenance actions at all times. *Users shall not share their authentication information with maintenance personnel.*	MA-5

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.j	Components shall define and utilize a process for the scheduling, performance, approvals, documenting, testing, and clearing of equipment requiring maintenance. The process shall protect sensitive information by requiring authorized personnel to explicitly: a. Approve the removal of an information system or system Components from organizational facilities for off-site maintenance or repairs; b. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and c. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	MA-2
4.8.4.k	Components shall approve, control, and monitor information system maintenance tools.	MA-3
4.8.4.l	Components shall obtain information system maintenance support and/or spare parts within a Component-defined time period after failure.	MA-6
4.8.4.m	Components shall include requirements for software assurance and supply chain risk management prior to acquisition of any hardware or software products. Components shall ensure that commercial-off-the-shelf (COTS) hardware and software products in use by or being considered for use in moderate and high criticality systems, shall be analyzed for supply chain risk prior to acquisition activities that procure new products, upgrade existing products, or that will integrate these products with commercial services.	

4.8.5 Personal Use of Government Office Equipment and DHS Systems/Computers

Policy ID	DHS Policy Statements	Relevant Controls
4.8.5.a	DHS employees may use Government office equipment and DHS systems/computers for authorized purposes only. "Authorized use" includes limited personal use as described in DHS MD 4600.1, *Personal Use of Government Office Equipment*, and DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*.	---

Policy ID	DHS Policy Statements	Relevant Controls
4.8.5.b	Limited personal use of DHS email and Internet services is authorized for DHS employees as long as this use does not interfere with official duties, inhibit the security of information and information systems, or cause degradation of network services. Specifically prohibited activities include streaming of audio or video, social networking, peer-to-peer networking, software or music sharing/piracy, online gaming, Webmail, Instant Messaging (IM), hacking, and the viewing of pornography or other offensive content. DHS users shall comply with the provisions of DHS MD 4500.1, *DHS Email Usage*, and DHS MD 4400.1, *DHS Web and Information Systems*.	---
4.8.5.c	Anyone granted user account access to any DHS information system (including DHS employees, contractors, and others working on behalf of DHS) shall have no expectations of privacy associated with its use. By completing the authentication process, the user acknowledges his or her consent to monitoring.	AC-8
4.8.5.d	The use of Government office equipment and DHS systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.	AC-8
4.8.5.e	DHS users are required to sign rules of behavior prior to being granted system accounts or access to DHS systems or data. The rules of behavior shall contain a “Consent to Monitor” provision and an acknowledgement that the user has no expectation of privacy.	PL-4
4.8.5.f	Contractors, others working on behalf of DHS, or other non-DHS employees are not authorized to use Government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the contract or memorandum of agreement. When so authorized, the limited personal use policies of this section and the provisions of DHS MD 4600.1, DHS MD 4900, DHS MD 4400.1, and DHS MD 4500.1 shall apply.	---

4.8.6 Wireless Settings for Peripheral Equipment

Peripheral equipment (printers, scanners, fax machines) often includes capabilities, intended to allow wireless access to these devices. Although convenient, wireless access comes with additional risks. In general, wireless access is not allowed on DHS networks.

Policy ID	DHS Policy Statements	Relevant Controls
4.8.6.a	Components shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any DHS network or to systems processing or hosting DHS sensitive information.	CM-7
4.8.6.b	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, Components shall comply with all requirements outlined in Section 4.6, Wireless Communication *and* obtain a waiver in accordance with this policy.	CM-7, IR-4, IR-6

4.9 Department Information Security Operations

The DHS Security Operations Center (SOC) is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The Homeland Secure Data Network (HSDN) Security Operations Center (SOC) shall report incidents to the DHS SOC through appropriate channels to protect data classification. The HSDN SOC is subordinate to the DHS SOC, acting as the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department.

The CIO is responsible for implementing firewall changes in a timely manner.

Policy ID	DHS Policy Statements	Relevant Controls
4.9.a	It is the policy of DHS that employees, contractors, or others working on behalf of DHS have no privacy expectations associated with the use of any DHS network, system, or application. This policy is further extended to anyone who is granted account access to any network, system, or application in use in the Department. By completing the account login process the account owner acknowledges their consent to monitoring.	AC-8, PL-4
4.9.b	Component SOCs shall be operationally subordinate to the DHS SOC, which shall provide them operational oversight and guidance. HSDN SOC will oversee the handling of all incidents occurring on HSDN and coordinate the sharing of incident information with DHS SOC.	IR-1, IR-4, IR-6

Policy ID	DHS Policy Statements	Relevant Controls
4.9.c	The DHS SOC or Component SOCs shall lead the coordination and administration of Department and Component policy enforcement points, such as firewalls.	SC-7
4.9.d	The DHS SOC shall implement the Department logging strategy, coordinated with Component SOCs, to enable endpoint visibility and Departmental situational awareness. DHS SOC is responsible for monitoring shared infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Points (PEP), and Email Secure Gateway (EMSG). Component SOCs are responsible for monitoring at a minimum internal enclave network traffic and internal host network and host-based activity.	---
4.9.e	All SOCs shall have the capability to process intelligence information at the collateral level or above. The DHS SOC and Component SOCs shall have the ability to process SECRET level information continuously and shall have the capability to receive Top Secret / Sensitive Compartmented Information (TS/SCI) information.	IR-4
4.9.f	SOCs shall ensure that personnel are appropriately cleared to access the DHS C-LAN. SOC managers are free to determine the number and type of personnel to be cleared, but at least one cleared person shall be available per shift (this person may be on call). A Government officer shall be available continuously for incident response and management.	IR-4
4.9.g	All Department SOCs shall establish and maintain a Digital Malware Analysis (DMA) capability as outlined in the DHS Security Operations Concept of Operations (SOC CONOPS).	IR-7
4.9.h	Department information security operations shall provide a vulnerability management capability. DHS SOC provides Information Security Vulnerability Management (ISVM) messages and vulnerability assessment capabilities. Components are required to comply with the ISVMs released by the DHS SOC. Component SOCs shall develop a robust vulnerability management capability to compliment the DHS SOC.	SI-5
4.9.i	Component CISOs shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other appropriate persons.	SI-5
4.9.j	Component SOCs shall report operationally to their respective Component CISO. Each CISO shall exercise oversight over their Component's information security operations functions, including the Component SOCs.	IR-1
4.9.k	The DHS SOC shall report operationally to the DHS CISO.	---

Policy ID	DHS Policy Statements	Relevant Controls
4.9.l	The NOC/SOC shall be under the direction of a Government employee who shall be present at all times.	

4.9.1 Security Incidents and Incident Response and Reporting

Policy ID	DHS Policy Statements	Relevant Controls
4.9.1.a	Components shall establish and maintain a continuous 24x7 incident response capability.	IR-1
4.9.1.b	Component SOCs shall report significant incidents to the DHS SOC via EOCOnline (https://eoconline.dhs.gov) as soon as possible but not later than one hour after the DHS SOC report. Other means of reporting, such as calling 1-877-DHS1NET (1-877-347-1638) or emailing DHS.SOC@dhs.gov are acceptable, but the Component shall positively verify that notification, if not submitted via EOConline, is acknowledged by the DHS SOC.	IR-6
4.9.1.c	Significant HSDN incidents shall be documented with an initial detailed report to the HSDN Government Watch Officer and to the DHS SOC via secure communications, via HSDN or Secure Terminal Equipment (STE) cleared to the level commensurate with the incident being reported, as soon as possible but not later than one hour after the DHS SOC report. Subsequent updates and status reports shall be provided to the HSDN SOC and to the DHS SOC via secure email whenever new information is discovered. Significant incidents are reported individually and shall not be reported in the monthly summary report.	IR-6
4.9.1.d	Components shall report minor incidents via the DHS SOC portal (https://eoconline.dhs.gov) within 24 hours of validation. Components without portal access shall temporarily report minor incidents via email to dhs.soc@dhs.gov. HSDN incidents or incidents involving SECRET information shall be documented in a summary report and sent via secure email to the HSDN SOC.	IR-6
4.9.1.e	DHS personnel shall follow DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with the DHS SOC CONOPS. Reports shall be classified at the highest classification level of the information contained in the document. Unsanitized reports shall be marked and handled appropriately.	IR-1

Policy ID	DHS Policy Statements	Relevant Controls
4.9.1.f	The DHS SOC shall report incidents to the United States Computer Emergency Readiness Team (US-CERT) in accordance with the DHS SOC CONOPS. Components shall not send incident reports directly to US-CERT.	IR-6
4.9.1.g	The DHS SOC shall receive classified spillage incident reports, and support the DHS CSO for containment and cleanup. All classified spillages are significant incidents.	IR-6
4.9.1.h	The DHS SOC shall maintain information security "playbooks" that implement procedures and provide guidance on how to respond rapidly to developing incidents.	IR-1
4.9.1.i	The DHS SOC shall respond to cyber-attacks, events, and incidents pertaining to DHS assets. When an external organization is involved, the DHS SOC will coordinate with the external organization through US-CERT, except in time-sensitive cases where a response requires direct contact with the external organization.	IR-1
4.9.1.j	Components shall maintain a full SOC capability or outsource SOC capability to the DHS SOC. The DHS SOC shall provide SOC services to Components in accordance with formal agreements. Information regarding incident response capability is available in "Incident Response," Attachment F to the *DHS 4300A Sensitive Systems Handbook*.	IR-7 IR-8
4.9.1.k	Components shall develop and publish internal computer security incident response plans and incident handling procedures, and make copies available to the DHS SOC upon request. Each procedure shall include a detailed Configuration Management (CM) process for modification of security device configurations.	IR-1
4.9.1.l	Component Heads shall ensure that corrective actions are taken when security incidents and violations occur, and shall hold personnel accountable for intentional misconduct.	IR-1
4.9.1.m	The DHS SOC shall monitor and report incident investigation and incident remediation activities to the DHS Chief Information Officer (CIO) and CISO in accordance with the DHS SOC CONOPS until the incident is closed.	IR-5
4.9.1.n	The DHS CISO shall determine the frequency and content of security incident reports.	IR-6
4.9.1.o	The Component SOC shall report incidents only to the DHS SOC and to no other external agency or organization.	IR-6
4.9.1.p	The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required.	IR-1

Policy ID	DHS Policy Statements	Relevant Controls
4.9.1.q	The Component CISO for each Component that provides an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO.	IR-3

4.9.2 Law Enforcement Incident Response

The DHS SOC shall notify the DHS Chief, Internal Security and Investigations Division, Office of Security (CISID-OIS) whenever an incident requires law enforcement involvement. Law enforcement shall coordinate with the DHS SOC, the CISID-OIS, the Component, and other appropriate parties whenever a crime is committed or suspected.

Policy ID	DHS Policy Statements	Relevant Controls
4.9.2.a	Components shall coordinate all external Law Enforcement (LE) involvements through the DHS SOC and obtain guidance from the DHS SOC before contacting local law enforcement. Exceptions are only made during emergencies where there is risk to life, limb, or property. In cases of emergency notification, the Component shall notify the DHS SOC as soon as possible, by the most expedient means available.	IR-6
4.9.2.b	Security incidents may include law enforcement (LE) or counterintelligence (CI) elements, such as maintaining a chain of custody. All incidents containing a LE/CI aspect shall be coordinated with the DHS CSO through the DHS SOC.	IR-6

4.10 Documentation

Policy ID	DHS Policy Statements	Relevant Controls
4.10.a	Components shall ensure that information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.	CM-8

Policy ID	DHS Policy Statements	Relevant Controls
4.10.b	System Owners shall update system documentation annually or whenever significant changes occur. Changes that may require updates include: • New threat information • Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach • A redefinition of mission priorities or business objectives resulting in a change to the security category of the information system • A change in the information system (e.g., adding new hardware, software, or firmware; or establishing new connections) or the system's environment of operation	CM-3, CM-8, SA-5
4.10.c	Documentation shall be kept on hand and shall be accessible to authorized personnel (including auditors) at all times.	CM-3, SA-5
4.10.d	System documentation may be categorized as Sensitive if deemed appropriate by the Component CISO/ISSM. This category shall not be used as a means of restricting access to auditors or other authorized personnel.	CM-3

4.11 Information and Data Backup

Policy ID	DHS Policy Statements	Relevant Controls
4.11.a	The policies in this document, including Security Authorization Process requirements, apply to any devices that process or host DHS data.	---
4.11.b	Component CISOs/ISSMs shall determine whether or not automated process devices shall be included as part of an information system's Security Authorization Process requirements.	---
4.11.c	Components shall implement and enforce backup procedures as part of their contingency planning.	CP-9
4.11.d	All portable backup media in transit shall use encryption in compliance with Section 5.5.1 of this Policy Directive.	CP-9
4.11.e	Components shall follow the procedures established by DHS Management Directive (MD) 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, for the transportation or mailing of backup media.	MP-5

Policy ID	DHS Policy Statements	Relevant Controls
4.11.f	Backup media shall be shipped using an accountable delivery service (e.g. U.S. Postal Service First Class Mail, Federal Express, United Parcel Service) and shall be properly inventoried.	CP-9, MP-5
4.11.g	Every information system shall have a documented chain of custody process for the handling and transportation of portable backup media.	MP-5

4.12 Converging Technologies

Advances in technology have resulted in the availability of devices that offer multiple functions. Many devices such as multifunctional desktop computers, copiers, facsimile machines, and heating, ventilation and air conditioning (HVAC) systems may contain sensitive information and may also be connected to data communications networks.

Policy ID	DHS Policy Statements	Relevant Controls
4.12.a	The policies in this document apply to any networked devices that contain Information Technology (IT), including copiers, facsimile machines, and alarm control systems.	---
4.12.b	Components shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.	CM-2
4.12.c	Components shall ensure that network printers, copiers, and facsimile machines are configured for least required functionality.	CM-7
4.12.d	Components shall ensure that each network printer, copier, and facsimile machine is within the system definition of a DHS information system that has a current ATO.	CM-8, PL-2
4.12.e	Components shall ensure that remote maintenance of network printers, copiers, and facsimile machines is conducted only from within DHS networks. If maintenance planning does not include performing remote maintenance, Components shall ensure that remote maintenance capabilities are disabled.	MA-4
4.12.f	Components shall ensure that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized individuals or groups.	MA-5

Policy ID	DHS Policy Statements	Relevant Controls
4.12.g	Components shall ensure that maintenance or disposal of network printers, copiers, or facsimile machines, approved for sensitive reproduction, is performed only while escorted by a properly cleared person with knowledge to detect any inappropriate action.	MA-5
4.12.h	Components shall ensure that memory and hard drives do not leave the facility; they are to be replaced and the old part destroyed as sensitive media.	MP-6
4.12.i	Components shall locate network printers, copiers, and facsimile machines approved to process sensitive information in areas where access can be controlled when paper output is being created.	PE-18
4.12.j	Any multifunction device connected to a DHS network or other information system containing sensitive information shall have the inbound dial in capabilities disabled.	AC-17

5.0 TECHNICAL POLICIES

The design of information systems that process, store, or transmit sensitive information shall include the automated security features discussed in this section. Security safeguards shall be in place to ensure that each person having access to sensitive information systems is individually accountable for his or her actions while utilizing the system.

5.1 Identification and Authentication

Policy ID	DHS Policy Statements	Relevant Controls
5.1.a	Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1, IA-2
5.1.b	For information systems requiring authentication controls, Components shall ensure that the information system is configured to require that each user be authenticated before information system access occurs.	IA-1, IA-2
5.1.c	For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after 90 days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after 45 days of inactivity. This policy applies to anyone who is granted account access to any network, system, or application in use in the Department.	IA-4
5.1.d	Department of Homeland Security (DHS) users shall not share identification or authentication materials of any kind, nor shall any DHS user allow any other person to operate any DHS system by employing the user's identity.	IA-5
5.1.e	All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive information to which that user is granted access using that authenticator.	IA-7
5.1.f	Components shall implement strong authentication on servers, for system administrators and personnel with significant security responsibilities, within six (6) months of the Component's implementation of HSPD-12 [9].	IA-2

[9] *HSPD = Homeland Security Presidential Directive*

Policy ID	DHS Policy Statements	Relevant Controls
5.1.g	Personal Identification Verification (PIV) credentials or alternative solutions that provide NIST SP 800-63-2 Level of Assurance (LOA) 4 of the user's identity shall be used as the primary means of logical authentication for DHS sensitive systems. Per NIST SP 800-63-2, "Electronic Authentication Guideline," a username, password and single factor one-time password (e.g. RSA SecurlD) is not LOA 4-compliant.	---
5.1.h	Mandatory smart card logon shall be implemented by means of Identity (user) Based Enforcement	IA-2
5.1.i	Privileged network users shall use the DHS HSPD-12 credential for authentication to all DHS Privileged network user accounts.	IA-2
5.1.j	Only approved DHS Privileged Network User Management solutions shall be employed. A waiver request will be required for use of any other solution(s).	---
5.1.k	Systems shall prompt privileged users to enter the PIV PIN to initiate an encrypted authenticate session.	---
5.1.l	Password authentication shall be disabled for all accounts. Where applicable, all password-based authentication modules shall be disabled. This policy applies to all IP-addressable devices.	---
5.1.m	All system access shall be by use of the user's PIV card.	IA-2
5.1.n	Users shall report lost, stolen, or inadvertently destroyed PIV cards to the Help Desk, who shall supply for logon a temporary password account that shall expire within 5 days of creation.	---
5.1.o	Users shall report forgotten or misplaced PIV cards to the Help Desk, who shall supply for logon a temporary password account that shall expire 24 hours after creation.	---

5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as Smart Cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), shall be cost-justified through the risk assessment process.

Guidance for the creation of strong passwords is available in Section 5.1.1.1 of the *DHS 4300A Sensitive Systems Handbook.*

Policy ID	DHS Policy Statements	Relevant Controls
5.1.1.a	In those systems where user identity is authenticated by password, Components shall ensure that DHS information systems follow the hardening guides for operating systems (found at http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sscg.aspx) and the configuration guides for applications promulgated by the DHS CISO to determine and enforce appropriate measures to ensure that strong passwords are used. In the absence of appropriate password complexity guidance, the system Information Systems Security Officer (ISSO) shall determine and enforce appropriate measures to ensure that strong passwords are used.	IA-5
5.1.1.b	The ISSO shall determine and enforce the appropriate frequency for changing passwords in accordance with appropriate guidance documentation (if published). In the absence of specific guidance documentation, passwords shall not remain in effect longer than ninety (90) days.	IA-5
5.1.1.c	DHS users shall not share personal passwords.	IA-5
5.1.1.d	Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. Use of a group User ID and password shall be approved by the appropriate Authorizing Official (AO).	IA-4
5.1.1.e	Components shall prohibit passwords from being embedded in scripts or source code.	IA-5
5.1.1.f	Components shall ensure that all passwords are stored in encrypted form.	IA-5
5.1.1.g	Systems shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	IA-6

The use of a personal password by more than one individual is prohibited throughout DHS. It is recognized, however, that, in certain circumstances such as the operation of crisis management or operations centers, watch team and other duty personnel may require the use of group User IDs and passwords.

5.2 Access Control

Policy ID	DHS Policy Statements	Relevant Controls
5.2.a	Components shall implement access control policy and procedures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control shall follow the principles of least privilege and segregation of duties and shall require users to use unique identifiers. *Social Security Numbers shall not be used as login IDs.*	AC-5 AC-6
5.2.c	Users shall not provide their passwords to anyone, including system administrators.	IA-5
5.2.d	Emergency and temporary access authorization shall be strictly controlled and shall be approved by the Component Chief Information Security Officer (CISO) or Information Systems Security Manager (ISSM) or his/her designee prior to being granted.	AC-2
5.2.e	System Owners shall ensure that users are assigned unique account identifiers.	IA-4
5.2.f	DHS systems with a Federal Information Processing Standard (FIPS) 199 confidentiality categorization of high shall limit the number of concurrent sessions for any user to one (1) unless strong authentication is used.	AC-10
5.2.g	Components and Programs shall ensure that all data-at-rest, particularly in cloud or other virtual environments, preserves its identification and access requirements (anyone with access to data storage containing more than one type of information must have specific access authorization for every type of data in the data storage).	---

5.2.1 Automatic Account Lockout

Components shall configure each information system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts. Users shall be locked from their account for a period of 20 minutes after three consecutive failed logon attempts. All failed logon attempts must be recorded in an audit log and periodically reviewed.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.a	Components shall configure accounts to automatically lock a user's *account* after three consecutive failed logon attempts.	AC-7

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.b	The automatic lockout period for accounts locked due to failed login attempts shall be set for 20 minutes.	AC-7
5.2.1.c	Components shall establish a process for manually unlocking accounts prior to the expiration of the 20 minute period, after sufficient user identification is established. This may be accomplished through the help desk.	AC-7

5.2.2 Automatic Session Termination

The term *session* refers to a connection between a terminal device (workstation, laptop, mobile device) and a networked application or system. The term also refers to accessing an application or system such as a database or networked application through the DHS network. The term does not apply to a direct connection to a DHS network, as when authenticating from a device that is directly connected to a DHS network. When a session is locked, the user may resume activity by reauthenticating.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.2.a	Components shall configure networked applications or systems to automatically lock any user session in accordance with the appropriate configuration guide. In the absence of configuration guidance, the session shall lock following 20 minutes of inactivity.	AC-11
5.2.2.b	Locked sessions shall remain locked until the user re-authenticates.	AC-11
5.2.2.c	Sessions shall be automatically terminated after 60 minutes of inactivity.	SC-10

5.2.3 Warning Banner

The DHS CISO stipulates that a warning banner statement be displayed on all DHS systems during logon. The most current language can be found on the DHS CISO Web page.

Please note that the current warning banner was developed specifically for use on DHS workstations. Due to differing functions, purposes and situations, and to length requirements, warning banners for other environments, such as routers, switches and public-facing websites, will be developed and included in a future version of the *DHS 4300A Sensitive Systems Handbook.*

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.3.a	Systems internal to the DHS network shall display a warning banner specified by the DHS CISO.	AC-8
5.2.3.b	Systems accessible to the public shall provide both a security and a privacy statement at every entry point.	AC-8

5.3 Auditing

Policy ID	DHS Policy Statements	Relevant Controls
5.3.a	Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the SP. The audit record shall contain at least the following information: - Identity of each user and device accessing or attempting to access the system - Time and date of the access and the logoff - Activities that might modify, bypass, or negate information security safeguards - Security-relevant actions associated with processing - All activities performed using an administrator's identity When the technology is available, Components shall ensure implementation of enterprise auditing and recording of sessions (keystroke and graphical).	AU-3, AU-12
5.3.b	Audit records for financial systems or for systems hosting or processing Personally Identifiable Information (PII) shall be reviewed each month. Unusual activity or unexplained access attempts shall be reported to the System Owner and to the Component CISO/ISSM.	AU-6
5.3.c	Components shall ensure that their audit records and audit logs are protected from unauthorized access, modification, or destruction.	AU-9

Policy ID	DHS Policy Statements	Relevant Controls
5.3.d	Components shall ensure that audit logs are recorded and retained in accordance with the Component's Record Schedule or with the DHS Records Schedule. At a minimum audit trail records shall be maintained online for at least 90 days. Audit trail records shall be preserved for a period of three years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. Components shall allocate appropriate audit record storage capacity in accordance with these requirements.	AU-4, AU-11
5.3.e	Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SP.	AU-1, AU-2, AU-3, PM-9
5.3.f	Component Security Operations Centers (SOC) shall implement both general and threat-specific logging.	AU-1, AU-2
5.3.g	Components shall ensure that information systems alert the Component or DHS SOC in the event of an audit processing failure and overwrite the oldest audit records, if an analysis of the mission needs and the risk to the system preclude system shutdown.	AU-5
5.3.h	Components shall ensure that information systems provide an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents b. Does not alter the original content or time ordering of audit records. (This capability could be as simple as a text editor that allows the administrator to produce a sorted text file, or extract data from an audit log.)	AU-7
5.3.i	Components shall ensure that audit logs employ a consistent time stamp across all systems.	AU-8

5.4 Network and Communications Security

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access DHS networks by dialing in via modem or accessing the DHS network via the Internet. This allows mobile employees to stay in touch with the home office while traveling. There are significant security risks, however, associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks.

Policy ID	**DHS Policy Statements**	**Relevant Controls**
5.4.1.a	Data communication connections via modem shall be limited and shall be tightly controlled, as such connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless they have been authorized by the Component CISO/ISSM. Approved remote access to DHS networks shall only be accomplished through equipment specifically approved for that purpose. Tethering with wireless devices is prohibited unless approved by the appropriate AO.	AC-17,
5.4.1.b	Components shall centrally manage all remote access and dial-in connections to their systems and shall ensure that remote access and approved dial-in capabilities provide strong two-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. DHS has an immediate goal that remote access shall only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication shall be based on Department-controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions shall comply with the encryption requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. See Section 3.14 of this Policy Directive, “Privacy and Data Security” for additional requirements involving remote access of PII.	AC-4, AC-17, AU-2, SC-7, SC-8,
5.4.1.c	Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished by means of Virtual Private Network (VPN) or equivalent encryption and two-factor authentication. The Risk Assessment and Security Plan (SP) shall document any remote access of PII, and the remote access shall be approved by the AO prior to implementation.	AC-4, AC-17, AU-2, SC-7, SC-8,
5.4.1.d	Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented in the SP.	---

5.4.2 Network Security Monitoring

Security monitoring, detection, and analysis are key functions and are critical to maintaining the security of DHS information systems. Network monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.2.a	Components shall provide continuous monitoring of their networks for security events, or outsource this requirement to the DHS Security Operations Center (SOC). Monitoring includes interception and disclosure as to the extent necessary for rendering service or to protect Department or Component rights or property as well as properly identified and categorized information of third parties when required by the Department or a Component. Here *rights* refers to ownership or entitlements or to property or information as in intellectual property. Service observation or random monitoring shall not be used except for mechanical or service quality control checks in accordance with the Electronic Communications Privacy Act.	SI-4
5.4.2.b	The DHS SOC shall administer and monitor DHS intrusion detection system (IDS) sensors and security devices.	SI-4
5.4.2.c	Component SOCs shall administer and monitor Component IDS sensors and security devices.	SI-4
5.4.2.d	Components shall establish monitoring scope at least as comprehensive and stringent as described in Attachment F, "Incident Response," to *DHS 4300A Sensitive Systems Handbook*.	---

5.4.3 Network Connectivity

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources by passing data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. System interconnections include connections that are permanent in nature, connections that are established by automated scripts at prescribed intervals, and/or connections which utilize Web and Service Oriented Architecture (SOA) services. System interconnections do not include instances of a user logging on to add or retrieve data, nor users accessing Web-enabled applications through a browser. External connections are defined as system(s) or IP addressable end points that are not under the direct control of DHS, systems that have IP addressing not in the DHS addressing scheme (routable and non-routable), or systems that have an authorizing official who is not a DHS employee.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.a	Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network element.	AC-1, AC-2, AU-1, AU-2, IA-1, IA-2
5.4.3.b	Interconnections between DHS and non-DHS systems shall be established only through the Trusted Internet Connection (TIC) and by approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memorandums of understanding, Service Level Agreements (SLA) or Interconnection Security Agreements (ISA).	CA-3
5.4.3.c	Components shall document all interconnections to the DHS OneNet with an ISA signed by the OneNet AO and by each appropriate AO. Additional information on ISAs is published in, “Preparation of Interconnection Security Agreements,” Attachment N to the *DHS 4300A Sensitive Systems Handbook.*	CA-3
5.4.3.d	ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.	CA-3
5.4.3.e	ISAs shall be reviewed and updated as needed as a part of the annual Federal Information Security Modernization Act of 2014 (FISMA) self-assessment.	CA-3
5.4.3.f	Components may complete a master Interconnection Security Agreement (ISA) that includes all transitioning systems as part of their initial OneNet transition. After transition, each additional system or General Support System (GSS) shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. (In this context, *security policies* refers to the set of rules that controls a system’s working environment, and not to DHS information security policy). ISAs shall be signed by the appropriate AO.	---
5.4.3.g	Components shall document interconnections between their own and external (non-DHS) networks with an ISA for each connection.	CA-3
5.4.3.h	The DHS Chief Information Officer (CIO) shall approve all interconnections between DHS enterprise-level information systems and non-DHS information systems. The DHS CIO shall ensure that connections with other Federal Government agencies are properly documented. A single ISA may be used for multiple connections provided that the security authorization is the same for all connections covered by that ISA.	CA-3

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.i	The Department and Components shall implement Trust Zones by means of Policy Enforcement Points (PEP), as defined in the DHS Security Architecture Framework.	SC-7
5.4.3.j	DHS OneNet shall provide secure Name/Address resolution service. Domain Name System Security Extensions (DNSSEC) has been designated as the DHS service solution.	SC-20, SC-21, SC-22
5.4.3.k	All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.	SC-20, SC-21, SC-22
5.4.3.l	The appropriate Change Control Board (CCB) shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.	CM-3
5.4.3.m	Interconnections between two authorized DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as an SLA or contract, and the risks have been assessed and accepted by all involved AOs.	CA-3
5.4.3.n	Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.	---
5.4.3.o	The information system shall protect the authenticity of communications sessions.	SC-23
5.4.3.p	For systems with high or moderate impact for any of the FIPS 199 security objectives, system resource sharing shall be limited to an operational need. The information system shall prevent unauthorized and unintended information transfer via shared system resources. All information transfer is limited to that information which has been included in the SP and has been analyzed in the risk assessment for the system.	SC-4

5.4.4 Firewalls and Policy Enforcement Points

Policy Enforcement Points (PEP) separate Trust Zones as defined in the DHS Security Architecture. Boundary protection between DHS and external networks is implemented by firewalls at the TICs and other approved direct system interconnections. DHS TICs are provided by OneNet and monitored by the DHS SOC. Component SOCs may protect DHS-internal boundaries across Trust Zones.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.a	Components shall restrict physical access to firewalls and PEPs to authorized personnel.	AC-4, SC-7
5.4.4.b	Components shall implement identification and strong authentication for administration of the firewalls and PEPs.	--
5.4.4.c	Components shall encrypt remote maintenance paths to firewalls and PEPs.	MA-4, SC-7
5.4.4.d	Components shall conduct quarterly firewall and PEP testing to ensure that the most recent policy changes have been implemented and that *all* applied policies and controls are operating as intended.	SC-7
5.4.4.e	Component SOCs shall ensure that reports on information security operations status and incident reporting are provided to the DHS CISO as required by this Policy Directive.	IR-6
5.4.4.f	All Department and Component firewalls and PEPs shall be administered in coordination with DHS security operation capabilities, through the DHS SOC or Component SOC.	SC-7
5.4.4.g	All DHS PEPs shall provide protection against denial-of-service attacks.	SC-5
5.4.4.h	Components shall determine protocols and services permitted through their Component-level PEPs. Components may restrict traffic sources and destinations at their Component-level PEPs.	SC-7
5.4.4.i	The DHS CISO shall establish policy to block or allow traffic from sources and to destinations at the DHS TIC PEPs. The DHS CISO policy shall prevent traffic as directed by the DHS CIO.	SC-7
5.4.4.j	The DHS SOC shall oversee all enterprise PEPs.	---
5.4.4.k	Components shall ensure each information system separates user functionality (including user interface services) from information system management functionality. User interface services (e.g., public web pages) are separated physically and logically from information storage and management services (e.g., database management). The separation may be accomplished through the use of different computers, different central processing units, different instances of operating systems, different network addresses, or a combination of these or other techniques. (Isolation of a public Web page in a Demilitarized Zone (DMZ) is an example of this separation.)	SC-2, SC-32
5.4.4.l	For high impact systems, the information system isolates security functions from other functions.	SC-3

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.m	For high impact systems, the information system shall fail to a known-state while preserving system state information in failure.	SC-24
5.4.4.n	For high impact systems, the information system shall: a. Verify the correct operation of related security functions b. Perform this verification upon reboot, or command by user with appropriate privilege c. Notify an authorized person of failed security verification tests d. Provide for a Component-defined action (e.g., shut the information system down, or restart the information system) when anomalies are discovered.	SI-6

5.4.5 Internet Security

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.a	Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS TIC PEPs. The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time.	SC-7
5.4.5.b	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.	CM-7, SC-7, SC-8
5.4.5.c	Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by the Program Manager prior to the code being allowed to execute within the DHS environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be "Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS systems."]	SC-18
5.4.5.d	Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.e	File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8
5.4.5.f	Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange).	AC-17, IA-2
5.4.5.g	In order to ensure the security and availability of DHS information and information systems, the DHS CIO or DHS CISO may direct that specific Internet websites or categories be blocked at the DHS TICs, on advice from the United States Computer Emergency Readiness Team (US-CERT), the DHS SOC, or other reputable sources.	---

5.4.6 Email Security

The DHS email gateway Steward provides email monitoring for spam and virus activity at the gateway.

DHS SOC personnel shall be trained to respond to incidents pertaining to email security and shall assist the email gateway Steward as necessary. Components shall provide appropriate security for their email systems.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.a	Components shall correctly secure, install, and configure the underlying email operating system.	---
5.4.6.b	Components shall correctly secure, install, and configure mail server software.	---
5.4.6.c	Components shall secure and filter email content.	---
5.4.6.d	Components shall deploy appropriate network protection mechanisms, such as: - Firewalls - Routers - Switches - Intrusion detection systems	---
5.4.6.e	Components shall secure mail clients.	---

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.f	Components shall conduct mail server administration in a secure manner. This includes: - Performing regular backups - Performing periodic security testing - Updating and patching software - Reviewing audit logs at least weekly	---
5.4.6.g	The DHS email gateway Steward shall provide email monitoring for malware activity at the gateway.	SI-3
5.4.6.h	The DHS email gateway Steward shall provide email monitoring for spam at the gateway.	SI-8
5.4.6.i	Auto-forwarding or redirecting of DHS email to any address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risks or consequences are minimal.	---
5.4.6.j	All DHS email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other Departments and agencies.	---
5.4.6.k	When sending email containing any unencrypted sensitive information, particularly sensitive PII, users should use caution. When sending such information outside the dhs.gov domain, users shall ensure that the information is encrypted.	
5.4.6.l	Only Government email accounts shall be used to perform Government business.	

5.4.7 Personal Email Accounts

Policy ID	DHS Policy Statements	Relevant Controls
5.4.7.a	The use of Internet Webmail (e.g., Gmail, Yahoo, AOL) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---

5.4.8 Testing and Vulnerability Management

The DHS SOC takes a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through Information System Vulnerability Management (ISVM) messages, and conducting Vulnerability Assessments.

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security control assessments.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.8.a	Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or whenever significant changes are made to the information systems. This shall include scanning for unauthorized wireless devices on the network. Evidence that annual assessments have been conducted shall be included in SARs and with annual security control assessments.	---
5.4.8.b	Component CISOs/ISSMs shall approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SLC support.	---
5.4.8.c	Component CISOs/ISSMs or their designated representatives shall acknowledge receipt of ISVM messages.	SI-5
5.4.8.d	Components shall report compliance with the ISVM message within the specified time. Components not able to do so shall submit documentation of a waiver request via the DHS SOC Online Portal (https://eoconline.dhs.gov).	SI-5
5.4.8.e	When vulnerability assessment responsibilities encompass more than one Component, Component CISOs/ISSMs shall coordinate with the relevant Component SOC and the DHS SOC.	RA-3, AU-2Re
5.4.8.f	The DHS SOC shall be notified before any ISVM scans are run.	RA-3, RA-5
5.4.8.g	System Owners shall report the security alert and advisory status of the information system to the AO, Component CISO/ISSM, and DHS CISO upon request and on a periodic basis.	SI-5

Core elements of vulnerability management include continuous monitoring and mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk.

5.4.9 Peer-to-Peer Technology

Policy ID	DHS Policy Statements	Relevant Controls
5.4.9.a	Peer-to-peer software technology is prohibited on any DHS information system.	CM-7, CM-10

5.5 Cryptography

Cryptography is a branch of mathematics that deals with the transformation of data. Cryptographic transformation converts ordinary text (plaintext) into coded form (ciphertext) by encryption; and ciphertext into plaintext by decryption.

5.5.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy.

Policy ID	DHS Policy Statements	Relevant Controls
5.5.1.a	Systems requiring encryption shall comply with the following methods: • Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2 • National Security Agency (NSA) Type 2 or Type 1 encryption (Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.)	IA-7, SC-13
5.5.1.b	Components shall develop and maintain encryption plans for sensitive information systems.	IA-7, SC-13
5.5.1.c	Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use.	IA-7, SC-13

5.5.2 Public Key Infrastructure

A Public Key Infrastructure (PKI) is an architected set of systems and services that provide a foundation for enabling the use of public key cryptography. This is necessary in order to implement strong security services and to allow the use of digital signatures.

The principal Components of a PKI are the public key certificates, registration authorities (RA), certification authorities (CA), directory, certificate revocation lists (CRL), and a governing certificate policy.

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.a	**DHS shall implement two distinct PKIs:** **DHS Federal PKI (FPKI):** DHS shall implement a DHS Public Key Infrastructure (PKI) that is part of the FPKI to facilitate the use of PKI within DHS, and to facilitate the interoperable use of PKI between DHS and its external mission and business partners, such as other Federal agencies; state, local and tribal governments; public and private sector entities; and U.S. citizens. **DHS Internal Use NPE PKI:** At the DHS Enterprise-level, a single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented to issue certificates to DHS NPEs to support NPE-to-NPE authentication across DHS networks, where the certificates have no external relying parties. At the DHS Component-level, a DHS Component may implement one or more DHS Internal Use Non-Person Entity (NPE) PKIs for use solely by that Component to issue certificates to that Component's NPEs to support NPE-to-NPE authentication on that Component's networks, where the certificates have no external relying parties.	SC-17
5.5.2.b	The DHS CISO shall be the DHS PKI Policy Authority (PKIPA) to provide PKI policy oversight for all DHS PKIs. **DHS FPKI:** A detailed description of DHS PKIPA roles and responsibilities is provided in the Registration Practice Statement for the DHS Principal Certification Authority. **DHS Internal Use NPE PKI:** A detailed description of DHS PKIPA roles and responsibilities is provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.5.2.c	The DHS CISO shall represent DHS on the Federal PKI Policy Authority (FPKIPA).	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.d	The DHS PKIPA shall appoint a PKI Management Authority (PKIMA) to provide management and operational oversight for all DHS PKIs. **DHS FPKI:** A detailed description of DHS PKIMA roles and responsibilities is provided in the Registration Practice Statement for the DHS Principal Certification Authority. **DHS Internal Use NPE PKI:** A detailed description of DHS PKIMA roles and responsibilities is provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.5.2.e	**DHS FPKI:** The DHS FPKI shall be governed by the U.S. Common Policy Framework certificate policy approved by the FPKIPA, and by the relevant portions of the Department of the Treasury Infrastructure (PKI) X.509 Certificate Policy approved by the Department of the Treasury Policy Management Authority (PMA). **DHS Internal Use NPE PKI:** DHS Internal Use NPE PKIs shall be governed by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines approved by the DHS PKIPA.	SC-17
5.5.2.f	**DHS FPKI:** DHS shall have a single DHS Principal CA (i.e. named DHS CA4) that has the U.S. Common Policy Root CA as its trust anchor. The DHS Principal CA shall be operated for DHS by the Department of Treasury under the Federal Shared Service Provider (SSP) program.	SC-17
5.5.2.g	**DHS FPKI:** The DHS Principal CA shall be the only DHS CA subordinated to the Treasury Root CA. Additional DHS CAs subordinate to the DHS Principal CA are not permitted. **DHS Internal Use NPE PKI:** A single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented. A DHS Component may implement one or more DHS Internal Use NPE PKIs. Each PKI shall be a hierarchical PKI with one or more levels. • For a single-level hierarchy, the PKI shall consist of a single self-signed Internal Use NPE CA. • For a two-level hierarchy, the PKI shall consist of a single self-signed Internal Use NPE Root CA at the top level, and one or more Internal Use NPE CAs that are each directly subordinated to the Internal Use	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	NPE Root CA. • Additional Internal Use NPE CAs may be directly subordinated to an existing subordinate Internal Use NPE CA, thereby adding an additional level to the hierarchy. The requirements and process for implementing a DHS Enterprise Internal Use Non-Person Entity (NPE) Root and Subordinate CAs, and for implementing a DHS Component Internal Use NPE Root and Subordinate CAs shall be specified in the NPE PKI Configuration and Operation Practices Guidelines.	
5.5.2.h	**DHS FPKI:** The DHS Principal CA shall have a trust path resolving to the U.S. Common Policy Root CA via the Treasury Root CA. Establishing direct trust relationships with any other CAs is not permitted. The U.S. Common Policy Root CA is cross-certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels. **DHS Internal Use NPE PKI:** If a DHS Internal Use NPE PKI consists of a single NPE CA, the CA shall be self-signed and function as its own trust anchor. If a DHS Internal Use NPE PKI is a multi-level hierarchical PKI, with a Root and subordinate CAs, the trust path from the subordinate CAs shall resolve to the Root CA as the PKI's trust anchor. A request to implement trust relationships between DHS Component Internal Use Non-Person Entity (NPE) PKIs, or between the DHS Enterprise Internal Use Non-Person Entity (NPE) PKI and a DHS Component Internal Use Non-Person Entity (NPE) PKI must be submitted to the DHS PKIMA for review and approved by the DHS PKIPA.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.i	**DHS FPKI:** The DHS Principal CA shall operate under an X.509 Certification Practice Statement (CPS). The CPS shall comply with the U.S. Common Policy Framework and the Treasury Certificate Policy. Since the Department of the Treasury, as the SSP for DHS, operates the DHS Principal CA, the Department of the Treasury PKI Policy Management Authority, shall approve the CPS for the DHS Principal CA. DHS shall operate two Registration Authorities for the DHS Principal CA (PC4). The DHS PCA Registration Authority (DHS PCA RA) shall be responsible for performing the life-cycle administration for non-PIV certificates, and the DHS PCA PIV Registration Authority (DHS PCI PIV RA) shall be responsible for performing the life-cycle administration of PIV certificates. The two DHS Registration Authorities for the DHS Principal CA shall operate under the Registration Practice Statement for the DHS Principal Certification Authority (RPS). The RPS shall be approved by the DHS PKIMA and the DHS PKIPA, and shall be approved for conformance to the U.S. Common Policy Framework and the Treasury Certificate Policy by the Department of the Treasury PKI Policy Management Authority. **DHS Internal Use NPE PKI:** DHS Internal Use NPE CAs shall operate under the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines, which shall be approved by the DHS PKIPA.	SC-17
5.5.2.j	**DHS FPKI:** The DHS PKIMA shall ensure that the DHS PCA Registration Authority (DHS PCA RA) operates in compliance with the RPS. The DHS PIV Card Issuer (PCI) Organization Identity Management Official (DHS OIMO) shall ensure that the DHS PCA PIV Registration Authority (DHS PCI PIV RA) operates in compliance with the RPS. **DHS Internal Use NPE PKI:** The DHS PKIMA shall ensure that every DHS Internal Use NPE CA operates in compliance with the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.k	**DHS FPKI:** The DHS Principal CA shall undergo regular PKI compliance audits as required by the U.S. Common Policy Framework. The audit findings, report, and Plans of Action and Milestones (POA&Ms) that address deficiencies found shall be provided to the DHS PKIPA and DHS PKIMA. **DHS Internal Use NPE PKI:** Every DHS Internal Use NPE CA shall undergo regular PKI compliance assessments as required by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines. The assessment report, findings, and Plans of Action and Milestones (POA&Ms) that address the deficiencies found, shall be provided to the DHS PKIPA and DHS PKIMA.	SC-17
5.5.2.l	**DHS FPKI:** The DHS Principal CA shall archive records as required by the U.S. Common Policy Framework, the Treasury Certificate Policy, and the DHS Principal CA CPS. **DHS Internal Use NPE PKI:** Every DHS Internal Use NPE CA (Root and Subordinates) shall archive records as required by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.	SC-17
5.5.2.m	**DHS FPKI:** All operational PKI facilities shall be established in accordance with U.S. Common Policy Framework physical security requirements based on the CA's assurance level and its intended use. Location/protection of the CA shall be determined by its level of assurance. Measures taken to ensure the continuity of PKI operations shall provide at least the same level of PKI Services availability as the individual and composite availability requirements of the systems and data protected by the certificates.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.n	**DHS FPKI:** The DHS Principal CA shall only issue certificates to internal DHS entities, e.g., Person Entities (PEs) such as employees, contractors, affiliates, roles, groups, and NPEs such as hardware devices, systems, and applications. External entities that require certificates to securely interact with DHS shall acquire the certificates from: (1) another Federal Agency's PKI or SSP PKI operating under the U.S. Common Policy Framework or (2) a non-Federal Agency PKI that is cross-certified with the FBCA at medium, medium Hardware, PIV-I, or high assurance level). **DHS Internal Use NPE PKI:** DHS Enterprise Internal Use Non-Person Entity (NPE) CAs shall only issue authentication certificates to DHS NPEs (i.e**.,** hardware devices and systems) when all of the following conditions apply: • There are no relying parties for the certificates external to DHS • The certificates shall only be used for authentication • The certificates are explicitly authorized to be issued by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines DHS Component Internal Use NPE CAs shall only issue authentication certificates to DHS Component NPEs (i.e**.,** hardware devices and systems) when all of the following conditions apply: • There are no relying parties for the certificates external to the DHS Component • The certificates shall only be used for authentication • The certificates are explicitly authorized to be issued by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines A DHS Enterprise Internal Use NPE Root CA may issue a CA certificate to subordinate a DHS Enterprise Internal Use NPE CA to the Root CA. A DHS Component Internal Use NPE Root CA may issue a CA certificate to subordinate a DHS Component Internal Use NPE CA for that Component to the Root CA. A DHS Enterprise Internal Use NPE CA may issue a CA certificate to subordinate a DHS Enterprise Internal Use NPE CA to itself. A DHS Component Internal Use NPE CA may issue a CA certificate to subordinate a DHS Component Internal Use NPE CA for that Component to itself.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.o	**DHS FPKI:** Only the DHS Principal CA shall issue certificates to DHS PEs, i.e., DHS employees, contractors, affiliates, roles and group entities. Types of PE certificates that may be issued include authentication, digital signature verification and encryption certificates, including certificates for DHS HSPD-12 Personal Identity Verification (PIV) Cards, code signing and content signing, as well as all other types of certificates allowed under the U.S. Common Policy. Only the DHS Principal CA shall issue certificates to DHS NPEs, i.e., hardware devices, systems and applications, when any of the following conditions apply: • There are external relying parties for the certificates • The certificates will be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive information, and • The certificates are not explicitly authorized to be issued by DHS Internal Use NPE CAs in the DHS X.509 Internal Use NPE Certificate Policy.	SC-17
5.5.2.p	**DHS FPKI:** The Treasury Root CA shall be used by Relying Parties in DHS as the trust anchor for the validation of certificates issued by the DHS Principal CA (DHS CA4). The U.S. Common Root CA shall be used by Relying Parties external to DHS as the trust anchor for the validation of certificates issued by the DHS Principal CA (DHS CA4). The U.S. Common Root CA shall also be used by Relying Parties in DHS as the trust anchor for the validation of certificates issued by CAs external to DHS.	SC-17
5.5.2.q	The use by DHS of any non-DHS PKI provider for CA or PKI services is prohibited unless approved by the DHS CISO on a case-by-case basis.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.r	**DHS FPKI:** Only certificates that are issued by the DHS Principal CA under the U.S. Common Policy Framework at medium assurance or above shall be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data. Certificates issued by test, pilot, third party, self-signed or other CAs shall not be used to protect sensitive information, or to authenticate to DHS operational systems containing sensitive information. **DHS Internal Use NPE PKI:** Certificates issued by DHS Internal Use NPE CAs, shall only be used for authentication.	SC-17
5.5.2.s	**DHS FPKI:** For an external-facing DHS web server, where the browsers used by external relying parties are unable to validate DHS Secure Socket Layer/Transport Layer Security (SSL/TLS) certificates, the use of an Extended Validation (EV) SSL/TLS certificate acquired from a major U.S. commercial certificate provider may be used, if approved by the DHS CISO on a case-by-case basis.	SC-17
5.5.2.t	Commercial applications or appliances used by DHS that require the use of PKI certificates shall obtain those certificates from the DHS Principal CA or a DHS Component Internal Use NPE CA, as appropriate. Commercial applications or appliances, that require the use of a proprietary CA implemented as an internal feature, shall not be acquired or used, unless prior concurrence by the DHS PKIMA and approval by the DHS PKIPA are obtained.	SC-17
5.5.2.u	**DHS FPKI:** Certificate trust stores contain root certificates, each of which is the trust anchor for a PKI. Certificates in trust stores are implicitly trusted by certificate validation software. Vendors' products come pre-populated with many root certificates in their trust stores, including certificates for PKIs that DHS does not want to implicitly trust. DHS Components shall manage the content of installed product's trust stores, including: • Leveraging automated management, such as with Microsoft Group Policy Objects (GPOs) • Removing all certificates that have passed their expiration date • Removing all certificates that are no longer trusted • Removing all certificates that are no longer required	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.v	**DHS FPKI:** Commercial products used by DHS and applications developed by DHS that enable the use of PKI shall at a minimum support the following cryptographic algorithms and associated key sizes: • SHA 1 and SHA 256 • RSA 1024 and 2048 • AES 128 and 256 Whenever possible, they should also support use of the following algorithms and associated key sizes, to ensure future interoperability across the Federal PKI and PKIs cross-certified with the Federal Bridge Certification Authority. • SHA 384 and 512 • RSA 3072 • Elliptic Curve 224, 256, and 384 • ECDSA 224 and 256 *(Note: Older algorithms and smaller key sizes (e.g., SHA 1 and RSA 1024) should continue to be supported since they may be required to validate digital signatures executed in the past and to decrypt objects encrypted in the past using the older algorithms and key sizes.)*	SC-17

5.5.3 Public Key/Private Key

A public key certificate is used to obtain subscribers’ public keys in a trusted manner. Once a certificate is obtained, the public key can be used:

- To encrypt data for that subscriber so that only that subscriber can decrypt it
- To verify that digitally signed data was signed by that subscriber, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.a	**DHS FPKI:** Any key pair and associated certificate issued to a human subscriber to support digital signature use, shall not be used to support any other use.	SC-12
5.5.3.b	**DHS FPKI:** A single public/private key pair and its associated certificate issued to an NPE may be used for signing (including authentication), key management (for encryption), or both. Device certificates shall not assert non-repudiation.	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.c	**DHS FPKI:** An authorized human sponsor shall represent each role, group, code-signer, system, application and device subscriber when the subscriber applies for one or more certificates from a DHS CA.	SC-12
5.5.3.d	**DHS FPKI:** An authorized DHS employee shall sponsor DHS contractors or other affiliates who apply for one or more certificates from a DHS CA.	SC-12
5.5.3.e	**DHS FPKI:** A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, role, group, code signer, system, application, or device to receive one or more certificates.	SC-12
5.5.3.f	**DHS FPKI:** A mechanism shall be provided for each DHS CA to enable PKI registrars to determine and verify the identity of the authorized human sponsor for each DHS contractor, affiliate, role, group, code signer, system, application, or device.	SC-12
5.5.3.g	**DHS FPKI:** Human subscribers shall not share their private keys and shall be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.	SC-12
5.5.3.h	**DHS FPKI:** Sponsors for non-human subscribers (systems, application and devices,) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Device Sponsor Acknowledgement of Responsibilities" as a pre-condition for sponsoring non-human subscribers.	SC-12
5.5.3.i	**DHS FPKI:** Subscriber private keys shall not be used by more than one entity, with the following exceptions: • Authorized members of a Group Subscriber, may use the Group's private keys. • Multiple systems or devices in a high availability configuration may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared.	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.j	**DHS FPKI:** Every human subscriber shall read, understand, and sign a "DHS PKI Human Subscriber Acknowledgement of Responsibilities" as a pre-condition for receiving certificates from a DHS CA. Signed PKI Human Subscriber Agreements shall be maintained by the DHS PKI Registrar.	SC-12

5.6 Malware Protection

Policy ID	DHS Policy Statements	Relevant Controls
5.6.a	Component CISOs/ISSMs shall establish and enforce Component-level malware protection control policies.	SI-3
5.6.b	Components shall implement a defense-in-depth strategy that: - Installs anti-malware software on desktops and servers - Configures anti-malware software on desktops and servers to check all files, downloads, and email - Installs updates to anti-malware software and signature files on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update - Installs security patches to desktops and servers in a timely and expeditious manner	SI-3
5.6.c	System Owners shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	AC-20, SI-3

5.7 Product Assurance

Policy ID	DHS Policy Statements	Relevant Controls
5.7.a	Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated commercial-off-the-shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.	---
5.7.b	*Strong preference* shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following: - The National Institute of Standards and Technology (NIST) FIPS validation program - The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program - The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	---
5.7.c	The evaluation and validation of COTS IA and IA-enabled products shall be conducted by authorized commercial laboratories or by NIST.	---
5.7.d	Components shall use only cryptographic modules that meet the requirements set forth in Section 5.5, Cryptography.	---
5.7.e	Transaction-based systems (e.g., database management systems and transaction processing systems) shall implement transaction rollback and transaction journaling, or technical equivalents.	CP-10
5.7.f	For systems with moderate or high impact for the integrity security objective, Components shall perform a risk-based analysis to determine any data inputs that are critical to the system mission or the correct handling of the security controls, which should be checked for accuracy, completeness, and validity of the information as close to the input point (e.g., user interface) as possible. Inputs that go through interpreters should be prescreened.	SI-10
5.7.g	For systems with moderate or high impact for the integrity security objective, the information system shall check the validity of these Component-defined information inputs.	SI-10

Policy ID	DHS Policy Statements	Relevant Controls
5.7.h	For systems with moderate or high impact for any of the FIPS 199 security objectives, Components shall perform a risk-based analysis to determine what error conditions should be identified and how expeditiously they should be handled.	SI-11
5.7.i	For systems with moderate or high impact for any of the FIPS 199 security objectives, the information system shall generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. Error messages shall be revealed only to authorized personnel.	SI-11

5.8 Supply Chain

Supply chain threats shall be considered during every sensitive system acquisition and throughout those systems' life cycle.

Policy ID	DHS Policy Statements	Relevant Controls
5.8.a	Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-161 controls as tailored specifically to the security objective at the determined impact level.	SA-12
5.8.b	Components shall implement NIST SP 800-161security controls, using the FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	SA-12

5.8.1 Business Impact

DHS depends on numerous external supply chains for the hardware, software, and services needed in order to accomplish its missions effectively. Many of these supply chains are independent of one-another and come with their own set of risks. All program risk owners need to make risk management decisions on how best to manage these risks. It is often no longer enough for acquisition staff to perform due diligence at the beginning of an acquisition. Effective Supply Chain Risk Management (SCRM) requires the analysis of the Business Impact Assessment (BIA) to determine if supply chain threats represent unacceptable business or mission risk and the optimal countermeasures.

Policy ID	DHS Policy Statements	Relevant Controls
5.8.1.a	A Business Impact Assessment (BIA) shall be used to determine the level of risk introduced to the system by the supply chain and whether supply chain threats introduce sufficient risk to require the implementation of countermeasures.	SA-12

5.8.2 Supply Chain Risk Management Plans

For the development of SCRM plans, no prescriptive set of mitigations can be provided; rather, it is necessary for organizations across DHS to consider the range of countermeasures which could be selected. It will be up to individual programs to establish the appropriate supply chain risk reduction strategies and determine the best way to implement them.

Policy ID	DHS Policy Statements	Relevant Controls
5.8.2.a	DHS Components shall develop, document, and disseminate requirements for all programs under their control to develop a plan to address supply chain risk.	SA-1 SA-12
5.8.2.b	DHS Components shall assess supply chain threats for risks associated with all hardware, software, and services acquired or projected to be acquired with the goal of mitigating those risks to the greatest extent possible.	SA-12

6.0 DOCUMENT CHANGE REQUESTS

Changes to *DHS Sensitive Systems Policy Directive 4300A* and to the *DHS 4300A Sensitive Systems Handbook* may be requested in accordance with Section 1.9, Changes to Policy.

7.0 QUESTIONS AND COMMENTS

For clarification of DHS information security policies or procedures, contact the DHS Director for Information Systems Security Policy at infosecpolicy@hq.dhs.gov.

APPENDIX A ACRONYMS AND ABBREVIATIONS

ACRONYM	MEANING
3DES	Triple Data Encryption Standard
3PAO	Third Party Assessors
AES	Advanced Encryption Standards
AIS	Automated Information System
A-Number	Alien Registration Number
AO	Authorizing Official
ARB	Acquisition Review Board
ASCII	American Standard Code for Information Interchange
ATO	Authority to Operate
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
CA	Certification Authority
CAC	Common Access Card
CBP	Customs and Border Protection
CCB	Change Control Board
CCE	Common Configuration Enumeration
CD	Compact Disc
CFO	Chief Financial Officer
CI	Counterintelligence
CIO	Chief Information Officer
CISID	Chief, Internal Security and Investigations Division
CISID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMA	Computer Matching Agreements

ACRONYM	MEANING
CMG	Core Management Group
CMP	Configuration Management Plan
CNSS	Committee on National Security Systems
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan Continuity of Operations Planning
COTS	Commercial-off-the-shelf
CP	Contingency Plan Contingency Planning
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EMSG	Email Security Gateway
EO	Executive Order
EOC	Enterprise Operations Center 2,
ESSA	Enterprise System Security Agreement
ESSWG	Enterprise Services Security Working Group

ACRONYM	MEANING
EV	Extended Validation
FAM	Foreign Affairs Manual
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credentialing, and Access Management
FIPS	Federal Information Processing Standard
FIPPS	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act of 2014
FLETC	Federal Law Enforcement Training Center
FNVMS	Foreign National Vetting Management System
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPKI	Federal Public Key Infrastructure
FPKI PA	Federal PKI Policy Authority
FTP	File Transfer Protocol
FYHSP	Future Years Homeland Security Program
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HQ	Headquarters
HSAR	Homeland Security Acquisition Regulations
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation and Air Conditioning
I&A	Intelligence and Analysis
IA	Identification and Authentication

ACRONYM	MEANING
	Information Assurance
IACS	Information Assurance Compliance System
IATO	Interim Authority to Operate
ICAM	Identity, Credentialing, and Access Management
ICCB	Infrastructure Change Control Board
ICE	Immigration and Customs Enforcement
IDS	Intrusion Detection System
IOC	Initial Operating Capability
IPS	Intrusion Prevention System
IPT	Integrated Project Team
IR	Infrared
IRB	Investment Review Board
ISA	Interconnection Security Agreement
ISMS	Integrated Security Management System
ISO	Information Security Office
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVM	Information System Vulnerability Management
IT	Information Technology
JAB	Joint Authorization Board
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LE	Law Enforcement
LMR	Land Mobile Radio
MA	Major Application
MBI	Moderate Risk Background Investigation
MD	Management Directive
MMS	Multimedia Messaging Service
NARA	National Archives and Records Administration

ACRONYM	MEANING
NCCIC	National Cybersecurity and Communications Information Center
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPPD	National Protection and Programs Directorate
NPE	Non-person Entity
NSA	National Security Agency
NSS	National Security System(s)
NTP	Network Time Protocol
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
OCSP	Online Certificate Status Protocol
OID	Object identifier
OIG	Office of Inspector General
OIMO	Organization Identity Management Official
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
ORMB	Operational Risk Management Board
OTAR	Over-The-Air-Rekeying
PA	Policy Authority
PAdES	PDF Advanced Electronic Signatures
P-ATO	Provisional Authority to Operate
PBX	Private Branch Exchange
PCI	PIV Card Issuer
PCS	Personal Communications Services
PDVAL	Path Development and Validation
PEP	Policy Enforcement Point

Acronym	Meaning
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identity Number
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI MA	PKI Management Authority
PM	Program Manager
PMA	Policy Management Authority
PMO	Program Management Office
PNS	Protected Network Services
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
~~RMS~~	~~Risk Management System~~ Term superseded by IACS
RMF	Risk Management Framework
RPS	Principal Certification Authority
S&T	Science and Technology [Component of DHS]
SA	Security Architecture
SAISO	Senior Agency Information Security Officer
SAN	Subject Alternative Name

ACRONYM	MEANING
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SELC	Systems Engineering Life Cycle
SEN	Security Event Notification
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SOA	Service Oriented Architecture
SOC	Security Operations Center
SOC CONOPS	Security Operations Center Concept of Operations
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication Security Plan
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
Stat.	Statute (refers to a law found in *U.S. Statutes at Large*)
STE	Secure Terminal Equipment
~~TAF~~	~~Trusted Agent FISMA~~ Term superseded by IACS
TFPAP	Trust Framework Provider Adoption Process
TIC	Trusted Internet Connections
TLS	Transport Layer Security
TOS	Terms of Service
TRAL	Trigger Accountability Log
TRM	Technical Reference Model

ACRONYM	MEANING
TS	Top Secret
TS/SCI	Top Secret, Sensitive Compartmented Information
TSA	Transportation Security Administration
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USGCB	U.S. Government Configuration Baseline
USSS	United States Secret Service
VAT	Vulnerability Assessment Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XML	Extended Markup Language

APPENDIX B GLOSSARY

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms* and the *National Information Assurance (IA) Glossary*.

TERM	MEANING
Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the Risk Executive after adequate security has been provided.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [OMB Circular A-130, Appendix III]
Annual Assessment	Department of Homeland Security (DHS) activity for meeting the annual Federal Information Security Modernization Act of 2014 (FISMA) self-assessment requirement.
Authorization Package	The documents submitted to the AO for the Authorization Decision. An Authorization Package consists of: • Security Plan • Security Assessment (SPR) Plan • Security Assessment Report (SAR) • Signed Accreditation Decision Letter/ATO • Contingency Plan (CP) • Contingency Plan Test (CPT)
Authorizing Official (AO)	An official within a Federal Government agency empowered to grant approval for a system to operate.
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certificate Authority (CA)	A trusted third party that issues certificates and verifies the identity of the holder of the digital certificate.
Chief Information Officer (CIO)	The executive within a Federal Government agency responsible for its information systems.

TERM	MEANING
Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.
Component	A DHS *Component* is any organization which reports directly to the Office of the Secretary (including the Secretary, the Deputy Secretary, the Chief of Staff's, Counselors, and staff, when approved as such by the Secretary), including both Operational Components and Support Components (also known as Headquarters Components). [Source *DHS Lexicon* and DHS Management Directive 112-01]
Computer Security Incident Response Center (CSIRC)	DHS organization that responds to computer security incidents.
Designated Approval Authority (DAA)	Obsolete term; see Authorizing Official (AO).
Digital Signature	Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.
Electronic Signature	The process of applying any mark in electronic form with the intent to sign a data object. See also digital signature.
For Official Use Only (FOUO)	The marking instruction or caveat "For Official Use Only" will be used within the DHS community to identify sensitive but unclassifed information that is not otherwise specifically described and governed by statute or regulation. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).
General Support System (GSS)	A *general support system* (GSS) is an interconnected set of information resources that share common functionality and are under the same direct management control. [expanded definition in the Section 1.4, "Definitions"]
Information and Communications Technology (ICT)	Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information. Source: NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*

TERM	MEANING
ICT Supply Chain	The organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers. Source: National Defense Industry Association (NDIA), *Engineering for System Assurance,* September 2008
Information Security Vulnerability Management (ISVM)	A DHS system that provides notification of newly discovered vulnerabilities, and tracks the status of vulnerability resolution.
Information System	Any information technology that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. Information systems include general support systems and major applications (MA).
Information System Security Officer (ISSO)	A Government employee or contractor who implements and/or monitors security for a particular system.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. [Source: Clinger-Cohen Actof 1996 (Public Law 104-106), Division E]
Major Application (MA)	An automated information system (AIS) that requires special attention to security due to the risk and magnitude of harm that can result from the loss, misuse, or unauthorized access to or modification of the information in the application. [Source: OMB Circular A-130] An MA is a discrete application, whereas a GSS may support multiple applications.
Management Controls	The security controls for an information system that focus on the management of risk and the management of information system security.
Operational Controls	The security controls for an information system that are primarily implemented and executed by people (as opposed to being executed by systems).
Operational Risk	The risk contained in a system under operational status. It is the risk that an AO accepts when granting an ATO.

TERM	MEANING
Personally Identifiable Information (PII)	Any information information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. [see also Sensitive Personally Identifiable Information]
Pilot	A test system in the production environment that may contain operational data and may be used to support DHS operations, typically in a limited way.
Policy Enforcement Point (PEP)	A firewall or similar device that can be used to restrict information flow.
Policy Statement	A high-level rule for guiding actions intended to achieve security objectives.
Privacy Sensitive System	Any system that collects, uses, disseminates, or maintains PII or sensitive PII.
Production	The applications and systems that DHS end users access and use operationally to execute business transactions.
Privileged Network User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions for purposes including but not limited to network system administration, security policy and procedure management, and system maintenance and controls.
Prototype	A test system in a test environment that must not contain operational data and must not be used to support DHS operations.
Remote Access	Access to a DHS information system by a user (or an information system) communicating through an external, non-DHS-controlled network (e.g., the Internet).
Residual Risk	The risk remaining after security controls have been applied.
Risk Executive (RE)	An individual who ensures that risks are managed consistently across the organization. An RE can be at the Departmental or Component level.

TERM	MEANING
Security Assessment Plan	The security assessment plan and privacy assessment plan provide the objectives for the security and privacy control assessments, respectively, and a detailed roadmap of how to conduct such assessments. These plans may be developed as one integrated plan or as distinct plans, depending upon organizational needs. [per NIST SP 800-53A]
Security Control	A particular safeguard or countermeasure to protect the confidentiality, integrity, and availability of a system and its information.
Security Control Assessor	A senior management official who certifies the results of the security control assessment. He or she must be a Federal Government employee.
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security Operations Center (SOC)	The DHS SOC coordinates security operations for the DHS enterprise. Each Component also has a SOC that coordinates Component security operations.
Security Requirement	A formal statement of action or process applied to an information system and its environment in order to provide protection and attain security objectives. Security requirements for any given system are contained in its Security Plan.
Senior Agency Information Security Official (SAISO)	The point of contact within a Federal Government agency responsible for its information system security.
Sensitive But Unclassified	Obsolete designation; see Sensitive Information. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).

TERM	MEANING
Sensitive Information	Any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. Note: The term *sensitive information* as well as others such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) will no longer be used upon implementation of 32 CFR 2002, which will require use of the term Controlled Unclassified Information (CUI).
Sensitive Personally Identifiable Information (SPII)	*Sensitive PII* is Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. [see also Personally Identifiable Information]
Significant Incident	A computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate leadership notification.
Spam	Emails containing unwanted commercial solicitation, fraudulent schemes, and possibly malicious logic.
Strong Authentication	A method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have). Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. [See the discussion of Level 4 assurance in NIST SP 800-63-2, "Electronic Authentication Guideline," (August 2013)]
Supply Chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Source: CNSSI 4009
Supply Chain Risk Management	A decision making process, usually supported by imperfect or incomplete information, undertaken for the purpose of prioritizing actions related to procuring ICT in support of the mission. Source: DHS SCRM PMO

TERM	MEANING
System	A discrete set of information system assets contained within the authorization boundary.
System Owner	The agency official responsible for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.
Technical Controls	The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in system hardware, software, or firmware.
Two-Factor Authentication	The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication: • *Something you know* (for example, a password or Personal Identification Number (PIN) • *Something you have* (for example, an ID badge or a cryptographic key) • *Something you are* (for example, a fingerprint or other biometric data) The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor.” A requirement for two of the three factors listed above constitutes two factor authentication.
Unclassified Information	Information that has not been determined to be classified pursuant to Executive Order 13526, as amended.
USB Device	A device that can be connected to a computer via a USB port.
USB Drive	A memory device small enough to fit into a pocket that connects to a computer via a USB port.

TERM	MEANING
Visitor	A guest or temporary employee who presents themselves or is presented by a sponsor, for entry for less than 6 months to a secured facility that is not their primary work location. [Source: DHS Lexicon] The visitor is placed in one of two categorizes, either ***escort required*** or ***no escort required***. ***Escort required*** visitors are escorted at all times. ***No escort required*** visitors are granted limited general access to the facility without an escort. Escort procedures for classified areas are indicated in Management Directive 11051 "SCIF Escort Procedures." [Source: DHS Lexicon]
Vulnerability Scanning	An automated scan for potential security vulnerabilities.
Waiver	Temporary dispensation of a policy requirement, granted to a Component to operate a system while working toward compliance.

APPENDIX C REFERENCES

The DHS information security program and organization are based upon public laws, executive orders, national policy, external guidance, and internal DHS guidance.

Public Laws and U.S. Code

- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, DC, July 14, 1987
- Computer Security Act of 1987, as amended, codified at 40 U.S.C. 759 , Public Law 100-235
- *Clinger-Cohen Act* of 1996, Public Law 104-106
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
- E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 44 U.S.C. 101
- Freedom of Information Act of 2002, as amended, 5 U.S.C 552, Public Law 93-579
- Intelligence Reform and Terrorism Prevention Act of 2004, 118 Stat. 363
- Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283, 128 Stat 3087
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, "Standards of Ethical Conduct for Employees of the Executive Branch"

Executive Orders

- Executive Order 13526, "Classified National Security Information," December 29, 2009
- Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004

Office of Management and Budget Directives

- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources, Transmittal Letter No. 4," 2010
- OMB Bulletin 06-03, "Audit Requirements for Federal Financial Statements," August 23, 2203
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information," May 22, 2006
- OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," June 23, 2006
- OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007

- OMB Memorandum M-09-02, “Information Technology Management Structure and Governance Framework,” October 21, 2008
- OMB Memorandum 12-20, “FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,” September 27, 2012
- OMB Memorandum 10-28, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),” July 6, 2010
- OMB Memorandum 11-06, “WikiLeaks - Mishandling of Classified Information,” November 28, 2010

Other External Standards and Guidance

- Intelligence Community Directive (ICD) 503 “”Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation,” September 15, 2008
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), including:
  - NIST FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
  - NIST FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
- NIST Information Technology Security Special Publications (SP) 800 series, including:
  - NIST SP 800-16, “Information Technology Security Training Requirements: A Role- and Performance-Based Model,” April 1998
  - NIST SP 800-34, Rev 1, “Contingency Planning Guide for Information Technology Systems,” May, 1010
  - NIST SP 800-37, Rev 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,” February 2010
  - NIST SP 800-39, “Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View,” March 2011
  - NIST SP 800-50, “Building an Information Technology Security Awareness and Training Program,” October 2003
  - NIST SP 800-52, Rev 1, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,” April 2014
  - NIST SP 800-53, Rev 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” April 2013, with updates as of January 22, 2015
  - NIST SP 800-53A, Rev 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” December 2014

  - NIST SP 800-60, Rev 1, "Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices," August 2008
  - NIST SP 800-63-2, "Electronic Authentication Guideline," August 2013
  - NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process (CPIC)," January 2005
  - NIST SP 800-88 Rev 1, "Guidelines for Media Sanitization," December 2014
  - NIST SP 800-92, "Guide to Computer Security Log Management," September 2006
  - NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)," February 2007
  - NIST SP 800-95, "Guide to Secure Web Services," August 2007
  - NIST SP 800-100, "Information Security Handbook: A Guide for Manager," October 2006 (Including updates as of 03-07-2007)
  - NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," November 2008
  - NIST SP 800-118, Draft, "Guide to Enterprise Password Management (Draft)," April 21, 2009
  - NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010
  - NIST SP 800-123, "Guide to General Server Security," July 2008
  - NIST SP 800-124, Rev 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," June 2013
  - NIST SP 800-128, "Guide for Security-Focused CM of Information Systems," August 2011
  - NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011
  - NIST SP 800-160, "DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems," May 2014
  - NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," April 2015
- NIST IR 7298 Rev 2, "Glossary of Key Information Security Terms," May 2013
- CNSS Instruction No. 1001, "National Instruction on Classified Information Spillage," February 2008
- CNSS Instruction No. 4009 (Revised), "National Information Assurance Glossary," April 2015

Internal Guidance

- Department of Homeland Security Acquisition Regulation (HSAR)
- DHS Management Directives (MD), especially:
  - MD 140-01, “Information Technology Security Program,” July 6, 2014
  - MD 11042.1, “Safeguarding Sensitive but Unclassified (For Official Use Only) Information,” January 6, 2005
  - MD 102-01a, “Acquisition Management Directive Rev01,” January 20, 2010
  - MD 102-01b, “Acquisition Management Directive Rev02,” February 21, 2013
  - MD 1030, “Corrective Action Plans,” May 15, 2006
  - MD 4400.1, “DHS Web (Internet, Intranet, and Extranet Information) and Information Systems,” March 1, 2003
  - MD 4500.1, “DHS Email Usage,” March 1, 2003
  - MD 4600.1,” Personal Use of Government Office Equipment,” April 14, 2003
  - MD 4900,” Individual Use and Operation of DHS Information Systems/Computers

APPENDIX D DOCUMENT CHANGE HISTORY

Version	Date	Description
0.1	December 13, 2002	Draft Baseline Release
0.2	December 30, 2002	Revised Draft
0.5	January 27, 2003	Day One Interim Policy
1.0	June 1, 2003	Department Policy
1.1	December 3, 2003	Updated Department Policy
2.0	March 31, 2004	Content Update
2.1	July 26, 2004	Content Update
2.2	February 28, 2005	Content Update
2.3	March 7, 2005	Content Update
3.0	March 31, 2005	Includes updates to PKI, Wireless Communications, and Media Sanitization (now Media Reuse and Disposition) sections
3.1	July 29, 2005	New policies: 3.1b,e,f, 3.1g. 4.1.5b, 4.8.4a. Modified policies: 3.7b, c, 3.9b,g, 3.10a, 4.3.1b, 4.8.2a, 4.8.5e, 5.1.1b, 5.2.2a, 5.3a, c, 5.4.1a, 5.4.5d, 5.4.8c, 5.5.1a, 5.7d. Policies relating to media disposal incorporated into policies within Media Reuse and Disposition section. Deleted policy regarding use of automated DHS tool for conducting vulnerability assessments.
3.2	October 1, 2005	Modified policies 3.8b, 4.8.1a, 5.2.1a&b, 5.2.2a, and 5.4.3c; combined (with modifications) policies 4.1e and 4.1f; modified Section 1.5
3.3	December 30, 2005	New policies: policies 3.9a–d; 3.11.1b; 4.3.1a; 4.6c; 5.4.3d&e. Modified policies: policies 3.9i&j; 4.3.2a; 4.6a, b; 4.6.1e; 4.6.2j; 4.6.2.1a; 4.6.3e; 5.4.3c; 5.5.2k. Modified sections: 2.5, 2.7, 2.9, 2.11, 3.9, 5.5.2.
4.0	June 1, 2006	New policies: 3.5.3.c&g, 4.6.2.3.c, 5.1.c, 5.2.c, 5.4.1.a. Modified policies: 3.5.1.c, 3.5.3.d–f, 3.7.a&b, 3.9.a&b, d, 4.1.4.b&c, 4.2.1.a, 4.3.1.a, 4.6.c, 4.6.1.a, 4.6.2.f, 4.10.3.a, 5.2.1.b, 5.3.a&b, 5.4.1.b, 5.4.3.c, 5.4.5.d. Modified section: Section 2.9.
4.1	September 8, 2006	New policies: 3.14.1.a–c; 3.14.3.a–c; 4.10.1.c; 5.3.d&e; 5.4.1.c–e. Modified policies: 3.9.b; 4.6.2.d; 4.8.2.a–c; 4.10.1.b; 5.1.c; 5.3.c; 5.4.1.b. New sections: 3.14, 3.14.1, 3.14.3. Modified sections: 2.9, 4.8.2.
4.2	September 29, 2006	New policies: 4.6.4.a–f. Modified policies: 4.3.3.a–c. New section: 4.6.4.

Version	Date	Description
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f, &g, 4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.12, 4.1 and subsections, 4.6.1–4.6.4, 4.9, 5.2.1. Renumbered sections: 4.1.2–4.1.6, 4.9, 4.10, 4.11, 4.12.
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, *Sensitive But Unclassified* to *For Official Use Only*
5.2	June 1, 2007	Updates Sections 2.7, 2.9, 2.12, 3.3, 3.5.1, 3.5.3, 3.6, 3.8, 3.9, 3.10, 3.14, 3.15, 4.1.5, 4.1.6, 4.10, 4.12, 5.1.1, 5.2, 5.3, 5.4.1, 5.4.3, 5.4.4, 5.4.8, 5.5.1, 5.7
5.3	August 3, 2007	Revised policy in Sections 3.5.1 and 5.5.1, and removed Section 3.5.2. Removed Sections 3.11.2 and 3.11.4
5.4	October 1, 2007	Content update, incorporation of change requests
5.5	September 30, 2007	**Section 1.0:** 1.1 – Added text regarding policy implementation and DHS security compliance tool updates. 1.2 – Removed two references from list; deleted "various" from citation of standards. **Section 2.0:** 2.0 – Insert the following after the first sentence in the second paragraph: “Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions.” 2.3 – Removed parentheses from "in writing." **Section 3.0:** 3.9 – Inserted new policy element “l” regarding CISO concurrence for accreditation. 3.15 – Added text regarding Component CFOs and ISSMs. **Section 4.0:** 4.1.1 – Capitalized “Background,” and added "(BI)." 4.3.1 – Two new elements were added to the policy table. 4.7 – Inserted "where required or appropriate" before the sentence. 4.8.3 – Title changed to “Personally Owned Equipment and Software (not owned by or contracted for by the Government).” 4.8.6 – Included new section regarding wireless settings for peripheral equipment. **Section 5.0:** 5.1c – Changed inactive accounts to “disable user identifiers after forty-five (45) days of inactivity.” 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to “Automatic Session Termination.”
6.0	May 14, 2008	**Global change** “Shoulds” changed to “shalls” throughout the document. Replaced certain instances of “will” with “shall” throughout document to indicate compliance is required. Various changes were made throughout the document to ensure that the 4300A Policy and Handbook align with the 4300B Policy and Handbook. “ISSM” changed to “CISO/ISSM” throughout the document.

Version	Date	Description
		"CPO" changed to "Chief Privacy Officer" throughout the document. "IT Security Program" changed to "Information Security Program" throughout the document." "System Development Life Cycle" changed to "System Life Cycle" and "SDLC" changed to "SLC" throughout the document. **Title Page** Title page of 4300A Policy - Language on the Title Page was reworded. "This is the implementation of DHS Management Directive 4300.1." **Section 1.0** 1.1 – Updated to clarify 90 day period in which to implement new policy elements. 1.2 – Added OMB, NIST, and CNSS references. 1.4 – Added reference and link to Privacy Incident Handling Guidance and the Privacy Compliance documentation. 1.4.2 – Added definition of National Intelligence Information. 1.4.3 – Inserted definition of National Security Information to align with 4300B Policy. 1.4.8.1 – Definition of General Support System was updated. 1.4.8.2 – Definition of Major Application was updated. 1.4.10 – Section was renamed "Trust Zone." 1.4.16 – Inserted new definition for FISMA. 1.5 – Language was updated to increase clarity for financial system owners for waivers and exceptions. **Section 2.0** 2.3 – Added a new responsibility for DHS Chief Information Officer (CIO). 2.4 – Added a new responsibility for Component CIOs. 2.5 - Chief Information Security Officer (CISO) renamed DHS Chief Information Security Officer (CISO). Updated to include privacy-related responsibilities. 2.6 – Added a new section in Roles and Responsibilities called "Component CISO." 2.7 – Updated Component ISSM Role and Responsibilities. 2.8 – Changed name of the section from "Office of the Chief Privacy Officer (CPO)" to "The Chief Privacy Officer". Updated to include privacy-related responsibilities. 2.9 – Added a new role for DHS CSO. 2.10 – Updated to include privacy-related responsibilities. 2.11 - Added privacy-related responsibilities.

Version	Date	Description
		2.12 – Added a new section, “OneNet Steward.” 2.13 – Added a new section, “DHS Security Operations Center (DHS SOC) and Computer Security Incident Response Center (CSIRC).” 2.14 – Added a new section, “Homeland Secure Data Network (HSDN) Security Operations Center (SOC).” 2.16 – Added a new section, “Component-level SOC.” 2.18 – Updated to include privacy-related responsibilities. 2.19 – Last sentence of first paragraph has been updated to say: “ISSO Duties shall not be assigned as a collateral duty. Any collateral duties shall not interfere with their ISSO duties.” 2.20 – Updated to include privacy-related responsibilities. **Section 3.0** 3.9 – Added C&A information for unclassified, collateral classified and SCI systems. Also, prior to DHS Policy table, included sentence regarding C&A. 3.9.b – Language updated to clarify that a minimum impact level of moderate is required for confidentiality for CFO designated financial systems. 3.9.h – New guidance is provided to clarify short term ATO authority. 3.11.1 – Added new section discussing the CISO Board. 3.11.3 – Removed DHS Wireless Security Working Group. 3.14.1 – Added new text defining PII and sensitive PII. At the end of bullet #4, added definition of computer-readable data extracts. Updated 3.14.1.a and 3.14.1.b based on input from the Privacy Office. Added sentence “DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. 3.14.2 - Added new section called "Privacy Threshold Analyses." 3.14.3 - Updated Privacy Impact Assessment Responsibilities table. 3.14.4 - Added new section called "System of Record Notices." **Section 4.0** 4.1.5.c – Updated to address training requirements. 4.1.5.g – Deleted “Training plans shall include awareness of internal threats and basic IT security practices.” 4.1.5.h (now 4.1.5.g) – Updated to include the following sentence: “Components shall account for Contingency Plan Training, and Incident Response Training conducted for Moderate and High IT Systems.” 4.3.1.d – FIPS 140-2 compliance language was updated. 4.8.1.a and 4.8.1.c – Language has been updated to provide clarification of timeout values.

Version	Date	Description
		4.8.2.a – FIPS 140-2 compliance language was updated. 4.8.2.b – Added a new policy element regarding powering down laptops when not in use. 4.9 – Section was renamed “Department Information Security Operations.” 4.9, 4.9.1, 4.9.2 – Updated policy elements to support Department security operations capabilities, based on the SOC CONOPS. 4.9.2.b – Updated to say “Components shall obtain guidance from the DHS SOC before contacting local law enforcement except where there is risk to life, limb, or destruction of property.” 4.12.a – Added policy element to align with Handbook. **Section 5.0** 5.2.1.a, 5.2.1.b, and 5.2.1.c – Language has been updated to provide clarification of timeout values. 5.2.2 Introductory language, 5.2.2.a, 5.2.2.b, and 5.2.2.c – Language and policy updated to clarify the meaning of a session termination. 5.3.f - Updated to clarify responsibilities of the System Owner regarding computer-readable data extracts. 5.4.1.d – Added sentence “DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.” 5.4.3.a through i – New guidance is provided regarding the preparation of ISAs for interconnections to the DHS OneNetwork. 5.4.3.g – Replaced “interconnect service agreements” with “interconnection security agreements.” 5.4.4.f - New guidance is provided regarding internal firewalls. 5.4.5.f – New guidance is provided regarding the use of the RDP protocol. 5.4.6 – Added text “NOTE: Due to many attacks that are HTML-based, please note that DHS will be following the lead of the DoD and moving to text based email.” 5.4.8.a – Language updated to reflect that annual vulnerability assessments should be conducted. 5.4.8.f – Policy updated to clarify automated system scanning. 5.5.1.c – Updated element to specify usage of cryptographic modules that “are FIPS 197 compliant and have received FIPS 140-2 validation.” 5.5.2.f – Policy updated to clarify hosting of DHS Root CA.
6.1	September 23, 2008	**Global Changes** Replaced all instances of “CISO/ISSM” with “Component CISO/ISSM.” Replaced all DHS-related instances of “agency/agency-wide” with “Department/Department-wide.” Replaced all instances of “24x7” with “continuous” or “continuously,” as

Version	Date	Description
		appropriate. Replaced all instances of “IT security” with “information security.” Various minor editorial and grammatical changes were made throughout the document. **Section 1.0** 1.2 – Added reference to E-Government Act of 2002, January 7, 2003. 1.4 – Replaced “National InfoSec Glossary” with “National Information Assurance (IA) Glossary.” 1.4.5 – Replaced third sentence with “System vulnerability information about a financial system shall be considered Sensitive Financial Information.” 1.5.2 – Added text regarding acceptance of resulting risk by the Component CFO for financial systems. 1.5.3 – Corrected the title and location of Attachment B. Added text regarding PTA requirements. **Section 2.0** 2.1 – Updated to clarify Secretary of Homeland Security responsibilities. 2.2 – Updated to clarify Undersecretaries and Heads of DHS Components responsibilities. 2.3 – Updated to clarify DHS CIO responsibilities. 2.4 – Updated to clarify Component CIO responsibilities. 2.5 – Updated to clarify DHS CISO responsibilities. 2.6 – Updated to clarify Component CISO responsibilities. 2.8 – Moved “The Chief Privacy Officer” section to 2.9. 2.11 – Updated to clarify Program Managers’ responsibilities. 2.14 – Updated to clarify HSDN SOC responsibilities. Updated HSDN SOC unclassified email address. 2.19 – Updated to clarify ISSO responsibilities and the assignment of ISSO duties as a collateral duty. 2.20 – Updated to clarify System Owners’ responsibilities. 2.23.2 – Updated to clarify DHS CIO responsibilities for financial systems. **Section 3.0** 3.1.e – Replaced “FISMA and OMB requirements” with “FISMA, OMB, and other Federal requirements.” 3.1.h – Replaced “maintain a waiver” with “maintain a waiver or exception.” 3.14.1 – Included text regarding the type of encryption needed for laptops. 3.14.3 – Included text stating that the PTA determines whether a PIA is conducted.

Version	Date	Description
		3.14.4 – Moved first sentence of second paragraph to be the first sentence of the first paragraph. Included “that are a system of record” after “IT Systems” in the second sentence of the first paragraph. **Section 4.0** 4.3.1.a – Included “locked tape device” in media protection. 4.3.1.d – Updated to clarify that AES 256-bit encryption is mandatory. 4.8.2.a – Updated to clarify that AES 256-bit encryption is mandatory. 4.8.3.c – Included new policy element regarding use of seized IT equipment. 4.8.4.f – Included new policy element regarding management and maintenance of system libraries. 4.8.5.b – Policy updated to clarify limited personal use of DHS email and Internet resources. 4.9 – First paragraph updated to clarify DHS SOC and HSDN SOC responsibilities. 4.9.b – Updated to specify that the HSDN SOC is subordinate to the DHS SOC. 4.9.1 – First two paragraphs updated to clarify relationship between the DHS SOC and the HSDN SOC. 4.9.1.a – Removed the words “Component SOC.” 4.9.1.b – Updated to clarify means of communication for reporting significant incidents. 4.9.1.c – Updated to clarify the length of time by which significant HSDN incidents must be reported. 4.9.1.d. – Updated to clarify reporting for HSDN incidents. **Section 5.0** 5.2.d – Replaced “Component CISO/ISSM” with “Component CISO/ISSM or his/her designee.” 5.2.1 – Changed “48 hour time period” to “24 hour time period.” 5.4.5.g – Included new policy element regarding blocking of specific Internet websites or categories. 5.4.7 – Updated the policy element to prohibit use of Webmail and other personal email accounts. 5.5.1.c – Updated to clarify that AES 256-bit encryption is mandatory. 5.7.d – Included new policy element regarding use of cryptographic modules in order to align with 4300A Handbook. 5.7.e – Included new policy element regarding rollback and journaling for transaction-based systems.
6.1.1	October 31, 2008	5.2.3 – Included new language and a link to the DHS computer login warning banner text on DHS Online.

Version	Date	Description
7.0	July 31, 2009	**General Updates** Added section and reference numbers to policy elements Added NIST 800-53 reference controls to policy elements Added hyperlinks to most DHS references Introduced new terminology Senior Agency Information Security Officer, Risk Executive, and Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53 Added Appendix A – Acronyms Added Appendix B – Glossary Added Appendix C – References list has been updated and moved to Appendix C. (these are detailed references, an abbreviated list is still found at the beginning of the document) Added Appendix D – Change History (This was moved from the front of the document) **Specific Updates** **Section 1.1 – Information Security Program Policy** – Added the statement, “Policy elements are designed to be broad in scope. Specific implementation information can often be found in specific National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Systems.” **Section 1.4.17-19 – Privacy** – Added definitions for PII, SPII, and Privacy Sensitive Systems **Section 1.5 – Exceptions and Waivers** – Updated this section, clarified policy elements, and consolidated all exceptions and waivers requirements. **Section 1.5.4 – U.S. Citizen Exception Requests** – Updated section to include policy elements: 1.5.4.a – Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this directive. 1.5.4.b – Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO. **Section 1.6 – Information Sharing and Communication Strategy** – Added policy element: 1.6.a - For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases except where pen & ink signatures are required by public law, Executive Order, or other agency requirements. **Section 1.7 – Changes to Policy** – Updated entire section **Section 2.0 – Roles and Responsibilities** – Reformats entire section. Places emphasis on DHS CISO and Component-level Information Security Roles. Secretary and senior management roles are moved to the end of the section. Some specific areas to note include: **Section 2.1.1 – DHS Senior Agency Information Security Officer** – Introduces this term and assigns duties to DHS CISO **Section 2.1.2 – Chief Information Security Officer** – Adds the following

Version	Date	Description
		responsibilities: - Appoint a DHS employee to serve as the Headquarters CISO - Appoint a DHS employee to serve as the National Security Systems (NSS) CISO **Section 2.1.3 – Component Chief Information Security Officer** – Adds policy element: 2.1.3.b - All Components shall be responsible to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO. Adds 4 additional CISOs to the list of Component CISOs: Federal Law Enforcement Training Center Office of the Inspector General Headquarters, Department of Homeland Security The DHS CISO shall also appoint an NSS CISO **Section 2.1.4 – Component Information Systems Security Manager** – Component CISO now works directly with the HQ CISO, rather than with the DHS CISO. **Section 2.1.5 – Risk Executive** – Introduces this term as per NIST. Assigns responsibilities to CISOs (already performing these functions) **Section 2.1.6 – Authorizing Official** – Introduces this term as per NIST. Replaces the term Designated Approval Authority (DAA) **Section 2.2.10 – DHS Employees, Contractors, and Vendors** – Adds the requirement for vendors to follow DHS Information Security Policy **Section 3.2 – Capital Planning and Investment Control** – Adds policy element: 3.2.f – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.3 – Contractors and Outsourced Operations** – Adds policy element: 3.3.g – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.5.2 – Contingency Planning** – Updates and expands entire section. **Section 3.7 – CM** – Adds policy elements Section 3.7.f – If the information system uses operating systems or applications that do not have hardening or do not follow configuration guidance from the DHS CISO, the System Owner shall request an exception, including a proposed alternative secure configuration. Section 3.7.g – Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes. **Section 3.9 – Certification, Accreditation, and Security Assessments** – Updates entire section **Section 3.11.1 – CISO Council** – Updates the term from CISO Board

Version	Date	Description
		Section 3.14-3.14.6 – Privacy Sections – Updates all sections pertaining to privacy and privacy information, adds section 3.14.5 – Protecting Privacy Sensitive Systems **Section 3.14.7 – E-Authentication** – Renumbers this section from 3.14.6 (due to adding of privacy section 3.14.5 **Section 3.15 – DHS Chief Financial Officer Designated Systems** – Section renamed from DHS Chief Financial Officer Designated Financial Systems **Section 3.16 – Social Media** – Added Social Media section to provide guidelines and address the Federal Government's (including DHS) use of social media sites (You Tube, Twitter) **Section 4.1.2 – Rules of Behavior** – Added policy element: 4.1.2.b – Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data. **Section 4.1.5 – IT Security Awareness, Training, and Education** – Updates entire section **Section 4.1.6 – Separation from Duty** – Updates policy element to require that all assets and data are recovered from departing individuals 4.1.6.b – Components shall establish procedures to ensure that all DHS information system-related property and assets are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual. Adds policy elements: 4.1.6.c - Accounts for personnel on extended absences shall be temporarily suspended. 4.1.6.d – System Owners shall review information system accounts supporting their programs at least annually. **Section 4.3.2 – Media Marking and Transport –** Adds "Transport" to section title and adds policy element: 4.3.2.b – Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel. **Section 4.6 – Wireless Network Communications** – Updated section title from "Wireless Communication" and specifies "network communication" technologies in policy, rather than the more general "Wireless." Removes references to the defunct "WMO." **Section 4.6.1 – Wireless Systems** – Adds policy elements: 4.6.1.f – Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO at least annually. 4.6.1.g – Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize,

Version	Date	Description
		monitor, and control wireless access to DHS information systems. **4.9.1 – Security Incidents and Incident Response and Reporting** – Adds requirement for Components to maintain full SOC and CSIRC capability (May outsource to DHS SOC). Adds policy elements: 4.9.1.k – Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS SOC. The DHS SOC shall provide SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F of the DHS 4300A Sensitive Systems Handbook. 4.9.1.q – The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required. 4.9.1.r – The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO. **Section 5.1 – Identification and Authentication** – Adds requirement for strong authentication following HSPD-12 implementation. 5.1.f – Components shall implement strong authentication on servers, for system administrators and significant security personnel, within six (6) months of the Component's implementation of HSPD-12. **Section 5.4.1 – Remote Access and Dial-In** – Updates section and adds policy element: 5.4.1.f – The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time. **5.4.3 – Network Connectivity** – Requires DHS CIO approval for all network connections outside of DHS. Also specifies requirement for CCB. 5.4.3.g – The DHS CIO shall approve all interconnections between DHS information systems and non-DHS information systems. Components shall document interconnections with an ISA for each connection. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA. 5.4.3.l - The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB. **Section 5.4.4 – Firewalls and Policy Enforcement Points** – Updates language to include Policy Enforcement Points. Adds policy elements: 5.4.4.i – The DHS CISO shall establish policy to block or allow traffic sources and destinations at the DHS TIC PEPs. The DHS CISO policy will prevent traffic as directed by the DHS CIO. 5.4.j – The DHS SOC shall oversee all enterprise PEPs. **Section 5.4.5 – Internet Security** – Prohibits Public Switched Telephone Network (PSTN) connection to OneNet.

Version	Date	Description
		5.4.5.a – Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS Trusted Internet Connection (TIC) PEPSs. The PSTN shall not be connected to OneNet at any time. **Section 5.5.3 – Public Key/Private Key** – Assigns responsibility for non-human use of PKI to sponsors. 5.5.3.g – Sponsors for non-human subscribers (organization, application, code-signing, or device) shall be responsible for the security of and use of the subscriber’s private keys. Every sponsor shall read, understand, and sign a “DHS PKI Subscriber Agreement for Sponsors” as a pre-condition for receiving certificates from a DHS CA for the non-human subscriber. **Section 5.4.6 – Email Security** – Prohibits auto-forwarding of DHS email to other than .gov or .mil addresses. 5.4.6.i - Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low. **Section 5.4.7 – Personal Email Accounts –** Requires use of encryption when sending sensitive information to email addresses other than .gov or .mil addresses. 5.4.7.b - When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly privacy data, is attached as an encrypted file. **Section 5.6 – Malware Protection** – Updates term from “Virus.”
7.1	September 30, 2009	**General Updates** Standardized the term “IT system” to “information system” Standardized the term “DHS IT system” to “DHS information system” Updated the term “DHS Security Operations Center” to “DHS Enterprise Operations Center” and added definition in glossary Replaced “must” with “shall” in all policy statements Replaced “vendors” with “others working on behalf of DHS” **Specific Updates** **Section 1.4.20** – Strong Authentication – Added definition for Strong Authentication **Section 1.4.21** – Two-Factor Authentication – Added definition for Two-Factor Authentication **Section 2.2.4** – Component Chief Information Officer – Alleviated confusion regarding Component CIO responsibilities **Section 2.2.5** – Chief Security Office – Removed erroneous CSO responsibilities which belong to Component CIOs **Section 2.2.7** – DHS Chief Financial Officer – Updated policy elements to clarify applicable policies

Version	Date	Description
		Section 3.1 – Basic Requirements (3.1.d, 3.1.g-j) – Updated policy elements to CISO/ISSM/ISSO responsibilities **Section 3.7.f** – Clarified Operating system exception requirements **Section 3.9.l-m** – Clarified requirements regarding TAF/RMS **Section 3.15** – CFO Designated Systems – Major revisions to this section **Section 4.6.2 and 5.4.1.a** – Prohibits tethering to DHS devices **Section 5.4.3.g-h** – Clarifies interconnection and ISA approval **Section 5.5** – Cryptography – Removed unnecessary elements from introductions and updated entire section with input from DHS PKI Steward
7.2	May 17, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.4.8** – Added FISMA language (transmits, stores, or processes data or information) to definition of DHS System **Section 1.5.3.k** – Removed requirement for Component Head to make recommendation regarding waivers; removed requirement to report *exceptions* on FISMA report. **Section 2.1.6** – Adds requirement for AO to be a Federal employee **Section 2.1.7** – Clarifies that CO is a senior management official; stipulates that CO must be a Federal employee **Section 2.2.5** – Updated CSO role **Section 3.2** – Added intro to CPIC section and link to CPIC Guide **Section 3.5.2.h** – Added requirement to coordinate CP and COOP testing moderate and high FIPS categorizations **Section 3.15.a** – Added requirement for CFO Designated Systems security assessments for key controls be tracked in TAF and adds requirement for tracking ST&E and SAR annually. **Section 3.15.c** – Remaps control from RA-4 to RA-5 **Section 3.15.h** – Adds mapping to IR-6 **Section 3.15.i** – Remaps control from PL-3 to PL-2 **Section 3.17** – Added requirement to protect HIPAA information **Section 4.1.l.a** – Added requirement for annual reviews of position sensitivity levels **Section 4.1.1.c** – Exempts active duty USCG and other personnel subject to UCMJ from background check requirements **Section 4.1.4.c-d** – Adds additional separation of duties requirements and restricts the use of administrator accounts **Section 5.2.f** – Limits the number of concurrent connections for FIPS-199 high systems

Version	Date	Description
		Section 5.4.2.a – Limits network monitoring as per the Electronic Communications Act **Section 5.4.3** – Added introduction to clarify ISA requirements **Section 5.4.3.f** – Clarifies the term “security policy” in context **Section 5.4.3.m –** Clarifies that both AOs must accept risk for interconnected systems that do not require ISAs. **Section 5.4.3.m-n** – Adds stipulations to ISA requirements **Section 5.5** – Updates language in entire section **Section 5.5.3.j** – Assigns the DHS PKI MA responsibility for maintaining Human Subscriber agreements
7.2.1	August 9, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.1** – Removes reference to 4300C **Section 1.4.1/3** – Updates Executive Order reference from 12958 to 13526 **Section 1.4.17** – Updates the PII section **Section 1.4.18** – Updates SPII section **Section 1.5.3** – Adds requirement for Privacy Officer/PPOC approval for exceptions and waivers pertaining to Privacy Designated Systems **Section 1.6.b/c** – Requires installation and use of digital signatures and certificates **Section 2.1.6.d** – Allows delegation of AO duty to review and approve administrators **Section 2.2.6** – Updates DHS Chief Privacy Officer description **Section 3.7.e** – Adds requirement to include DHS certificate as part of FDCC **Section 3.14 –** Updates Privacy and Data Security section **Section 3.14.1** – Updates PII section **Section 3.14.2** – Updates PTA section **Section 3.14.2.e** – Updates impact level requirements for Privacy Sensitive Systems **Section 3.14.3** – Updates PIA section **Section 3.1.4.4** – Updates SORN section **Section 3.14.4.a** – Exempts SORN requirements **Section 3.14.5** – Updates Privacy Sensitive Systems protection requirements **Section 3.14.6.a** – Updates privacy incident reporting requirements

Version	Date	Description
		Section 3.14.7 – Updates privacy requirements for e-Auth **Section 3.14.7.e** – Adds PIA requirements for e-Auth **Section 4.1.1.e** – Expands U.S. citizenship requirement for access to all DHS systems and networks **Section 4.1.4.b** – Allows delegation of AO duty to review and approve administrators **Section 4.6.2.3.c** – Clarifies prohibited use of SMS **Section 4.8.4.h** – Updates the term “trusted” to “cleared” maintenance personnel **Section 4.12.i** – Updates escort requirements for maintenance or disposal **Section 4.12.j** – Requires disabling of dial up on multifunction devices **Section 5.4.3** – Clarifies definition of Network Connectivity **Section 5.4.3.m/n** – Clarifies requirement for ISA **Section 5.4.6.j** – Requires DHS email systems to use a common naming convention **Section 5.5.3.g** – Prohibits sharing of personal private keys
7.2.1.1	January 19, 2011	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 4.8.1.a** – Changes requirement for screensaver activation from five (5) to fifteen (15) minutes of inactivity.
8.0	March 14, 2011	**General Updates** Update date and version number Replace “certification and accreditation” and “C&A” with “security authorization process”. Replace “Certifying Official” with “Security Control Assessor”. **Replace** “ST&E Plan” with “security control assessment plan”. **Replace** “ST&E” with “security control assessment” **Replace** “system security plan” with “security plan” and “SSP” with “SP”. **Specific Updates** **Section 1.4.8.1:** Change definition to specify that a GSS has only one ISSO. **Section 1.4.8.2:** Change definition to specify that an MA has only one ISSO. **Section 1.5.1:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.2:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.3:** Clarify language regarding submission of waivers and exceptions for CFO designated systems.

Version	Date	Description
		Section 1.6.d: Added new policy element, "DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies." **Section 2.1.2:** Add DHS CISO role as primary liaison to Component officials, and to perform periodic compliance reviews for selected systems. **Section 2.13:** Update Component CISO duties and add to implement POA&M process and ensure that eternal providers who operate information systems meet the same security requirements as the Component. **Section 2.1.4:** Update list of Component ISSM duties and create a POA&M for each known vulnerability. **Section 2.1.5:** Add significantly expanded Risk Executive duties. **Section 2.1.6:** Add significantly expanded Authorizing Official duties. **Section 2.2.8:** Add Program Manager responsibility for POA&M content. **Section 2.2.9:** Add expanded System Owner duties. **Section 2.2.11:** Renumber 2.2.10 as 2.2.11. **Section 2.2.10:** Add a new 2.2.10 to introduce and describe duties of Common Control Provider. **Section 3.2.g:** Added new policy element, "Procurements for services and products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation." **Section 3.5.2.c:** Updated language to clarify requirements for backup policy and procedures. **Section 3.5.2.f:** Updated language to require table-top exercises for testing the CP for moderate availability systems. **Section 3.7.f:** Added new policy element, "Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool." **Section 3.9:** Add requirement for Components to designate a Common Control Provider. **Section 3.10.b:** Policy element language was updated to clarify the function of information system security review and assistance programs. **Section 3.14:** Language updated for readability. **Section 3.14.4.c:** Added new policy element, "Components shall review and republish SORNs every two (2) years as required by OMB A-130." **Section 3.14.7.f:** Added new policy element, "Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines." **Section 3.14.7.g:** Added new policy element, "All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational." **Section 3.17:** Added reference to NIST SP 800-66 for more information on HIPAA. **Section 4.1.4.d:** Language updated to clarify usage of administrator accounts. **Section 4.1.5.f:** Language updated to clarify requirements for security

Version	Date	Description
		awareness training plan. **Section 4.3.1.b:** Language updated to clarify protection of offsite backup media. **Section 4.5.4:** Added reference to NIST SP 800-58 for more information on VoIP. **Section 4.9.j:** Language updated to require that Component SOCs report operationally to the respective Component CISO. **Section 4.9.k:** New policy element added, “The DHS EOC shall report operationally to the DHS CISO.” **Section 4.10:** Revise list of annual system documentation updates. **Section 4.12.c:** Policy element replaced with new one stating that the policy applies “to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data.” **Section 5.4.1.e:** Policy element removed. **Section 5.4.1.f:** Policy element removed. **Appendix A:** Include new acronyms **Appendix B:** Revise definition of Accreditation Package to reflect new list of documentation. **Appendix C:** Update references
9.0	October 11, 2011	**General Updates** Various minor grammatical and punctuation changes were made throughout the document. Control references updated **Specific Updates** **Section 1.5.3.a:** New policy element added to state that the 4300A Policy and Handbook apply to all DHS systems unless a waiver or exception has been granted. **Section 2.1.3:** NPPD added to the list of Components having a fulltime CISO. **Section 2.1.8.g:** New policy element added to ensure ISSO responsibility for responding to ICCB change request packages. **Section 3.14.7.e:** Policy element revised to require consultation with a privacy officer to determine if a change requires an updated PTA. **Section 3.14.7.h:** New policy element added to ensure that all new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials. **Section 4.1.5.d:** Policy element revised to clarify awareness training records requirements. **Section 4.1.5.e:** Policy element revised to clarify role-based training records requirements. **Section 4.1.5.g:** Policy element revised to require submission of an annual role-based training plan.

Version	Date	Description
		Section 4.1.5.j: Policy element revised to require annual DHS CISO review of role-based training programs. **Section 4.1.5.k:** Policy element revised to require biannual submission of roster of significant information security personnel and to specify the standard information security roles. **Section 4.3.1.f:** Policy element prohibiting connection of DHS removable media to non-DHS systems. It was already stated in 4.3.1.e. **Section 4.12.c:** Policy element was moved to 1.5.3.a. **Section 5.2.f:** Policy element revised to allow concurrent sessions to one if strong authentication is used. **Section 5.2.g:** New policy element added to ensure preservation of identification and access requirements for all data-at-rest.
9.0.1	March 5, 2012	**Section 2.1.3:** Includes language to address the designation of a Deputy CISO by the Component CISO. Add two new responsibilities for Component CISO: Serve as principal advisor on information security matters; Report to the Component CIO on matters relating to the security of Component information Systems. **Section 2.2.4:** Includes new language stating that the Component CISO reports directly to the Component CIO. **Section 4.1.1.c:** Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to Federal employees. **Section 4.1.1.d:** Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to contractor personnel.
9.0.2	March 19, 2012	**Throughout the document:** *EOC* and *Enterprise Operations Center* replaced with *SOC* and *Security Operations Center* respectively **Section 1.6:** Section 1.6, Information Sharing and Electronic Signature was divided into two sections – Section 1.6, Electronic Signatures, and Section 1.7, Information Sharing. **Section 1.8:** Section 1.8, Threats, was added to the policy. **Section 3.9.w:** Policy element added to require common control catalogs for DHS enterprise services. **Section 3.9.x:** Policy element added to require the development of Enterprise System Security Agreements for enterprise services. **Section 5.1.g:** Policy element added to require use of PIV credentials for logical authentication where available.
9.1	July 17, 2012	**General Changes** Style, grammar, and diction edited. Updated control references. Updated links. **Specific Changes** **Section 1:** Updated citations. **Section 1.6.b:** Changed to require use of electronic signatures where practicable.

Version	Date	Description
		Section 1.8.5: Section added defining *supply chain threat* and *supply chain.* **Section 2.1.3:** Added Science and Technology (S&T) to the list of Components that shall have fulltime CISOs. **Section 2.1.6.a:** Clarified language (designation of AOs at Department level). **Section 2.1.6.b:** Clarified language (designation of AOs at Component level). **Section 3.1.k:** Added policy statement requiring SCAP compliance. **Section 3.11.3:** Added section, including two policy statements, relative to Security Policy Working Group. **Section 3.14.6.e:** Updated reference title and hyperlink. **Section 3.18:** Section added containing Cloud Services policy. **Section 4.10:** Policy statements revised. **Section 4.1.1.c:** Changed "Minimum Background Investigation (MBI)" to "Moderate Risk Background Investigation (MBI)." **Section 4.1.5.k:** Changed "Contracting Officer Technical Representative" to "Contracting Officer Representative." **Section 4.3.1.d:** Changed policy statement to pertain only to USB drives. **Section 4.9.1[four.nine.ell]:** Added policy statement requiring the NOC/SOC to be under the direction of a Government employee who shall be present at all times. **Sections and subsections 4.10 renumbered 4.91 and subsections** **Sections 4.11 through 4.13 renumbered 4.10 through 4.12** **Section 4.9.1.b:** Revised with clarification of reporting means and requirements. **Section 4.9.1.c:** Revised with clarification of reporting means and requirements. **Section 5.4.6.k:** Added policy statement moved from 5.4.7.b. **Section 5.4.7.b:** Deleted and becomes new policy statement 5.4.6.k. **Section 5.5.2** Section 5.5.2: Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI. **Section 5.5.3** Section 5.5.2: Revised to address the two DHS PKIs now functioning: DHS FPKI and DHS Internal NPE PKI. **Section 5.8:** Added new section, including two policy statements, relative to IT supply chain risks and protection against supply chain threats. **Appendix A, Acronyms and Abbreviations:** Additions and updates.
10.0	May 20, 2013	**General:** Changed version numbering system; all instances of "TAF" and "RMS" replaced with "IACS" throughout the document. **Section 1.5.3.n:** Included new policy element regarding expiration for exceptions. **Section 2.2.7.a:** Revised DHS CFO responsibility as AO for financial and mixed financial systems. **Section 3.11.4:** Included section on the ESSWG Section 3.18: Revised policy on cloud services/FedRAMP

Version	Date	Description
		Section 4.11: Revised policy on backup media protection. **Section 5.4.3:** Included new TIC traffic requirements.
11.0	April 30, 2014	**General:** Removed language regarding exceptions to policy from the document. **Section 1.5.2 and 4.1.1.e:** Revised to transfer responsibility to OCSO for granting access to IT systems by non-U.S. citizens. **Section 1.6:** Revised to align with NARA and OMB requirements and guidance on Electronic Signatures. **Section 3.18:** Revised policy on cloud services/FedRAMP **Section 4.62 (principally) and throughout:** “PED,” “PDA,” and “wireless PDA” have been replaced with the words “wireless mobile devices.” **Section 5.5.2:** PKI policy element revisions throughout. Element 5.5.2.w, requiring appointment of Component PKI Managers, is rescinded. **Section 5.8:** Revised policy on supply chain
12.0	September 21, 2015	**General:** Updated FISMA references (“Federal Information Security Management Act “ to “Federal Information Security Modernization Act of 2014”). **Section 1.4:** Alphabetized definition entries. **Section 1.4.7:** Removed statutory requirements language from FISMA definition **Section 1.4.14:** Revised definition of Personally Identifiable Information (PII) **Section 1.4.16:** Added definition of “privileged user” based on Cybersecurity Sprint communication **Section 1.4.19:** Revised definition of Sensitive Personally Identifiable Information. **Section 1.4.20:** Added definition of “Sensitive System” in response to Deputy CISO request **Section 1.4.21:** Revised definition of Strong Authentication based on Cybersecurity Sprint communication **Section 1.4.24:** Added definition of “visitor” in response to an OIG recommendation **Section 1.5.1.c:** Removed because the statement was procedure, not policy **Section 1.5.1.e:** Removed because the statement was procedure, not policy **Section 1.5.1.g:** Removed because the statement was procedure, not policy **Section 1.5.1.h:** Removed to align policy with actual procedure **Section 1.5.1.j:** Removed to align policy with actual procedure **Section 1.6:** Renamed to “Digital and Other Electronic Signatures”; section underwent major revision **Section 2.1.2:** Removed responsibilities related to COOP planning, security awareness training, and insider threat and Info Sec workforce development programs; added supply chain responsibilities **Section 2.1.3:** Removed responsibility related to execution of DHS Logging Strategy, which no longer exists **Section 2.1.4:** Added supply chain and software assurance responsibilities

Version	Date	Description
		Section 2.1.5: Added supply chain responsibilities **Section 2.1.7:** Security control assessor is assigned in writing by Component CISO or ISSM **Section 2.1.8:** Updated to require BIs for ISSOs; removed Secret clearance requirement **Section 2.2.3:** Added supply chain responsibilities **Section 2.2.4:** Added supply chain responsibilities **Section 2.2.8:** Added supply chain responsibilities and requirement to complete security control assessment for common controls **Section 2.2.9:** Added supply chain responsibilities **Section 3.7.i:** Added requirement for users to report IT changes to DHS Enterprise Configuration Management **Section 3.9.a:** Updated to include NIST SP 800-161 security controls in security authorization process **Section 3.9.b:** Updated to include NIST SP 800-161 security controls in security authorization process **Section 3.9.1:** Various changes throughout section **Section 3.14.1:** Per direction of the DHS Privacy Office, removed text following policy table **Section 3.14.1.g:** Removed; policy was incorporated into 3.14.1.f **Section 3.15.n:** Added supply chain responsibilities **Section 3.16:** Removed text following policy table **Section 4.1.4:** Replaced “separation of duties” with “segregation of duties” **Section 4.6.2.d:** Updated to include requirement for password complexity **Section 4.6.2.n:** Added to allow local access to mobile devices using fingerprint technology **Section 4.6.2.4:** Added new “Bluetooth” section **Section 4.8.4.d:** Revised to add requirement to protect against pass-the-hash & lateral movement vulnerabilities **Section 4.8.4.m:** Added requirement to include software assurance and supply chain in acquisition decisions **Section 4.8.4.n:** Added requirement to analyze COTS hardware and software for supply chain risk prior to procurement and upgrading **Section 5.1.c:** Updated to clarify policy related to disabling inactive user identifiers applies to all users **Section 5.1.g:** Revised based on Cybersecurity Sprint communication **Section 5.1.h:** Revised based on Cybersecurity Sprint communication **Section 5.1.k:** Added based on Cybersecurity Sprint communication **Section 5.1.l:** Added based on Cybersecurity Sprint communication **Section 5.3.j:** Added based on Cybersecurity Sprint communication **Section 5.4.2.a:** Updated continuous monitoring requirements to include information of third parties **Section 5.5.1.m:** Added to clarify PIV requirement **Section 5.5.1.n:** Added to clarify PIV requirement

Version	Date	Description
		Section 5.5.1.o: Added to clarify PIV requirement **Section 5.5.2:** Various changes throughout section **Section 5.5.3:** Various changes throughout section **Section 5.8.a:** Added to include NIST SP 800-161 security controls in security authorization process **Section 5.8.b:** Added to include NIST SP 800-161 security controls in security authorization process
12.01	February 12, 2016	**Section 1.6.2.c:** Updated to make the role of the signer mandatory in the visible signature block. **Section 5.4.6.l:** Added requirement for use of Government email accounts for Government business.

Question#:	17
Topic:	Family Case Management Program
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: I understand that ICE has started a new alternative to detention initiative, the Family Case Management Program (FCMP), and that Geo Care, a private company, will serve as the umbrella provider for the program. ICE has stated that partnering with community-based organizations "will be a cornerstone of the FCMP."

What steps will you take to involve local community organizations and service providers throughout the duration of the FCMP?

Response: GEO Care and U.S. Immigration and Customs Enforcement (ICE) recognize the expertise and experience of community-based immigration assistance organizations that have a long history of assisting recently-arriving populations. Building partnerships with these local community providers to promote compliance with immigration obligations has been a key focus from the inception of the Family Case Management Program (FCMP). GEO Care submitted its proposal with notice of intent letters and has since finalized formal partnerships with community-based social service organizations to provide holistic case management services. These services include:

- Assessments and individualized family service plans;
- Orientation and education to participants about their legal rights and responsibilities;
- Tracking and monitoring of immigration obligations (to include attendance at immigration court hearings);
- Referrals to legal services and community resources;
- Assistance with transportation logistics (if an emergency and needed only to attend a required ICE check-in, court appearance, or to further removal); and
- Safe repatriation and reintegration planning for participants who are returning to their home countries.

ICE is enrolling participants in five metropolitan areas, including Baltimore/Washington DC, Chicago, Los Angeles, Miami, and New York City/Newark. Each region has a mix of both GEO Care case managers and case managers from partnered community-based organizations (CBOs).

As of January 15, 2016, GEO Care has finalized Case Management partnerships with the following groups:

Question#:	17
Topic:	Family Case Management Program
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

- Baltimore/Washington DC – Bethany Christian Services;
- Chicago – Frida Kahlo Community Organization;
- Los Angeles – International Institute of Los Angeles;
- Miami – Youth Co-Op, Inc; and
- New York City/Newark – Catholic Charities NYC.

Additional partnerships to provide Know Your Rights presentations have also been finalized. These include:

- Baltimore/Washington DC – Bethany Christian Services, Catholic Charities Esperanza Center, and Immigration Solutions Group;
- Chicago – Frida Kahlo Community Organization;
- Los Angeles – International Institute of Los Angeles, Cinthia Rivera;
- Miami – Youth Co-Op, Inc, Guatemalan Maya Center; and
- New York City/Newark – Catholic Charities NYC and Lutheran Social Services of NYC.

Question: What plans are in place to monitor outcomes and the quality of services provided to immigrant families under the contract?

Response: Throughout the contract period, ICE Enforcement and Removal Operations (ERO) will evaluate the FCMP, including the contractor's delivery of FCMP deliverables, using a set of defined performance metrics. Ultimately, the success of the program will be judged based on the extent to which participants comply with their immigration obligations (to include attendance at all immigration court hearings and other ICE reporting requirements). These compliance rates will presumably be directly influenced by the quality of services provided to family units. Thus, it is in the best interest of ICE to ensure that GEO Care and all partnered CBOs perform their required services, as defined in the program statement of objectives.

Per the contract, the contractor is required to provide regular participant compliance reports to ICE including, but not limited to, ICE reporting dates, immigration court hearings, and services received by participants. FCMP case managers are also required to report any serious or emergent incidents, including loss of accountability of a participant's whereabouts, participant arrest on criminal charges or contact with law enforcement, or participant hospitalization. It is important to note that the contractor is contractually obligated to provide access to the set of defined program services but will not be responsible if, after reasonable efforts, FCMP participants fail to take advantage of services offered.

Question#:	17
Topic:	Family Case Management Program
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Patrick J. Leahy
Committee:	JUDICIARY (SENATE)

Question: What steps are you taking to address the potential conflict of interest posed by contracting with a private company?

Response: ICE does not believe there is a conflict of interest. ICE has contracted and continues to contract with private companies to provide a variety of services related to alternatives to detention, delivery of healthcare, transportation, telephone access, legal access, etc. Any issues related to contract compliance or the need to take remedial action against a contractor is done in accordance with the Federal Acquisition Regulation. ERO closely monitors GEO Care’s performance as a matter of contractual obligation.

Question#:	10
Topic:	Family detention 1
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: What is ICE's current policy regarding access by attorneys to family detention facilities? Please provide a copy of the policy.

Response: Over the past several months, U.S. Immigration and Customs Enforcement (ICE) has implemented significant modifications regarding the manner in which attorney access in family residential centers is facilitated. In order to ensure consistency, ICE also on October 30, 2015 issued a standard operating procedure (SOP) applicable to legal access and legal visitation at all ICE family residential centers. The SOP is consistent with the existing Family Residential Standards and provides greater detail with regard to operational practices locally. A copy of the SOP is enclosed.

Question: Does ICE require that this policy be posted at its family detention facilities? If so, where in the detention facilities is the policy posted?

Response: Yes. The Family Residential Standards require family residential centers to post attorney access and visitation rules and hours in the visitor waiting areas and housing areas; provide residents written notification of visitation rules and hours in the resident handbook; and make the schedule and procedures available to the public, both in written form and telephonically. ICE has made the SOP public, and it is available at the following link: https://www.ice.gov/sites/default/files/documents/Document/2016/acfrcBriefingMaterialsMar2016.pdf.

Question: Which ICE officials are responsible for implementing this policy at each of the family detention facilities? Do the officials check periodically to determine whether or not the policy is being followed?

Response: Compliance with the ICE Family Residential Standards is monitored by an extensive ICE presence in and oversight of the family residential centers, including a dedicated Detention Service Manager, who monitors daily operations as well as interaction between staff and facility residents. ICE also employs a variety of methods to monitor each family residential center. One such method is a robust independent compliance inspection program consisting of monthly audits conducted by independent consultants with expertise in child development and conditions of confinement. In all cases, appropriate corrective action is taken when needed.

Question#:	11
Topic:	Family detention 2
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: What role, if any, do contractors have in controlling attorneys' access to the family detention facilities?

How many attorneys have been banned from ICE family detention facilities to date? What are the duration of these bans? What is the justification for these bans? Have any bans been lifted?

Response: While U.S. Immigration and Customs Enforcement (ICE) contracts with other entities to assist with family residential center operations at each site, including managing visitor and attorney access to the facilities, contractors are required to comply with the Family Residential Standards and facility policies and processes. Their compliance is monitored by ICE staff.

With regard to bans, earlier this year, two attorneys were asked to leave a family residential center for violating existing policies. The first incident involved an individual who entered an unauthorized area, acted in a disruptive manner, and physically attempted to thwart an ICE supervisor from carrying out her duties. The second incident involved an individual who entered an unauthorized area, disrupted a staff briefing, and became hostile towards ICE staff. Future requests for access to the facility by these individuals will be considered on a case-by-case basis.

Generally, any visitor who exhibits inappropriate or unprofessional behavior, violates visitation policies, disrupts operations, or creates security issues may be asked to leave a family residential center in accordance with the Family Residential Standards. Any visitor's failure to abide by the visitation rules may result in immediate cancellation or termination of a visit and/or suspension of future visitation privileges. This process is necessary to ensure the safety, security, and good order of the facility, its staff, and residents.

Question#:	12
Topic:	Family detention 3
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: Please explain what role, if any, you or officials at ICE or DHS headquarters have in reviewing a determination to ban an attorney from an ICE family detention facility or to lift such a ban.

Response: Although the facility administrator may take immediate action to cancel or terminate a visit, a determination to suspend future visitation privileges is made by the U.S. Immigration and Customs Enforcement, Enforcement and Removal Operations (ERO) Field Office Director (FOD) with jurisdiction over that facility. The FOD is also responsible for considering requests to reinstate visitation privileges. ERO field office decisions concerning visitation privileges are also reviewed at the headquarters level, as appropriate.

Question#:	13
Topic:	Family detention 4
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: In the family detention context, is it ICE policy or practice to restrict or prohibit detained individuals' access to counsel during meetings at which the timing and conditions of their release are determined? Is it ICE policy or practice to have individuals in family detention—who have secured legal representation—sign documents or make decisions affecting their legal case or the terms of their custody and/or release outside the presence of their attorney? If so, which decisions, and which documents? Please explain.

Response: It is not U.S. Immigration and Customs Enforcement policy or practice to restrict or prohibit Family Residential Center residents' access to legal counsel. While a resident may be served with documentation outside the presence of his or her legal representative, a resident is not required to make legal decisions without the opportunity to consult with his or her legal representative.

Question#:	14
Topic:	Family detention 5
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: In the family detention context, what information do detained individuals receive from ICE regarding the possibility of bond as a condition of release?

Response: When U.S. Immigration and Customs Enforcement (ICE) serves a resident with a Notice to Appear, the ICE officer is also required to serve the resident a Notice of Custody Determination if the resident is detained pursuant to section 236 of the Immigration and Nationality Act. The Notice of Custody Determination explains the resident's initial custody determination and advises the resident of their right to seek a custody redetermination with the immigration judge. The Department of Justice's Executive Office for Immigration Review has programs that provide legal information to detained individuals. U.S. Immigration and Customs Enforcement defers to the Department of Justice's Executive Office for Immigration Review for more information in its programs.

Question: In the family detention context, what information do detained individuals receive from ICE regarding their right to seek a custody redetermination before an immigration judge?

Response: Residents who arrive at family residential centers generally fall into the Expedited Removal process or Reinstatement of Removal process. In both types of cases, individuals do not initially qualify for custody redetermination by an immigration judge.

However, if a resident, who is not an arriving alien, is processed for Expedited Removal and is determined by a U.S. Citizenship and Immigration Services (USCIS) asylum officer to possess a credible fear, the asylum office will issue a Notice to Appear, rendering them potentially eligible for release on bond or other conditions. As stated in the response to Question 8 above, such residents are provided with a Form I-286, Notice of Custody Determination, which advises them of their right to seek a hearing before an immigration judge to review ICE's custody determination.

Question: In the family detention context, what information do detained individuals receive from ICE regarding ankle monitors?

Response: Upon release, individuals who are enrolled in Alternatives to Detention with an ankle monitor receive a briefing on how the system operates and how to maintain and charge the device. Additionally, all Alternatives to Detention enrollees receive a

Question#:	14
Topic:	Family detention 5
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

pamphlet that explains the charging and messaging operations of the Global Positioning System ankle monitors as well as a handout with reporting instructions, location, and emergency contact information for their reporting office.

Question#:	15
Topic:	Noncitizen's ankle monitor
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: What written guidance do field offices-whether ICE or contractors-receive from DHS or ICE regarding the timing and circumstances under which a noncitizen's ankle monitor will be removed, and their supervision de-escalated?

Response: As a part of case management, U.S. Immigration and Customs Enforcement (ICE) recommends to the field that Deportation Officers conduct regular and recurring case reviews to make determinations on compliance. For those participants who are determined to be compliant with their release conditions, Deportation Officers should consider de-escalation of case management and the technology assigned.

Question#:	16
Topic:	Flores litigation
Hearing:	Oversight of the Administration's Criminal Alien Removal Policies
Primary:	The Honorable Al Franken
Committee:	JUDICIARY (SENATE)

Question: What steps has ICE taken to come into compliance with the recent federal court order by Judge Dolly Gee in the Flores litigation?

Response: The Department of Homeland Security (DHS) continues to monitor and evaluate its processes in order to remain in compliance with the order of the district court pending appeal of the decision. DHS is processing families who assert a fear of return as expeditiously as possible to screen for credible fear and reasonable fear claims.