

US-VISIT Program Overview

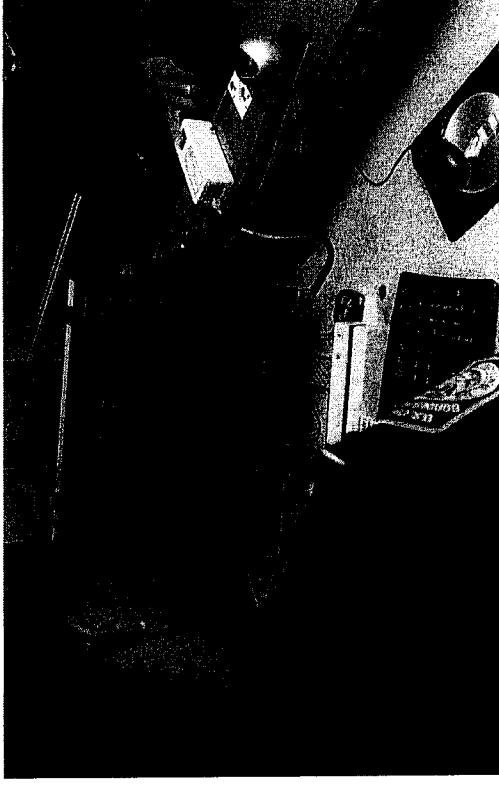
United States Visitor and Immigrant Status Indicator Technology

December 15, 2004

Steve Yonkers
DHS

US-VISIT Goals

- Enhance the security of our citizens and visitors
- Facilitate legitimate travel and trade
- Ensure the integrity of our immigration system
- Protect the privacy of our visitors



Homeland
Security

US-VISIT Mission

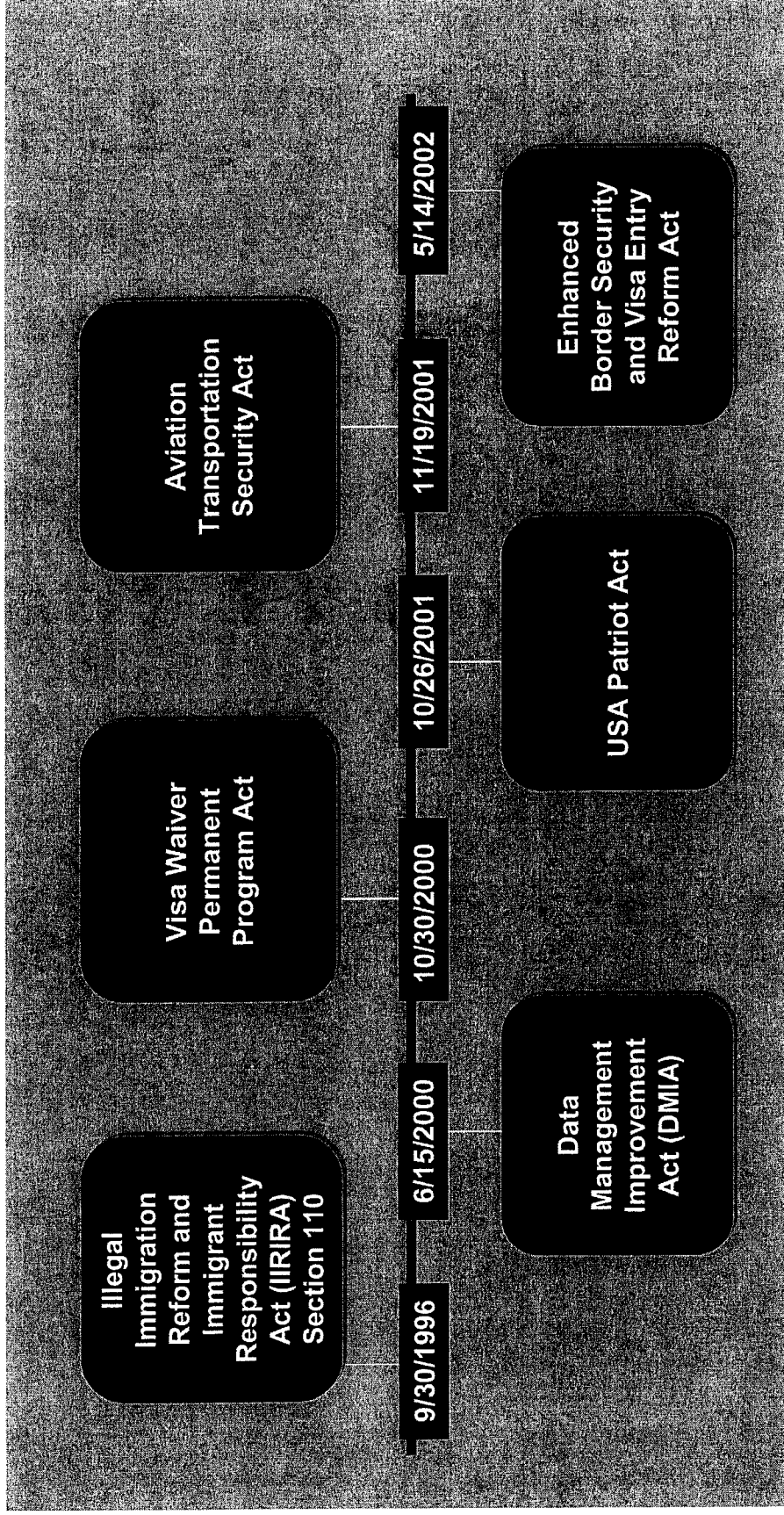
To collect, maintain, and share information, including biometric identifiers, through a dynamic system, on foreign nationals to determine whether the individual:

- Should be prohibited from entering the U.S.
- Can receive, extend, change, or adjust immigration status
- Has overstayed or otherwise violated the terms of their admission
- Should be apprehended or detained for law enforcement action
- Needs special protection/attention (i.e. refugees)



**Homeland
Security**

History/Legislation



**Homeland
Security**

Critical Dates

September 30, 2004

- US-VISIT procedures expanded to include visitors traveling to the U.S. under the Visa Waiver Program (VWP) arriving at air and sea ports of entry

December 31, 2004

- Deploy US-VISIT Program to 50 busiest land border POEs
- Biometric enrollments reduced at POEs as the biometric capture/process is increased at overseas Consular Offices.
- Biometric identity verification with biometric visas (one-to-one)



Homeland
Security

Critical Dates

October 26, 2005

- Deploy capability to read biometric travel documents at air, sea, and land ports of entry (POE)
- All countries under VWP must issue biometrically enabled travel documents following International Civil Aviation Organization (ICAO) standards

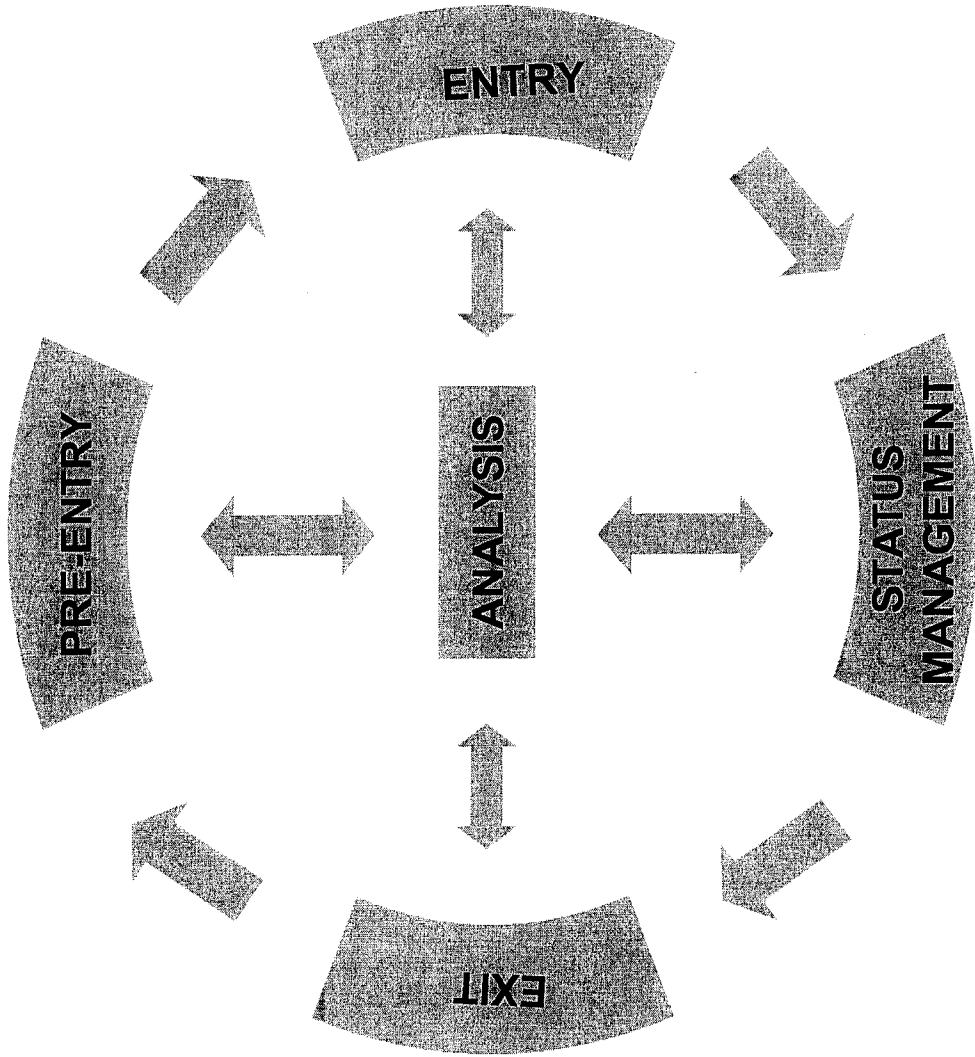
December 31, 2005

- Extend Entry capability to remaining land border ports



Homeland
Security

US-VISIT: Continuum of Security Measures



Homeland
Security

US-VISIT: Continuum of Security Measures – Current Status

Pre-entry:

- October 2004, all 211 visa-issuing posts collect biometric data

Process:

- Visitors place the left, then the right index finger on the fingerscanner
- Photograph is scanned into the system
- Fingerscans are checked against watchlists and are linked to the travel document



Homeland
Security

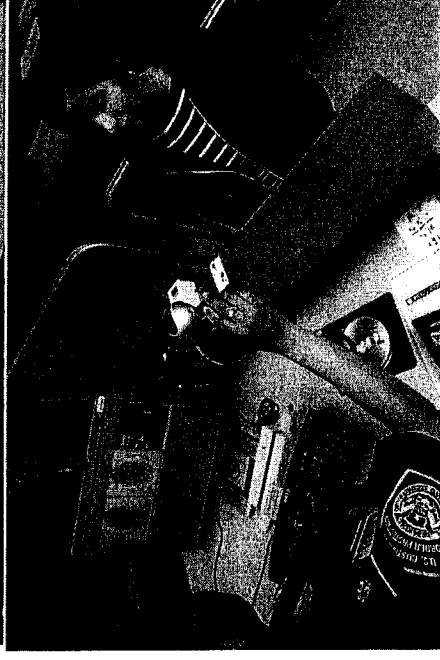
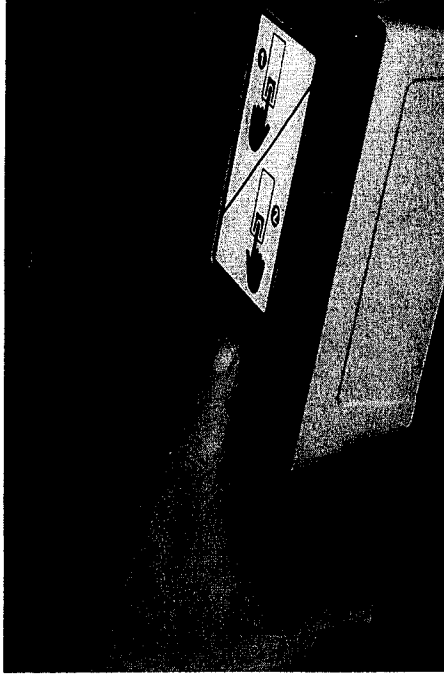
US-VISIT: A Continuum of Security Measures – Current Status

Entry:

Digital fingerscans are checked against a database of known and suspected terrorists and criminals to determine the person applying for entry into the U.S. is the same person issued the visa.

Process:

- Visitors place the left, then the right index finger on the fingerscanner
- A digital photograph is taken



Homeland
Security

US-VISIT: A Continuum of Security Measures

Status Management:

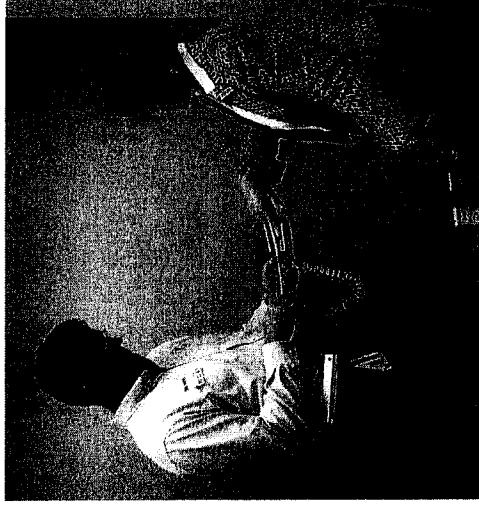
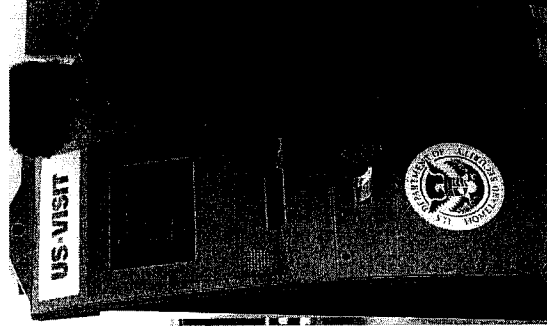
- Should the traveler seek to adjust status or extend his/her stay, US-VISIT would be updated with any modifications to the individual's status
- Arrival and departure records are reconciled, and any inconsistency allows US-VISIT to determine when a visitor has overstayed



Homeland
Security

Exit

- Biometric departure solutions are currently being tested. Additional alternatives will be tested and evaluated.
- Visitors are required to check out of the country if leaving from a port with exit stations to record their status for future visits.



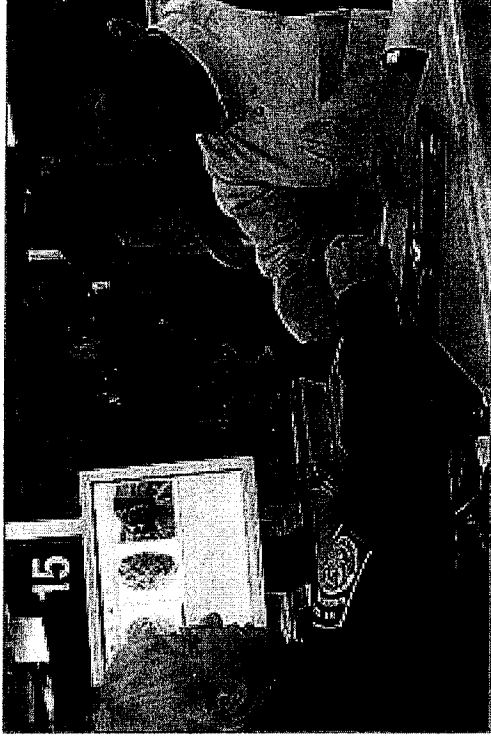
Homeland
Security

Who Is Processed Under US-VISIT

Today, most foreign travelers who visit the U.S. are enrolled in US-VISIT.

- Visitors under age 14 and over 79 are exempt
- Certain classifications of non-immigrants (A, C, G, NATO) are exempt
- September 30, 2004, enrollment expanded

to include visitors traveling under the Visa Waiver Program (VWP)



**Homeland
Security**

Positive Impacts of US-VISIT

- Increased ability to biometrically identify known or suspected wanted persons
 - i.e. fugitives, known terrorists
- Enhanced ability to focus DHS enforcement efforts on overstays
- Increased data sharing resulting with DHS and DOS in more effective and accurate visa and POE processing
- Expedited service for low-risk frequent travelers
- Increased reliability in matching departures and arrivals



Homeland
Security

US-VISIT: Successes

US-VISIT has been hailed as the greatest improvement in border security in three decades. Some of the US-VISIT successes are:

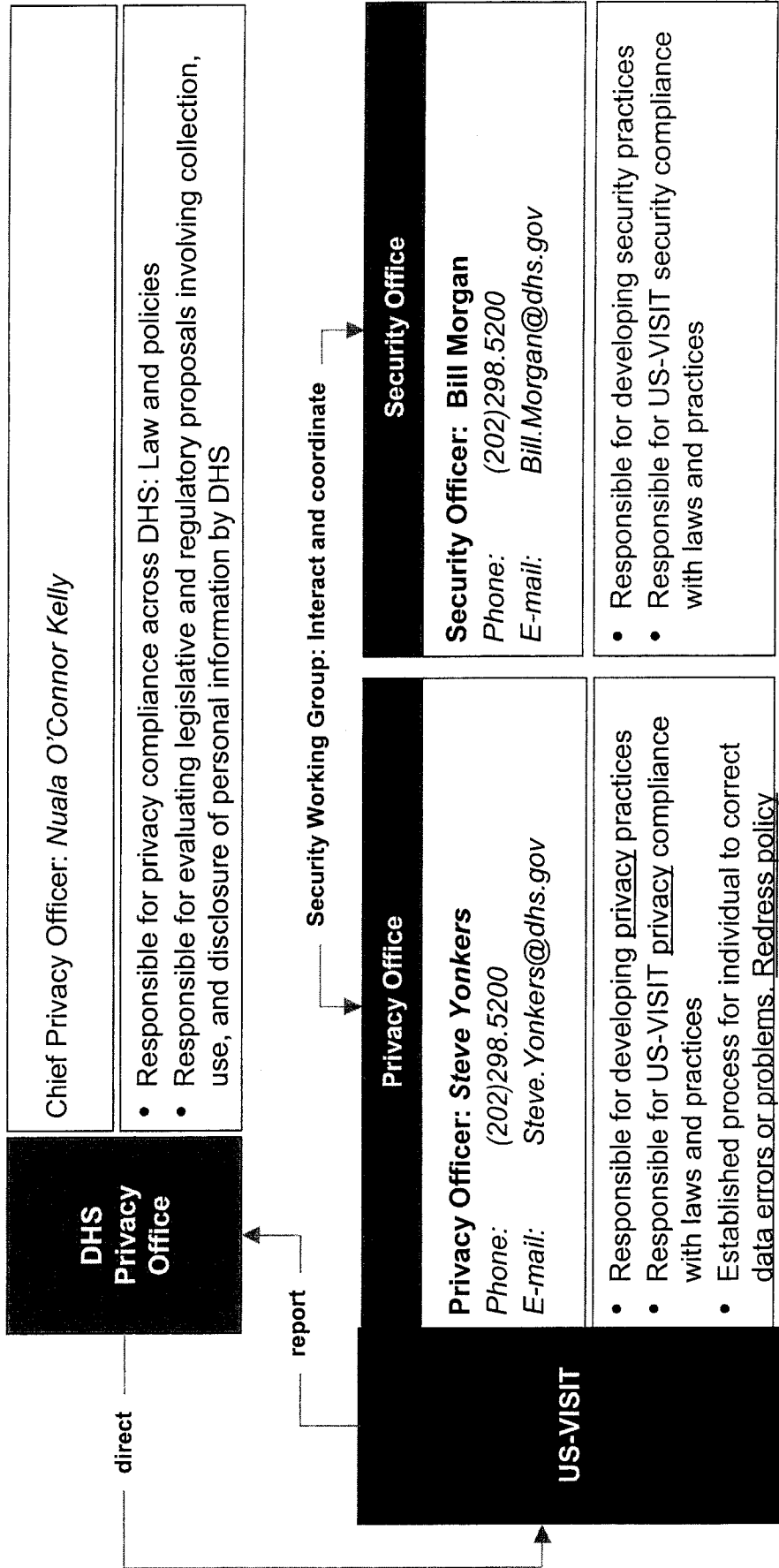
- Processed over 14 million passengers at air and sea ports of entry since January 5, 2004
- Passengers find it convenient, fast and non-intrusive
- As of December, over 330 criminals and individuals with immigration violations have been detected, detained, and/or denied entry.



Homeland
Security

US-VISIT Privacy Organization

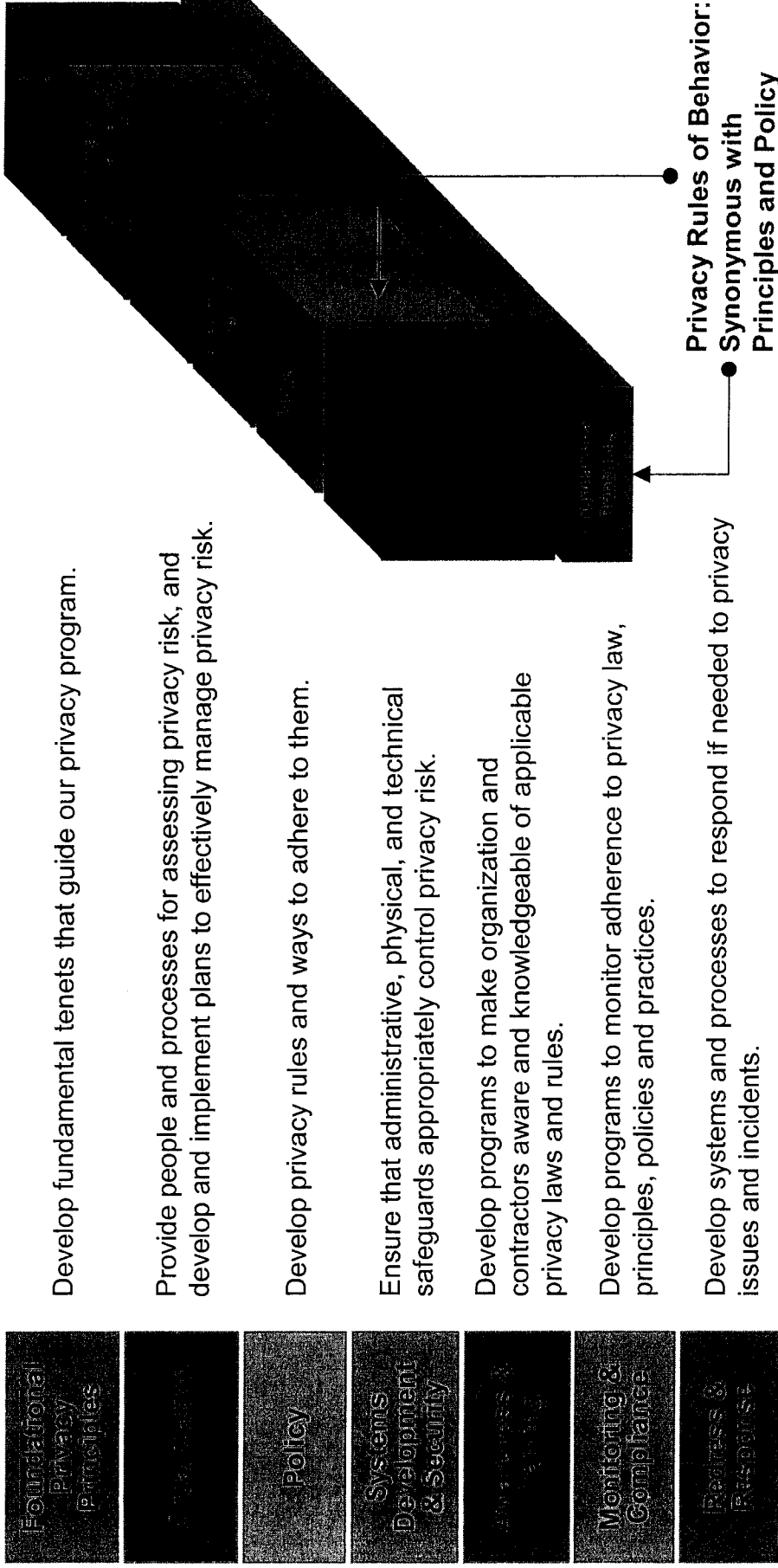
Key privacy-related responsibilities and interactions



Homeland Security

US-VISIT Privacy Program

Key elements and responsibilities



**Homeland
Security**

US-VISIT Commitment to Privacy

We are respectful and protective

Our beliefs: mission and principles

US-VISIT Privacy Office Mission Statement

We uphold the privacy of individuals while protecting our national borders. We do this by adhering to the letter and spirit of privacy law and complying with fair information practices, by treating individuals and their personal information with respect, and by ensuring a high standard of privacy protection.

Privacy Principles*

- | | |
|--------------------------------------|--|
| 1. Responsibility and Accountability | 6. Limiting Collection, Use, Disclosure, and Retention |
| 2. Privacy Awareness and Training | 7. Strict Confidentiality |
| 3. Openness and Redress | 8. Data Integrity |
| 4. Identifying Purpose | 9. Individual Access |
| 5. Informed Consent | 10. Security |

* Blend of U.S.⁶, Canadian¹¹ and European¹² privacy principles; one-slide definition of Principles appears in [Appendix A](#).



**Homeland
Security**

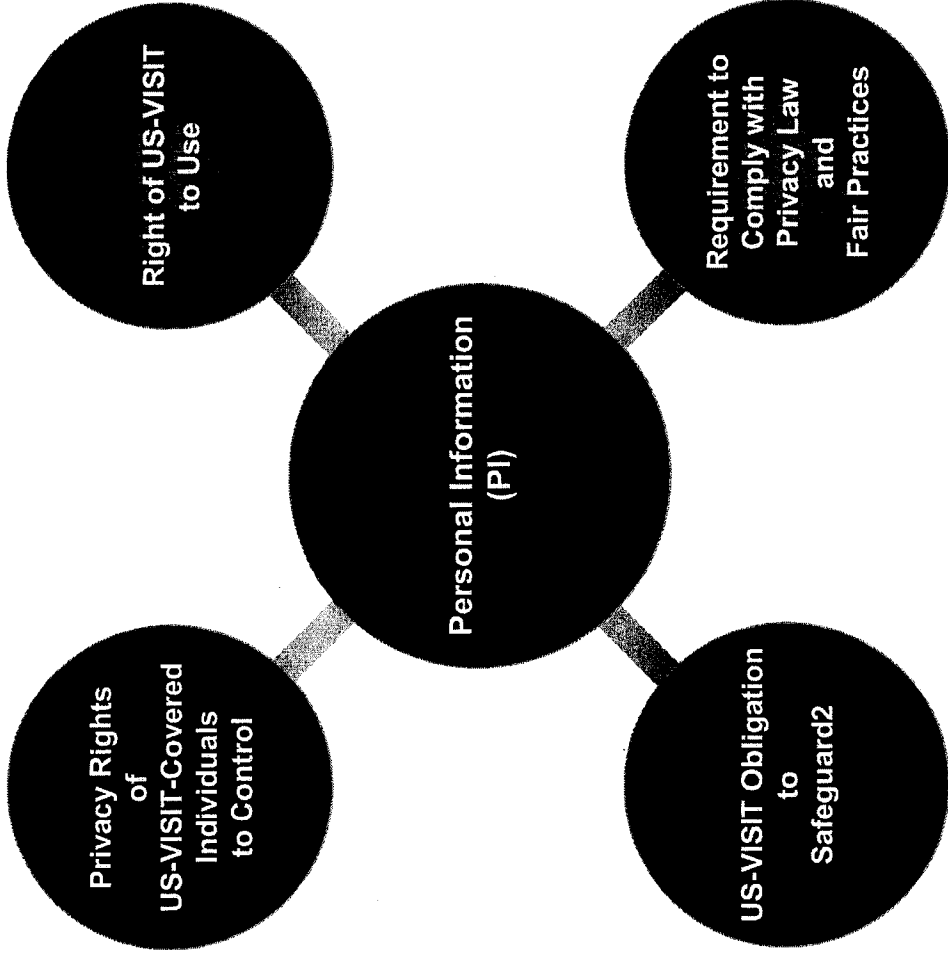
Redress Policy

- US-VISIT's Chief Privacy Officer established a redress process that provides a fast and convenient way for visitors to review the accuracy and completeness of their travel records.
- As of December, only 50 foreign visitors have inquired about their records.



Homeland
Security

Required Balancing Act



Homeland
Security

Privacy Rights and US-VISIT

<p>Privacy Rules of Behavior</p>	<ul style="list-style-type: none"> • US-VISIT privacy compliance requirements—principles, policies, and practices—that establish a high level of privacy protection that: <ul style="list-style-type: none"> – builds trust, and – is consistent with U.S. and international privacy standards.
<p>Covered Individual</p>	<ul style="list-style-type: none"> • An individual covered under the US-VISIT program: most foreign visitors traveling to the U.S.
<p>Personal Information</p>	<ul style="list-style-type: none"> • Information about a covered individual under the custodianship of the US-VISIT program. <ul style="list-style-type: none"> – Managed as sensitive but unclassified (SBU) information that is For Official Use Only (FOUO). – Confidentiality must be maintained.
<p>Confidentiality</p>	<ul style="list-style-type: none"> • Assurance that information is not disclosed to unauthorized entities (people, processes, or devices).
<p>System of Records</p>	<ul style="list-style-type: none"> • A grouping of personal information under the control of an agency from which information is retrieved by the name of the individual or a unique identifier assigned to the individual. <ul style="list-style-type: none"> – <u>The US-VISIT program does not currently have its own system of records.</u>



Homeland Security

Public Privacy Promises

Limit Collection of Personal Information	<ul style="list-style-type: none">• We collect only the personal information—biographic, travel information, and biometric identifiers (fingerprints and a digital photograph)—required for stated purposes.
Limit Use of Personal Information	<ul style="list-style-type: none">• We use personal information only to:<ul style="list-style-type: none">– Verify identity– Confirm compliance with terms of a covered individual’s admission to the U.S.– Enforce law and maintain national security– Meet other purposes specifically authorized or mandated by law
Limit Access and Disclosure of Personal Information	<ul style="list-style-type: none">• Disclosed only to those authorized by law and in the performance of official duties<ul style="list-style-type: none">– Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and Transportation Security Officers of DHS and Consular Officers of the DOS, <u>as well as foreign and domestic law enforcement agencies.</u>• Disclosed only in accordance with applicable law, regulation and US-VISIT policies, procedures, and practices.
Appropriately Secure Personal Information	<ul style="list-style-type: none">• We protect personal information.
Retain Personal Information Only As Long As Absolutely Needed	<ul style="list-style-type: none">• Personal information collected by US-VISIT will be retained and destroyed in accordance with applicable legal and regulatory requirements.



**Homeland
Security**

Comply with Letter and Spirit of Law

High-level summary of privacy requirements in select laws:

Privacy Act (PA)⁵

- Establishes how agencies (in executive branch of federal government) gather, maintain, and disseminate personal information
- Essentially implements privacy principles known as Fair Information Practices (FIPs): Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, Enforcement/Redress⁶ (US-VISIT privacy principles are adaptation of FIPs)
- Only applies to records kept about individual U.S. citizens and lawfully admitted permanent resident aliens in a “system of records”
- Allows individuals to access personal information about themselves subject to exemptions and conditions of disclosure

Freedom of Information Act (FOIA)⁷

- Provides the right for anyone to request access to federal agency records and information
- Disclosure is subject to exemptions and exclusions

E-Government Act of 2002⁸

- Promotes and guides federal agencies' use of Internet-based information technology
- *Privacy Provisions* (section 208) and OMB guidance⁹ require federal agencies:
 - To conduct Privacy Impact Assessments (more on next slide)
 - Post Web site privacy policies in both statement and machine-readable form



Homeland Security

Conduct Privacy Impact Assessments (PIAs)

What	<ul style="list-style-type: none">• PIA is an assessment of actual or potential impacts—including social and ethical—that a system may have on privacy and the ways in which any adverse impacts may be mitigated.
Requirement	<ul style="list-style-type: none">• Section 208—Privacy Provisions—of the <u>E-Government Act</u> requires all federal agencies to complete PIAs for new or substantially modified information systems that handle personal information.
OMB Guidance	<ul style="list-style-type: none">• <u>What</u> information is to be collected• <u>Why</u> the information is being collected• <u>Intended use</u> of the information• <u>With whom</u> the information will be <u>shared</u>• <u>What opportunities</u> individuals have to decline to provide information or <u>consent</u> to particular uses of the information• How the information will be <u>secured</u>• <i>Whether a system of records is being created under the Privacy Act</i>• Analysis of <u>choices an agency made</u> regarding an IT system or collection of information• <u>Information lifecycle analysis</u>



Contact Us for More Information

Steve Yonkers, Privacy Officer

steve.yonkers@dhs.gov

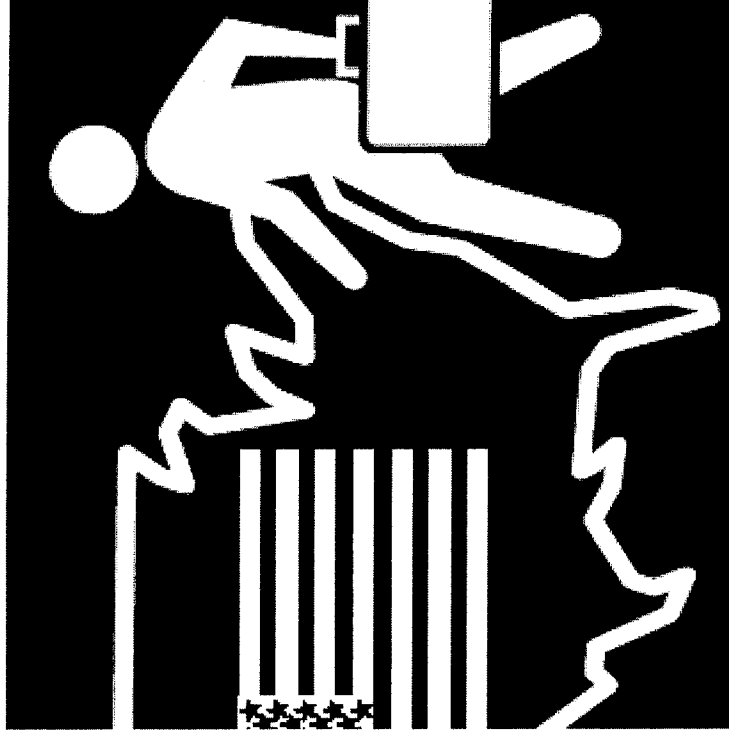
Anna Hinken, Outreach Director

anna.hinken@dhs.gov

Phone: 202-298-5200

Web site:

www.dhs.gov/us-visit



**Homeland
Security**