Goal 1: Strengthen the security and integrity of the immigration system

Objective 1.1: Enhance the security of the United States by ensuring that immigration benefits are granted only to eligible applicants and petitioners

A secure immigration system depends on the vigilance of every USCIS employee. To ensure the immigration benefits system fully supports our national security, we have planned and implemented improvements in several operational areas.

As part of USCIS' broad effort to modernize the agency, we have undertaken business transformation initiatives, including the conversion of the current mix of legacy infrastructure and paper-based business processes to electronic-based business process. This transformation will provide improved security and integrity throughout the business process by establishing and verifying the identity of individuals, applying advanced risk assessment tools to combat identity and benefit fraud, and enhancing data sharing with partners to ensure timely, relevant immigration information. Realization of this future transformed environment will significantly help close security gaps inherent in the current business process.

As part of the Transformation Program, we are piloting, in cooperation with the DHS US-VISIT biometric screening program, biometric-based enumeration to uniquely identify applicants and petitioners. We will link these unique enumerators in our automated systems to other applicant documentation, which will preserve an applicant's identity for future identification, verification, and benefits processing purposes.

To further strengthen security, we have implemented an Intelligence Program that is consistent with the DHS National Intelligence Plan. To ensure that our officers have useful and updated information to support quality decision making, we have developed the online Adjudicator's Toolbox, which provides ready access to legislative, regulatory, and fraud information, and other reference materials. There is also an Asylum Virtual Library, a searchable electronic library that contains relevant policy and procedures documents as well as country of origin information. It serves as the source for all basic information asylum staff require to carry out operational functions and conduct quality adjudications. These resources allow USCIS employees to focus efforts on maximizing timely service for eligible customers while preventing ineligible applicants from obtaining benefits. We will also continue to perform law enforcement background checks on all persons seeking immigration benefits to ensure that individuals

who pose a threat to our nation are not granted immigration or citizenship benefits.
To further promote the integrity of the immigration system, we will:

- Link all biometrics to a unique enumerator to ensure that each applicant is uniquely identified.

- Ensure that all fingerprint checks are completed and no adverse information received prior to the granting of immigration benefits.

- Enhance our Fraud Detection and National Security (FDNS) operation by deploying additional personnel and utilizing technology.

- Make ongoing improvements to the Fraud Detection and National Security Data System that will enhance our effectiveness in resolving issues with background checks and other national security and public safety concerns.

- Increase staffing for USCIS legal counsel for litigation support to ensure due process and the ability to address legitimate concerns in a timely manner.

- Develop templates for use in litigation and issue tracking to ensure the consistency and timeliness of issue resolution.

- Enhance interagency information-sharing mechanisms that ensure USCIS has access to all relevant information maintained by the U.S. government when making benefit decisions.

Objective 1.2: Deter, detect, and pursue immigration-related fraud
As USCIS strengthens and improves the systems it uses to provide immigration services, it remains committed to preventing and detecting all types of fraud. We will increase staffing and technology-based resources for our FDNS Division and expand the resources FDNS uses to perform site visits for fraud prevention and detection purposes. FDNS has completed reports and identified various trends of immigration fraud, and we will build upon these efforts to increase our ability to identify and track fraud. We will enhance efforts to train adjudicators to recognize fraud. As fraud is detected, we will promptly act to inform our law enforcement partners as necessary, and to implement methods to effectively counter any threats presented.

We have established standard operating procedures to facilitate collaboration between USCIS and U.S. Immigration and Customs Enforcement (ICE) in the joint effort to combat benefit fraud and detect persons seeking immigration benefits who pose a threat to national security and public safety. We will continue to work with ICE and refer suspected cases of immigration fraud for investigation and possible prosecution (pursuant to the standards of acceptance set by prosecuting authorities). We have also completed the integration of our asylum process with the DHS US-VISIT biometric verification program.

Our anti-fraud strategies will be:

- Replace Permanent Residence Cards (Form I-551) issued prior to 1989 and that do not contain expiration dates to reduce the incidence of fraud.

- Enhance USCIS' effectiveness in obtaining information from law enforcement and intelligence agencies that may influence or address concerns about national security or public safety involving persons seeking immigration benefits.

- Develop tools that help officers better recognize various types of fraud, thus improving USCIS' effectiveness in detecting and combating immigration benefit fraud.

- Develop tools that enhance communications and help officers take appropriate action in cases where there are indicators of a national security or public safety concern.

- Implement methods to analyze fraud reactively, as well as identify emerging fraud trends in a proactive manner.

- Conduct Benefit Fraud and Compliance Assessments aimed at identifying and analyzing the volume, types, and causes of benefit fraud committed, and potential solutions.

- Pursue development of the technology needed to better support anti-fraud and security-check related operations. This includes a case management system that captures the data necessary to measure performance and the analytics needed to identify and flag known fraud indicators and track fraud and national security cases from referral to completion to ensure all instances of fraud are captured.

- Reengineer aspects of the Fraud Detection and National Security Data System to improve security check processing to safeguard against individuals and entities that may seek to defraud our nation's immigration system.

- Provide guidance and coordinate the revocation of benefits for individuals who have fraudulently obtained benefits, are identified as a threat to national security or public safety after a benefit has been granted, or are otherwise no longer qualified to hold benefit status.

- Continue to train FDNS staff to analyze and identify fraud patterns and trends and to document evidence of fraud as part of our fraud fighting efforts.

- Continue to train staff to document the status and results of national security vetting and adjudicative activities, and establish procedures for evaluating systemic vulnerabilities that could be exploited.

- Design a system that, as necessary, allows for efficient policy and procedural changes when a systemic vulnerability or widespread fraud activity has been detected.

- Establish mechanisms to ensure individuals who have fraudulently obtained benefits, represent a national security threat, or are otherwise no longer qualified to receive benefit status, are appropriately processed and referred for prosecution and/or removal from the United States.

- Proactively share actionable fraud-related information with other appropriate federal agencies.

Objective 1.3: Identify and share immigration-related information with partners
USCIS recognizes its critical role within DHS in support of our nation's security and understands that this responsibility requires serving as a useful resource to its strategic partners. USCIS has devoted significant resources towards strengthening its automated systems so we can securely exchange digitized information with appropriate government entities. USCIS will continue to ensure accurate and current information about a person's immigration status is electronically available as needed by agencies entrusted to protect the public and safeguard the nation.

To help protect the security of the nation and support the mission responsibilities of our partners, we will:

- Review and improve standard and secure operating procedures to govern the exchange of digitized security information to ensure the privacy of our customers is safeguarded at all times.

- Increase the ability to share immigration related information electronically in order to enable our partner agencies to achieve their mission.

- Proactively identify the information needs and issues of common concern for our partners, including federal, state, and local agencies through regular meetings of collaborative bodies such as the Transformation Program Federal Stakeholder Advisory Board.

- Proactively share information and collaborate with other DHS components and agencies in accordance with law and regulation.

Objective 1.4: Integrate security precepts with immigration adjudication processes
USCIS fully recognizes its responsibilities as an integral part of our national effort to secure the United States from dangerous people, including terrorists and other criminals. We must carefully screen all individuals seeking immigration benefits to identify those who pose a risk to national security and public safety and prevent them from exploiting the immigration system.

We also are responsible for ensuring the security and integrity of USCIS employees. To coordinate all aspects of security management, USCIS created the Office of Security and Integrity (OSI) to support the integrity of the immigration processing system through active management of personnel security functions. Personnel security is a fundamental requirement for guaranteeing the proper one to one balance as the correct service reaches the correct individual. USCIS ensures that personnel undergo required background checks before beginning employment and that security clearances are granted only to the appropriate personnel. Additionally, OSI – working with the Office of Information Technology (OIT) – ensures the agency's critical automated systems and infrastructure are protected, that automated systems are not used for malicious or unlawful purposes, and that resources are properly used to achieve the agency's mission. If security incidents or breaches occur, USCIS investigates and documents any such events and applies the appropriate corrective measures. Our security strategies include:

- Ensuring the appropriate background checks are performed for those tasked with adjudicating applications and petitions, as well as for those performing related functions.

- Safeguarding information and assets across the USCIS enterprise through education and by conducting defensive activities to identify and analyze internal and external threats.

- Efficiently performing personnel security background checks for hiring, employment retention, and security clearance granting purposes.

- Continuing to emphasize the proactive usage of sound operations security measures, including protecting sensitive and classified documents and access to automated systems.

- Investigating all allegations of employee misconduct, corruption, and fraud that are not subject to investigation by the DHS Inspector General to improve the integrity of our processes.

"The bosom of America is open to receive not only the Opulent and respectable Stranger, but the oppressed and persecuted of all Nations and Religions; whom we shall welcome to a participation of all our rights and privileges, if by decency and propriety of conduct they appear to merit the enjoyment."

George Washington