Homeland Security

Cybersecurity & Privacy

Privacy at DHS

DHS empowers its programs to succeed by integrating privacy protections from the outset. The DHS Privacy Office is the first statutorily mandated privacy office in the Federal Government, and serves a unique role as both an advisor and oversight body for the Department.

DHS views privacy as more than just compliance with privacy law and policy. Privacy at DHS is also about public trust and confidence, and how the government acts responsibly and transparently in the way it collects, maintains, and uses personally identifiable information (PII).

DHS employs a layered approach to privacy oversight for the Department's cybersecurity activities. It starts with the Chief Privacy Officer and extends through NPPD's Senior Privacy Officer and dedicated privacy staff across the Department.

The Fair Information Practice Principles

DHS uses the Fair Information Practice Principles (FIPPs) to guide and inform the design, deployment, compliance, and oversight of all its programs and technologies. In 2008, DHS formalized these principles as department policy:

1. **Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII.
2. **Individual Participation:** DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
3. **Purpose Specification:** DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
4. **Data Minimization:** DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
5. **Use Limitation:** DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
6. **Data Quality and Integrity:** DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
7. **Security:** DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing:** DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

These principles were also adopted as part of the National Strategy for Trusted Identity in Cyberspace (NSTIC) and the 2013 Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

Transparency

DHS publishes its Privacy Impact Assessments (PIAs), Privacy Compliance Reviews (PCRs), and other reports on www.dhs.gov/privacy, the DHS Privacy Office's webpage. DHS also created a separate site dedicated to the Department's cybersecurity efforts, which includes its privacy work on cybersecurity: www.dhs.gov/cybersecurity.

Homeland Security

Cybersecurity & Privacy

Privacy Impact Assessments

As part of its privacy compliance responsibilities, DHS conducts PIAs. PIAs provide an opportunity for the Department to identify privacy issues early in the development process and to build privacy protections into programs from the beginning.

DHS has conducted PIAs on all stages of the Department's EINSTEIN program as well as other cybersecurity programs:

- EINSTEIN 1, 2004
- EINSTEIN 2, 2008
- National Cybersecurity Protection System (NCPS), 2012
- Enhanced Cybersecurity Services (ECS), 2015
- EINSTEIN 3 Accelerated, 2016
- Automated Indicator Sharing (AIS), 2016
- Continuous Diagnostics and Mitigation (CDM), 2016

Each PIA describes the particular program and analyzes privacy risks according to a standard set of considerations, from data collection, use, and retention to information sharing, notice, and safeguarding.

Oversight

DHS reinforces privacy compliance through a separate oversight process to assess performance of the privacy requirements established through PIAs and PCRs. In 2012, DHS conducted a PCR on the EINSTEIN program. The PCR report is published on the DHS website: www.dhs.gov/privacy. Following recommendations from the 2012 DHS PCR, the NPPD Office of Privacy periodically conducts Privacy Oversight Reviews for PII handling for its cyber programs.

Outreach

DHS participates in a whole of government approach to securing the nation's critical infrastructure and government services. A vital part of meeting its responsibilities to serve the public is to share its work on privacy with the rest of government so that other departments and agencies may integrate privacy protections into their systems and programs.

DHS also benefits from the advice it receives from its Data Privacy and Integrity Advisory Committee (DPIAC). DHS shares the Committee's reports with other agencies and the public through its webpage, www.dhs.gov/privacy so that all may benefit from the Committee's work. Additionally, in 2009, the DPIAC formed an ad hoc subcommittee to address privacy issues related to cybersecurity, as DHS is increasingly addressing cybersecurity in ways that impact privacy.

Education

The Federal Privacy Council sponsors a semi-annual Privacy Boot Camp, open to all staff at all federal agencies. For more information, email privacy.council@gsa.gov.

Revised September 2018