



Homeland Security Advisory Council


Openness and Transparency DHS Review
Final Report

March 16, 2023

This publication is presented on behalf of the Homeland Security Advisory Council, Openness and Transparency DHS Review Subcommittee, Co-Chaired by Catherine Chen and Noah Bookbinder to the Secretary of the Department of Homeland Security, Alejandro N. Mayorkas.



Catherine Chen, Co-Chair
Chief Executive Officer
Polaris



Noah Bookbinder, Co-Chair
President and CEO
Citizens for Responsibility and Ethics in
Washington (CREW)

This page is intentionally left blank.

TABLE OF CONTENTS

| | |
|--|----|
| OPENNESS AND TRANSPARENCY DHS REVIEW SUBCOMMITTEE | 5 |
| HOMELAND SECURITY ADVISORY COUNCIL STAFF | 5 |
| EXECUTIVE SUMMARY | 6 |
| METHODOLOGY | 8 |
| KEY FINDINGS | 9 |
| RECOMMENDATIONS | 13 |
| APPENDIX 1: TASKING LETTER | 22 |
| APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES | 28 |

OPENNESS AND TRANSPARENCY DHS REVIEW SUBCOMMITTEE

| | |
|----------------------------------|--|
| Noah Bookbinder, Co-Chair | President and CEO Citizens for Responsibility and Ethics in Washington (CREW) |
| Catherine Chen, Co-Chair | Chief Executive Officer Polaris |
| Cheryl Andrews-Maltais | Chairwoman Wampanoag Tribe of Gay Head Aquinnah |
| Allison Grossman | Managing Director, Campaigns and Policy Polaris |
| Carie Lemack | Co-Founder Zed Factor Fellowship |
| Adam Rappaport | General Counsel and Senior Advisor of CREW |
| Wendy Young | Managing Director, Campaigns and Policy Polaris |

HOMELAND SECURITY ADVISORY COUNCIL STAFF

| | |
|--------------------------------|---------------------------|
| Rebecca Kagan Sternhell | Executive Director |
| Alexander Jacobs | Senior Director |
| Joseph Chilbert | Senior Director |
| Carley Bennet | Intern |

EXECUTIVE SUMMARY

The Department of Homeland Security has long sought to adhere to the principles of transparency and Open Government laid out in the 2009 Presidential Memo on Transparency in Government and the follow-on Open Government Directive from the Office of Management and Budget. The Department has recognized that expanded access to research data and information can further research collaboration and cultivate success in meeting the nation's homeland security challenges, and that government-wide, the principles of Open Government help to promote transparency, fight corruption, energize civic engagement, and leverage new technologies.

Balancing the principles of openness and transparency with the responsibilities of keeping Americans safe and enforcing the law, which have historically been seen to benefit from secrecy, can present challenges. Despite these challenges, greater openness and transparency is important to building the bonds of trust that DHS holds with the public it serves and can help secure the cooperation necessary for the Department to successfully perform its mission and keep America safe. Recognizing these important benefits, the Secretary of Homeland Security identified the advancement of openness and transparency as a priority for the Department. The Department seeks to deepen openness and transparency through improved data transparency, robust external communication, better information sharing with stakeholders and the public, systems innovation, and leadership modeling.

In particular, the Secretary set the following tasking:

1. Recommendations on how the Department and its components can expand on the foundation set by previous Open Government Plans for DHS.
2. Recommendations on new initiatives to increase transparency and sustain the Department's mission to protect the homeland.
3. Recommendations on how the Department can be held accountable in meeting its commitment to leadership in governmental openness and transparency.

The Subcommittee met with leaders and subject matter experts from the Department and an outside expert. Several themes emerged from the briefings. While DHS components are committed to providing transparency and have made significant progress in recent years, resources have not kept pace with skyrocketing demand for information and data. Common difficulties surrounding the Freedom of Information Act include significant backlogs, increasing requests, insufficient personnel, and inefficient data management systems. Similar resource concerns affect other Department functions related to transparency, including data-focused offices. New technologies provide opportunities for greater openness and building trust, but also present challenges in terms of resources, training, and applicable law. Immigration detention facilities are sometimes beset with processes that can limit transparency and large contracts that can restrict DHS's ability to efficiently access and share timely information. Overall, recent improvements and a renewed commitment to openness provide significant opportunities to continue building a culture of transparency that will enhance the Department's

effectiveness in its core mission.

This report outlines the five specific recommendations that the Subcommittee believes can help DHS improve its commitment to transparency and Open Government.

- 1) **Provide increased and well-targeted resources for openness and transparency efforts to advance DHS's mission to safeguard the American people and the homeland by building community trust and supporting increased cooperation with the agency.** This includes resources for increased staffing for offices that can be most effective in spurring Department-wide transparency and those that face the most demand, for development of key policies and processes to promote openness, and for responding to challenges and opportunities for transparency from new technologies.
- 2) **Implement targeted increased training and continue to develop a Department-wide culture of transparency.**
 - a) Continue to develop a culture of transparency by reinforcing a Department-wide vision for how openness and transparency makes the nation more secure, including by continued leadership by example from DHS's top levels, and further opportunities for leadership and frontline staff to exchange experiences.
 - b) Ensure comprehensive training to develop large-scale compliance with new records retention policies related to text messaging and continue to deploy technology that satisfies convenience and security needs while complying with records retention requirements.
- 3) **Use data and technology to increase transparency and build trust.**
 - a) Build greater trust with the public through timely and proactive disclosure of performance data and core design principles that are under consideration in the deployment of new technology.
 - b) Prioritize user-centered design that ensures accessibility for marginalized and vulnerable communities, non-English speakers, and populations with low technology literacy and/or access as a core part of any platform or application development.
 - c) Continue to prioritize and appropriately resource the digitization of A-Files for all new applications and for those applications currently in immigration proceedings.
 - d) Prioritize streamlining policies and laws to provide FEMA and other disaster assistance agencies more speed and flexibility in emergencies.
- 4) **Establish an alternative system for making and responding to first-person requests in a more timely way than through the Freedom of Information Act for, at a minimum, records that affect an individual's eligibility for benefits or adversely affect an individual in proceedings.** Engage an appropriate expert (internal component or contractor) to assess DHS's first-person requests and make recommendations for the design and implementation of an alternative system.

5) Further improve transparency and accountability with regard to immigration detention facilities.

- a) Prioritize monitoring, evaluation, and accountability in DHS’s oversight of immigration detention facilities, including facilities that are operated by outside contractors.
- b) Promptly publicly disclose reports documenting findings of Prison Rape Elimination Act violations, rather than waiting six months until the problem is theoretically fixed before letting those who may be affected know about the problem.
- c) Promote transparency through continuing emphasis on fewer large contracts with private entities, particularly for immigration detention facilities, and increasing government control of data management, governance, and security.

METHODOLOGY

The Subcommittee conducted expert interviews and supplemental research from November 2022 to February 2023. The Subcommittee met with representatives, subject matter experts and leaders from U.S. Customs and Border Protection (CBP), the Federal Emergency Management Agency (FEMA), the DHS Chief Information Officer (CIO), Office of the Chief Human Capital Officer, the DHS Office of the General Counsel (OGC), DHS Privacy Office, U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), U.S. Secret Service (USSS), the DHS Office of Public Affairs (OPA), and the nonprofit sector. Each leader and representative provided updates and overviews of their transparency and open government efforts.

The recommendations developed by the Subcommittee were based on the following criteria:

1. Efforts that can tangibly improve efficiency, clarity, and access to information as a means to build trust and support for the agency’s mission and operations.
2. Transformative measures and structural changes that could reduce the load on Freedom of Information Act (FOIA) and otherwise facilitate greater openness.
3. Practical and technological improvements already underway in parts of the organization that could be enhanced, amplified, sped up, or otherwise supported to promote greater transparency.
4. Initiatives that integrate the values of transparency, openness, and accountability with the strategic mission of the agency.
5. Other dominant themes that emerged from the conversations.

KEY FINDINGS

General Themes

- The Department has introduced significant initiatives on openness and transparency in recent years including introducing the position of Chief Data Officer, prioritizing reducing FOIA backlogs, developing new records retention policies, creating a forthcoming independent Office of Homeland Security Statistics, and emphasizing openness and transparency as values of the Department.
- Multiple components emphasized the need for additional resources for headquarter offices focused on data and transparency and for FOIA offices and other transparency-focused offices to address significant demand. The demand for information from DHS is significantly greater than that for much of the rest of the government and is growing consistently. Resources have not increased at the same rate.
- Many of those the Subcommittee spoke with observed that the Department has many competing resource needs and that it will be important for those inside and outside of DHS to appreciate that investments in openness and transparency will help establish community trust and buy-in that in turn will strengthen the Department's ability to fulfill its core security missions.
- Many DHS offices and components are engaged in finding the balance between their mission and the mandate for transparency and finding the ways that transparency can complement their mission.
- Components of DHS focused on security and law enforcement have appropriately in the past limited access to information as a necessary tactic to accomplish their missions. Incorporating the principles of openness and transparency and understanding the ways in which those principles can actually help the security mission can take time. DHS leadership's emphasis on the principles of openness and transparency and modeling through clear policies and personal engagement help this transition.

Openness and Customer Service

- Openness and transparency are a key part of customer experience. Additional resources and tools are essential for the larger enterprise mission to achieve openness and customer service.
- DHS has set expectations that senior leaders will understand the experience of DHS's customers and the need for accessible and easy-to-use services. Senior leaders are encouraged to spend an hour watching someone try to fill out a form or interact with the service of their agency. Other customer service efforts across the Department include holding public listening sessions, building interactive data dashboards for the public, implementing language accessibility obligations, digitizing request submissions and account services, and ensuring a shared understanding of required and relevant travel documents for asylum seekers and refugees.

- There are restrictions on what can be communicated in public statements regarding ongoing investigations, making it difficult for the Department to be transparent on certain issues. Some departments have a policy not to comment on materials marked Law Enforcement Sensitive (LES) or For Official Use Only (FOUO). Disclosure of disciplinary actions is subject to restriction set forth in specific union agreements.

Digital Solutions and Data Management

- The Office of the Chief Data Officer (CDO) plays a central role in DHS transparency efforts through oversight of data operations, geospatial dataset management, and records management.
- Performance metrics could be a helpful way to view the correlation between transparency and operational impact, especially when it comes to budgetary support.
- Regarding digitization of an identity, DHS is operating under an NDAA-mandated clock to issue guidelines on acquisition and use of AI in the department. The public does not always understand the steps the agency is taking to ensure the protection of privacy, personal information, and civil liberties.
- There are rigorous standards throughout the organization around assessment for algorithmic effectiveness to make sure bias is limited and to build in protections for the individuals with whom DHS interacts. That involves careful incorporation of privacy and civil rights and civil liberties considerations as policies and processes are developed, and a focus on those considerations by internal oversight offices.
- FEMA's "share by default" culture seeks to increase data sharing and access for all stakeholders. To address the challenges of information sharing, FEMA seeks a different approach to privacy compliance that allows for more rapid and flexible procedures during disasters, while still complying with existing policies. For example, FEMA is responsible for consolidating 75 aid programs from 14 different federal agencies into one application process, potentially requiring the negotiation of 14 computer matching agreements under the Privacy Act and a series of systems of records notices and Paperwork Reduction Act collections.
- The Department's interagency effort to digitize new A-Files from the point of border apprehension will make it easier to be transparent and accessible to stakeholders including by allowing files to be proactively available to non-citizens. Digitization will also drastically reduce FOIA requests across multiple components. The Department's goal is to digitize A-Files moving forward, not to digitize existing paper A-Files.

Detention and Related Issues

- ICE facility inspection programs have two units that oversee their inspections and audits. Typically, an inspection takes one week and includes a visit, briefing, tour, and review of documentation. Once the inspection is completed, the inspectors gather facts and findings and draft a report. The report is posted in the FOIA library within 60 days,

unless there's a corrective action. In that case, the report only needs to be posted within 180 days to give the contractor the opportunity to correct the problems, and only the corrective action is posted. As a result, some reports are not released while action is needed.

- Over the past decade, there was a reliance on big contractors to develop information technology systems, which tended to work less well and meant less government control over the systems and all information they contained. The solution to the issues created by these large contracts was to bring in significantly increased technical capacity on the federal side so the federal government could develop and own major IT systems. The USCIS's transformation program is a great example of this. The system called Electronic Immigration System (ELIS) is their attempt to digitize benefits and forms processing.
- This shift provides for more openness and transparency because these new systems are developed with open architecture that gives the government more ability to own and operate its own systems and makes it much easier for the government to publish open data, respond to oversight requests, and be open with their work.
- Some of the problems with large contractors have been particularly apparent in the immigration detention context with private prison companies. Particularly in the immigration detention context, there is a need to shift from an older model of government relying on large contractors providing systems integration toward government acting as the integrator of its own IT solutions. More government control of IT systems will allow for significantly enhanced service delivery and improved responsiveness to requests for information. DHS contracts involving IT could be structured so that the department owns the code and has access to all data in a timely manner.
- DHS now has an IT acquisition review process where every contract that involves IT goes through a review by appropriate offices to ensure that data will be protected, but programmatic contracts that involve IT even if less directly, such as for medical services at the border, should prioritize attention on data security and IT elements.

FOIA

- DHS operates the largest FOIA program in the federal government. It is responsible for handling more than half of FOIA requests filed across the government. In FY 2022, DHS received approximately 520,000 FOIA requests, an increase of nearly 90,000, and processed about 500,000 requests.
- The vast majority of those are "first-person" requests from individuals seeking information about themselves that was previously submitted to the government or records that document their interactions with agency officials.
- Like past years, more than 98% of the received requests in FY 2022 were directed to CBP, ICE, USCIS, and the Privacy Office.
- DHS reached a decade-low backlog in FY 2021. DHS's backlog of FOIA requests is expected to grow in FY 2022 by approximately 25,000 requests, to about 50,000. CBP,

ICE, and USCIS account for more than 95% of DHS's backlog growth.

- USCIS has the largest FOIA program in the federal government, receiving approximately 25% of all FOIA requests government wide. USCIS has significantly reduced its A-File request backlog since 2020 and eliminated the backlog for requests from individuals in immigration proceedings.
- CBP is struggling to work through its backlog. FOIA requests roughly doubled from FY 2016 to FY 2022, to more than 132,000 requests. The backlog has increased from 1,172 in FY 2016 to 27,597 in FY 2022. CBP's litigation portfolio also has increased significantly, by about 85%. Staffing has not kept up with the growth in requests: CBP's FOIA office had 52 employees in FY 2016; it had 53 in FY 2022. While the FOIA office has received new technology, it has not sufficiently addressed staffing shortages. A third party found that CBP's FOIA office is understaffed by 50 employees.
- Requests for video footage from body-worn cameras is consuming an increasingly large amount of FOIA processing time for DHS and is likely to continue growing significantly soon. The need for frame-by-frame redaction makes processing challenging and time-consuming.
- DHS faces a significant challenge from requests for body-worn camera footage. Those requests have increased 50% in one component, and processing them requires training, different technology, and time. However, no additional funding has been provided for this work. A suggestion from the briefings was that cost savings and efficiency might be realized if DHS studied technology for processing video footage, determined which tool works best, and implemented it Department-wide.
- Agencies are increasingly posting documents to their electronic reading rooms. In FY 2022, USCIS published 168 items to its reading room, and TSA posted over 45,000 pages. ICE posted documents such as detention facility contracts and inspection reports.
- DHS is developing a set of targeted transparency engagements with internal and external stakeholders to create a foundation for the action plan to complement the Secretary's priority on openness and transparency. Components of this plan include standardizing FOIA websites and reading rooms, engaging with stakeholders to develop a policy requiring proactive disclosure of certain types of records, and transitioning to a modernized processing system that will include integrated e-discovery tools.
- Several components noted the value of e-discovery tools for processing FOIAs.
- Some non-DHS agencies have created alternative systems for individuals to access records about themselves, including DOJ's Executive Office for Immigration Review for records of immigration proceedings and the IRS for an individual's tax transcript.

Records Retention

- The Department developed last summer and fall, culminating in a memorandum approved by the Secretary in September, an improved series of policies for retention of electronic messages that included new more thorough policies and procedures for the

retention of messages from any departing senior employees, new guidance and training on records preservation and retention, and a move toward automated archiving of messages.

- On March 1, 2023, DHS disabled iMessage on Department-owned devices to ensure compliance with records retention policies because iMessage does not allow automated archiving of messages.
- iMessage is convenient and more secure than most other platforms, so there is a need to look for other platforms that will comply with records retention needs while successfully fulfilling the Department's security needs.
- These new policies and technological fixes do not necessarily stop employees from using Signal or iMessage, which do not comply with records retention policies, on their personal devices, and iMessage is sometimes still permitted for international travel.
- More training and education to make sure people understand records retention obligations will help to discourage use of non-compliant applications on personal devices or to ensure compliance with the additional steps required for records retention when use of a non-compliant application is unavoidable.

RECOMMENDATIONS

1. Increase Resources for Openness and Transparency

Provide increased and well-targeted resources for openness and transparency efforts to advance DHS's ultimate mission to safeguard the American people and the homeland by building community trust and supporting increased cooperation with the agency. Amongst all of the Subcommittee's briefings, one theme was abundantly clear – the need for more resources to support the call for increased openness and transparency. In the past decade, the availability of new technology for capturing data and facilitating sharing with the public as well as increased interest in DHS's records and data has stressed an already overloaded system. There was unanimous desire from components and outside experts for increased resources to support the growing demand for information flow.

It is clear there is a need for resources throughout the Department. Areas of acute need include headquarters components that can set the tone for the Department on openness and FOIA offices for those components that experience exceptional FOIA demand and have not had the resources to keep up. The limited resources these offices have are already stretched thin, and with the increase in data collected by DHS and in public awareness of and ability to request this data, these offices' abilities to perform their duties have been hampered despite major efforts to deliver transparency and bring down backlogs. The Department should also request increased resources in areas where significant increases in information requests are likely, such as components implementing body worn cameras.

DHS includes “respect” as a core value, which calls for valuing the relationships DHS builds with stakeholders. DHS also has a guiding principle to uphold privacy, transparency, civil rights, and civil liberties. Providing sufficient resources for those efforts is critical to upholding the values and principles. Moreover, openness and transparency builds trust among the people with whom the Department interacts. That trust will help foster the cooperation DHS employees need to effectively do their jobs, helping the Department better achieve its core missions. The Department should consider reallocating funds internally to the extent permitted by law to ensure these priorities are sufficiently supported, while also requesting additional resources for openness and transparency in the President’s annual budget request to Congress. The request in the President’s FY 2024 budget for substantial new funding for openness and transparency work at DHS is a significant step in that direction. With resources scarce and mission-critical needs many, it will be crucial for Department leadership to communicate both to Congress and within DHS how resources for openness and transparency help the Department perform its core duties.

Specifically, the Department should request funding for the following areas most in need of additional resources:

- **Increased staffing to keep up with FOIA demand** across components, targeted dynamically to the offices where the effect can be greatest and the components where the need is greatest.
- **Increased funding for offices responsible for data transparency** including the Office of the Chief Information Officer and the Office of Homeland Security Statistics.
- **Determining best practices for disclosing information** without harming vulnerable populations.
- **Creating more resources for proactive disclosure of information**, which builds trust and in the long term reduces information requests and litigation.
- **Proactively resourcing for the anticipated increase in information requests stemming from the implementation of body worn cameras**, including:
 - Hiring within CBP, US Secret Service and other components to address FOIA needs specifically from body cameras.
 - Procuring Department-wide technology for body cameras, including camera redaction, that is most efficient for responding to requests.
- **Developing a better, more current e-discovery system** for FOIA and litigation.

2. **Implement Training and Continue to Develop a Culture of Transparency**

DHS personnel are under pressure every day to uphold laws, increase security, and provide a sense of safety while also attempting to win the public’s trust, help individuals in vulnerable and desperate circumstances, thwart criminals, terrorists and violent extremists, navigate a complex political landscape, and welcome the world to the United States.

DHS increasingly views transparency and public engagement as a key tool for promoting security goals. Components of DHS focused on security and law enforcement view limiting access to information as a necessary tactic to accomplishing their missions. This tactical approach can at times conflict with the goal of transparency. For example, some DHS

components have policies not to comment on materials marked Law Enforcement Sensitive (LES) or For Official Use Only (FOUO) even when the public is already aware that those materials may exist.

To fulfill its mission, DHS would benefit from reinforcing a Department-wide vision for how openness and transparency makes the nation more secure. Openness and transparency increase public trust, which in turn increases community cooperation, which strengthens operational security and missions. Connecting the security mission with transparency will set the tone for an ongoing evolution of DHS's culture.

Leading by example is a crucial part of instilling a culture of openness and transparency, and the Secretary's focus and public emphasis on openness and transparency has helped foster progress throughout the Department. DHS leadership should continue to demonstrate their commitment to openness and transparency to set the example for their respective bureaus and agencies to emulate. That can include leadership implementing clear policies on transparency, as the Secretary has done on issues like records retention, and demonstrating personal adherence to those policies.

Education, training, and intentional exposure to the daily considerations faced by DHS staff and leaders can help to build a more cohesive one-DHS culture of transparency for security. Facilitating more opportunities for Department leadership and frontline/public-facing staff to exchange experiences could support this effort.

The Department should ensure comprehensive training to develop large-scale compliance with new records retention policies related to text messaging, and continue to deploy technology that satisfies convenience and security needs while complying with records retention requirements. Records retention, including with technologies like text messaging, is important for building public trust, which in turn breeds increased public cooperation and partnership with the Department's components. The destruction of records, even when inadvertent, can lead to distrust, which can hamper DHS's mission. Recognizing this, the Department, at the Secretary's direction, has implemented significantly improved records retention policies in the past year, particularly with regard to text messages, including implementing a comprehensive process to ensure that messages are preserved when senior employees leave the Department and starting to put into place automated archiving of messages sent and received on government phones. DHS has also taken technological steps to increase compliance with those policies, including removing iMessage from Department-owned phones since iMessage will not allow automated archiving of messages.

DHS can build on these important improvements by implementing comprehensive training to ensure employees are aware of the new policies and will not use platforms, including on personal devices, that are not in compliance with the new policies. Employees, without realizing that they could be violating the new policies, may be tempted for the sake of convenience to use applications like Signal or iMessage on their personal phones; clear training not only about what the policies are, but why they are important to DHS's mission, can help to discourage this behavior. The process to ensure that all messages are archived before an employee departs also depends heavily on education to ensure that employees understand why compliance matters and

take the steps necessary to do so even during offboarding, which can be a hectic time. While training is a component of the policies approved last year, leaning into training and education will help to ensure their success.

DHS should also continue looking for technologies that comply with the new retention policies while satisfying key security and convenience needs for employees, so employees are not tempted for mission-specific reasons to seek out and use non-compliant technology. The Department should also ensure that the review process for new technologies includes a review of those technologies' records management capabilities; components should not approve technological applications that work well in other respects only to realize after the fact that they may not comply with current records retention policies. A focus on finding technologies that satisfy both operational and records retention needs will help encourage compliance and make achieving openness goals easier.

3. Use Data and Technology to Increase Transparency and Build Trust

The Department's application of technology to increase efficiency, increase simultaneous access to essential documents, and improve the customer experience for applicants directly contributes to DHS's openness and transparency goals, and helps to build greater confidence in immigration processes, disaster response operations, and other high stakes situations that can be overwhelming to applicants.

The Department should seize the opportunity it now has to build greater trust with the public through timely and proactive disclosure of performance data and core design principles that are under consideration in the deployment of new technology. The Department is actively working to improve its data infrastructure and architecture to enable more timely releases of information sought by a variety of stakeholders. Through the creation of the new independent Office of Homeland Security Statistics, components will be able to more proactively share performance data and clarify interpretation of the data provided by the Department. This includes dashboards, explainers, trends, and more proactive transparency about politically salient issues. The agency should prioritize communicating with civil society stakeholders, media, and lawmakers about the potential presented by this new office and the schedule on which statistics will be released (e.g., weekly, monthly, quarterly, annually). Steady and reliable data releases similar to those provided by the Department of Labor's Bureau of Labor Statistics will strengthen the information ecosystem surrounding the Department's most important data.

DHS is a leader in the deployment of advanced technology at a population level to address security and improve efficiency at transit points like airports and border crossings, but the public does not necessarily understand the civil rights and civil liberties dimensions of these technologies. There is a unique opportunity to simultaneously build trust with the public and broaden buy-in for DHS's larger national security mission through proactive education and engagement about emerging technology, the measures the agency takes to protect privacy, and the policies and practices the agency uses in deploying facial recognition technology or artificial intelligence while safeguarding safety and privacy.

The Department should prioritize user-centered design that ensures accessibility for marginalized and vulnerable communities, non-English speakers, and populations with low technology literacy and/or access as a core part of any platform or application development, especially considering the population that so frequently comprises DHS’s customer base. The Subcommittee learned of instances where civil society groups are building user guides to help low tech-literate communities access DHS platforms. This user-centered approach should be owned by DHS in the development of these systems in order for the public to more easily access DHS information.

The Department should engage with the following stakeholders in these efforts (this list is not exhaustive): Primary applicants, family members, the immigration bar and stakeholders who use DHS systems regularly, scholars and academics who have studied these systems, technology companies, community leaders, advocacy organizations, local and tribal governments, and country of origin governments. Continued engagement with these communities to ascertain their needs and concerns and address them as technology is developed and deployed will increase trust and buy-in in the short term and will help foster cooperation which enhances DHS’s accomplishment of its mission in the longer term, while effectively serving its stakeholders.

The Secretary should continue to prioritize and appropriately resource the digitization of A-Files for all new applications and for those applications currently in immigration proceedings. Specific attention should continue to be paid to tribal, rural, non-English speaking, and vulnerable communities to ensure equitable access to online information.

The A-File digitization strategy is an excellent example of the Department’s efforts to use technology to innovate toward greater openness and transparency. The Subcommittee applauds the Department’s ongoing work to digitize documents that have traditionally required paper processing, including the work to digitize current and new A-Files. As documented in the [2020-2023 FOIA Backlog Reduction Plan](#), the vast majority of FOIA requests are for A-Files and other immigration related processes handled by USCIS, CBP and OBIM. Digitization will reduce the burden on FOIA offices, increase efficiency, reduce the need for paper file storage, and help ensure applicants can access their own information in a timely manner.

To help realize some of the opportunities offered by technology, DHS and the Secretary also should prioritize streamlining policies and laws to provide FEMA and other disaster assistance agencies more speed and flexibility in emergencies. In the aftermath of a disaster, there is an urgent need to help impacted communities. To best provide that assistance, disaster assistance agencies need to be able to share information quickly and seamlessly. Processes mandated by federal law, however, often hinder these efforts. In particular, the Privacy Act of 1974 and the Paperwork Reduction Act of 1980 impose regulatory burdens that delay information sharing. Under the Privacy Act, for example, FEMA must have a computer matching agreement before it can share information with another federal agency, and that agreement must be renegotiated or extended for every disaster, which requires publishing a public notice in the Federal Register.

Sharing information is especially important considering FEMA’s efforts to consolidate into a single portal application for multiple assistance programs at various agencies. Under the current

system, that potentially requires FEMA to negotiate numerous computer matching agreements and issue a myriad of other privacy and paperwork-related notices. Federal law has not kept up with technological advances, and a different approach to privacy compliance is needed.

Making modest changes to federal law is the best way to cut through this regulatory thicket and streamline information sharing. Bills that would address this issue by largely exempting data sharing between disaster assistance agencies from the Privacy Act and the Paperwork Reduction Act – like the Disaster Survivors Fairness Act – have made progress in Congress but have not yet passed.

DHS should make passage of this legislation a high priority. In addition, to the extent possible, DHS and FEMA also should make any policy and regulatory changes that would ease these burdens.

4. Establish an Alternative System for First-Person Records Request System

DHS receives and responds to more Freedom of Information Act (FOIA) requests than any other federal agency. The vast majority of those are “first-person” requests from individuals seeking information about themselves that was previously submitted to the government or records that document their interactions with agency officials, like an individual’s Alien File (A-File). Requesters often need these records for personally critical and time-sensitive reasons, such as defending themselves against removal and applying for immigration benefits.

FOIA was not designed for first-person requests, and it is a poor fit for them. FOIA’s primary purpose is to foster transparency and accountability by helping citizens know what their government is up to and shedding light on an agency’s performance of its duties. First-person requesters, however, usually have no alternative for obtaining records they need, and the heavy volume of these requests clogs the FOIA pipeline and severely strains DHS’s ability to respond to all requests.

As a result, requesters have often faced long delays in obtaining records about themselves, as have journalists, researchers, advocates, and others seeking records needed for transparency and accountability. The Subcommittee recognizes that DHS has reduced the size of its FOIA backlog in recent years and responded to requests more quickly, and the Subcommittee credits the hard work and innovations that went into this progress. But with ever-increasing requests, the backlog is again growing at some agencies, and DHS’s progress is no guarantee it will be able to provide timely responses in the future.

To help address these issues, DHS should establish an alternative system for making and responding to first-person requests in a more timely way than through FOIA for, at a minimum, records that affect an individual’s eligibility for benefits or adversely affect an individual in proceedings. That will allow those requests to be handled more expeditiously in a system better tailored for them, while freeing up the FOIA process for the transparency-focused requests for which it was created.

The specific details of the alternative system will require thorough research and thoughtful design that is beyond the purview and expertise of the Subcommittee. **DHS therefore should engage an appropriate expert (internal component or contractor) to assess DHS’s first-person requests and make recommendations for the design and implementation of an alternative system.** The appropriate experts should engage with internal and external stakeholders, consider ways to leverage technology and draw on a customer service model, and complete its work within 12 months.

The Subcommittee notes that some agencies have successfully created alternative systems for individuals to access records about themselves. DOJ’s Executive Office for Immigration Review recently developed a Record of Proceeding request process that allows immigrants to obtain records of their immigration court proceedings directly from those courts, rather than through FOIA. While not perfect, this system has simplified and sped up the process for obtaining these records. The IRS also implemented a new system to provide first-person requesters better and faster access to a document summarizing their tax information called a tax transcript.

Establishing an alternative system that is more effective, efficient, and responsive than the current one will require additional resources. **DHS should seek funding from Congress for this transformation and commit internal time and resources to accomplish it.**

5. Improve Transparency and Accountability with Regard to Immigration Detention Facilities

The Department’s oversight, monitoring, and evaluation of detention facilities used to house immigrants facing removal from the United States is an aspect of DHS programming that has received significant—and often critical—attention for more than two decades. It is also a program largely administered by outside contractors, which creates the possibility of greater noncompliance with two critical tools designed to protect individuals held in detention, the Prison Rape Elimination Act (PREA) and the performance-based national detention standards for which the Office of the Immigration Detention Ombudsman (OIDO) has oversight.

Steps that DHS can take to fulfill this recommendation include:

- **The Department should prioritize monitoring, evaluation, and accountability in its oversight of immigration detention facilities, including facilities that are operated by outside contractors, and increase timely transparency of that oversight process.** The Subcommittee understands that the OIDO carries responsibility for such oversight. Reporting mechanisms for violations of PREA and the detention standards must be readily accessible to those alleging noncompliance. Those held in detention should be regularly and consistently informed about complaint mechanisms and their legal rights, with full consideration of language accessibility. Detainees should also be provided access to counsel. Allegations of noncompliance must meet the highest confidentiality standards. Individuals alleging violations must be free from retaliation.

Reports of violations must be immediately followed up on by independent, expert investigators, and facilities and personnel found in violation of the standards must be held accountable and appropriately disciplined or fined.

The Subcommittee understands that contractors found in violation of PREA Standards are provided 180 days to implement a corrective action plan, and that the initial audit report revealing the violations is not made public during that time period, with only a final report posted publicly. **The Subcommittee strongly recommends that reports documenting findings of PREA violations should be promptly publicly disclosed, rather than waiting six months until the problem is theoretically fixed before letting those who may be affected by it know that the problem exists at all.** Moreover, with agencies on three (facilities not deemed low risk) or five (facilities deemed low risk) year audit cycles, the audit process should be reinforced with frequent and unscheduled investigations.

- **The Department should promote transparency through continuing emphasis on fewer large contracts with private entities, particularly for immigration detention facilities, and ensuring government control of all information and data related to contracts.** Under the Secretary's leadership, the Department has appropriately begun to move away from massive contracts with private entities, particularly with regard to immigration detention, and toward smaller contracts with greater control by the Department. This trend should continue, allowing the Department significantly more ability to ensure greater transparency and accountability in connection with its contracts and particularly with immigration detention facilities than has been the case with larger contracts. With smaller contracts, the Department retains greater control of each contract and can more easily require openness from contractors, who are then inherently more accountable.

More specifically, rather than relying on large contractors to create and control information technology systems, particularly in the detention context where contractors in the past have sometimes created vast proprietary systems, the Department should instead create and control those systems when possible, giving DHS more control over information and data. When the Department creates these systems, it can better protect privacy and more easily provide information to the public and comply with oversight requests. These systems should use open architecture, allowing more government access during and after the pendency of the contract, and should be consistent throughout the Department when possible.

In addition, regardless of whether the government or the contractor creates the information technology system used, the Department should obtain and enforce contract provisions specifying that any and all information, data, and source codes in connection with the contracted IT system are the property of the federal government rather than the contractor, which then makes it easier to control and protect that information and allows DHS to be appropriately transparent with data and information.

The Department should also provide education and training to ensure that all contractors understand they are bound by federal contracting regulations including transparency

requirements. Some contractors, particularly county and local detention facilities, may be more accustomed to complying with state requirements and would benefit from more exposure to the Department's openness and transparency requirements.

APPENDIX 1: TASKING LETTER

Secretary

U.S. Department of Homeland Security
Washington, DC 20528

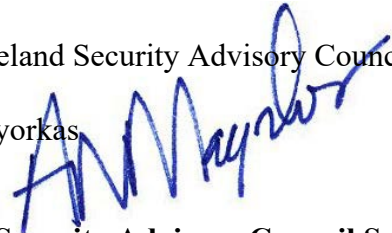


**Homeland
Security**

October 16, 2022

MEMORANDUM FOR: William J. Bratton and Jamie Gorelick
Co-Chairs, Homeland Security Advisory Council

CC: Karen Tandy
Vice Chair, Homeland Security Advisory Council

FROM: Alejandro N. Mayorkas
Secretary 

SUBJECT: **New Homeland Security Advisory Council Subcommittees**

Thank you for your completed efforts on Disinformation Best Practices and Safeguards. I greatly appreciate the Subcommittee's and Council's thoughtful insights and recommendations, which we are implementing. I also appreciate the work the Customer Experience and Service Delivery Subcommittee has underway.

I now respectfully request that the HSAC form four new subcommittees to provide findings and recommendations in these critical areas of our work:

1. How the Department can take a greater leadership role in supply chain security, including by strengthening supply chain cybersecurity.
2. How the Department can improve upon its intelligence and information sharing with our key federal, state, local, tribal, territorial, and private sector partners. The Subcommittee should assess whether the Department's information sharing architecture developed by the Office of Intelligence and Analysis (I&A) is adequate for the threats of today and tomorrow, and provide advice and recommendations to better enable I&A to rapidly and efficiently share information and intelligence with our key partners.
3. How the Department can improve its commitment to transparency and open government. The subcommittee should provide advice and recommendations that will position the Department as the leader in this critical area of model

government conduct.

4. How the Department can create a more robust and efficient Homeland Security Technology and Innovation Network. The Subcommittee should provide advice and recommendations that will develop the Department's innovation, research and development, and technology network with the private sector.

These subjects are described in more detail below. I will follow up with you shortly regarding formation of the Subcommittees.

I request that the HSAC submit its findings and key recommendations to me no later than 120 days from the date of this memorandum, consistent with applicable rules and regulations.

Thank you for your work on these important matters, your service on the HSAC, and your dedication to securing our homeland.

Leadership in Supply Chain Security

The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. The Department of Homeland Security continues to protect America's national and economic security by facilitating legitimate trade and travel and rigorously enforcing U.S. customs and immigration laws and regulations.

Secure and resilient supply chains facilitate greater domestic production, a range of supply, built-in redundancies, adequate stockpiles, and a world-class American manufacturing base and workforce. Technology and stable and secure networks are critical to facilitating this work. In the current digital age, it is imperative that the U.S. not only manufacture key technologies like lithium-ion batteries and semiconductors, but also ensure that technology is in place to secure the supply chains of raw materials necessary to this manufacturing. The recently enacted "The CHIPS and Science Act of 2022" (CHIPS Act) made an historic investment in this space and makes ensuring the security of supply chains an even greater priority.

Eliminating forced labor from U.S. and global supply chains is a moral imperative and critical to ensuring global economic security. The Department serves as the Chair of the Forced Labor Enforcement Task Force (FLETF), which has taken a leading role in the implementation of the Uyghur Forced Labor Prevention Act (UFLPA). The UFLPA seeks to prohibit goods made with forced labor from the People's Republic of China (PRC) from being imported into the United States. The PRC's use of forced labor has weakened our national security posture, as well as that of our international partners, by systemically undercutting economic competitiveness in key sectors such as polysilicon and agriculture. The *FLETF's Strategy to Prevent the Importation of Goods Mined, Produced, or Manufactured with Forced Labor in the People's Republic of China*, presents a whole of

government initiative to fight this scourge, and seeks stakeholder input to leverage partner capabilities.

Pandemics and other biological threats, cyberattacks, climate shocks and extreme weather events, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods and services. A resilient American supply chain will ensure domestic manufacturing capacity, maintain America's competitive edge in research and development, and create well-paying jobs.

The Department and its components have already begun to make strides in this space. The Cybersecurity and Infrastructure Security Agency (CISA) has advanced work to increase supply chain security. The Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force – sponsored by CISA's National Risk Management Center – is the United States' preeminent public-private supply chain risk management partnership. The ICT SCRM Task Force identifies and develops consensus strategies that enhance supply chain security and resilience.

The U.S. Coast Guard's Marine Transportation System Management mission enhances border security and defends the economic security of our \$5.4 trillion Marine Transportation System. This is in concert with the Maritime Security Operations mission program, which encompasses activities to protect waterways and ports by combating sea-based terrorism and other illegal activities.

The U.S. Customs and Border Protection (CBP) supply chain security mission is built on facilitation and layered enforcement. CBP's Customs Trade Partnership Against Terrorism (CTPAT) works with the trade community to strengthen international supply chains and improve United States border security. CTPAT is a voluntary public-private sector partnership program that recognizes that CBP can provide the highest level of cargo security only through close cooperation with the principal stakeholders of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers.

In addition to our work domestically, close cooperation on resilient supply chains with allies and partners who share our values will foster collective economic and national security. This request aligns with the DHS priority to maximize our international impact and strength, where we leverage our international footprint and relationships to advance homeland security objectives.

As the Department strives to stay ahead of the curve and take a greater leadership role by harnessing new technologies, minimizing environmental impact, and increasing partnerships in this vital area, I ask that you provide recommendations on how the Department can take a greater leadership role in supply chain security. The Subcommittee's assessment should include, but need not be limited to, the following:

- a. strengthening physical security;
- b. strengthening cybersecurity; and,

- c. increasing efficiencies to ensure a resilient, safe, and secure supply chain for critical manufacturing and technology sectors.

DHS Intelligence and Information Sharing

Federal, state, local, tribal, and territorial partners convened shortly after the September 11, 2001 terrorist attacks, creating a domestic information sharing architecture to enable the timely and seamless exchange of information to detect and eliminate terrorist threats. In the 21 years since 9/11, our law enforcement and homeland security community has made great progress in reshaping our information sharing environment. Working together, we put policies and processes in place that help us to be safer and more secure than we were years ago.

The Department of Homeland Security is committed to building on this foundation, as we are facing a more complex, diverse, and dynamic threat landscape than ever before. The wide array of threats we face impacts the safety and security of local communities of every size and location across our great country. The most effective way in which we address these challenges is through our partnerships, working together with one another.

DHS hosted an Intelligence Summit in August 2022, in partnership with the International Association of Chiefs of Police and other national law enforcement, public safety, and homeland security organizations. The Summit aimed to deepen partnerships and continue to improve intelligence and information sharing as public safety and national security threats evolve. The Summit also served as a forum to galvanize collaboration and commitment to supporting state, local, tribal, territorial, and campus (SLTTC) partners as they protect their communities. Senior leaders and key stakeholders convened with the goal of discovering new opportunities and improving existing avenues to enhance information sharing between all levels of government, while ensuring the protection of the privacy, civil rights, and civil liberties of U.S. citizens.

In June, DHS also launched a new mobile application titled DHS Intel, designed to deliver and share timely intelligence information with law enforcement and first responders across the country. Today, many of us consume information from news feeds, blogs, social media, podcasts, and a variety of other sources on our mobile phones; however, until last month, most intelligence information was either sent via e-mail distribution lists or viewed on sites optimized for desktops and laptops. Now, this information is available on-the-go for SLTTC and federal partners who rely on intelligence to keep the country safe.

As the Department approaches its 20th Anniversary, I ask that you provide recommendations on:

1. How the Department can rapidly and efficiently share intelligence and information with its federal, state, local, tribal, territorial, and private sector partners. Have DHS investments in information sharing technology and changes in law and policy resulted in increased knowledge transfer and resilience? Are further investments or changes in law or policy needed?

2. Has DHS created an information and intelligence sharing architecture that efficiently spreads knowledge and rapidly shares critical information? Are there steps that we need to take to revitalize or improve this architecture?
3. Whether the current DHS information sharing architecture optimizes information sharing for threats other than counterterrorism; for example, cyber, border security, foreign influence/propaganda, strategic advantage, and others.
4. Internal DHS Information Sharing: Has DHS fully implemented internal DHS information sharing policy – for example, the One DHS Memo – to leverage DHS data and information to support Departmental missions like border security as well as to develop and share relevant, quality intelligence with our partners?

DHS Transparency and Open Government

DHS is committed to transparency and promoting the principles of an Open Government. Initially developed in 2009 under the Obama Administration, the Presidential Memo on Transparency in Government and the follow-on Open Government Directive from the Office of Management and Budget laid a road map for increasing openness and transparency.

The United States has worked both domestically and internationally to ensure global support for Open Government principles to promote transparency, fight corruption, energize civic engagement, and leverage new technologies in order to strengthen the foundations of freedom in our own nation and abroad.

DHS has expanded transparency in concert with the development of Open Government Plans, recognizing that increased access to research data and information can encourage research collaboration and help successfully address the nation's constantly evolving homeland security challenges.

Further, I identified increasing openness and transparency as a key priority for our Department. It is important that DHS build and maintain trust with the communities we serve through improved data transparency, robust external communication, and strengthened oversight and disciplinary systems.

Therefore, I ask that you provide recommendations on:

1. How the Department and its components can expand on the foundation set by previous Open Government Plans for DHS.
2. New initiatives to increase transparency and sustaining its mission to protect the homeland.
3. How DHS can be held accountable in meeting its commitment to be a leader in modeling government openness and transparency.

Homeland Security Technology and Innovation Network

The Department of Homeland Security employs more than 240,000 individuals working in multiple offices and components across the country and the world. While the mission is uniform across the Department – to protect the homeland from foreign and domestic threats – the tools necessary to accomplish this can vary widely by office and can change in time. Moreover, while some threats are known and have been core to the DHS mission since our inception, we must remain ever vigilant and responsive to countering both unknown and future threats. In this scenario we may face accelerated timelines that do not fit into our normal acquisition life cycle to acquire key technology to counter a threat. It is critical to our nation’s security to have a robust and efficient Homeland Security Technology and Innovation Network that promotes an enhanced schedule of development and deployment of critical technology and assets to protect the homeland.

Such a network will necessarily require deep partnerships, especially with the private sector. From enterprise software to digital driver’s licenses, private sector entities have enabled the Department to advance its mission and modernize. It is therefore important for the Department to leverage its existing offices and relationships to further harness the potential of technology and innovation in the private sector to benefit the Department.

Current technology and innovation engagements are led by the DHS Science and Technology Directorate (S&T) and designated offices within component agencies. S&T is responsible for identifying operational gaps and conceptualizing art-of-the-possible solutions that improve the security and resilience of the nation. To facilitate this, S&T oversees programs that facilitate technology transfer and commercialization, funding for start-ups, research, and development challenges. Similarly, component offices partner with private sector entities to source technology and innovations for their discrete needs.

To maximize the opportunity afforded by partnership with the private sector and the expertise within the Department, I ask that you assess the private sector experience, specifically in the areas of technology development and innovation, and provide recommendations on how the Department can create a more robust and efficient Homeland Security Technology and Innovation Network.

The Subcommittee’s assessment should include, but need not be limited to, the following:

- a. an assessment of how the private sector engages with the current R&D and acquisition programs and opportunities, including where those can be maximized or improved;
- b. different means of increasing innovative technology partnerships with the private sector;
- c. recommendations on harmonizing existing innovation efforts across the Department and its components to best leverage funding and resources; and,
- d. identifying current barriers to developing a more robust technology and innovation network, including legal, contracting, and policy considerations.

APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES

| Name | Title | Organization |
|------------------------|---|---|
| Brenda Abdelall | Assistant Secretary | Office of Partnership and Engagement, DHS Headquarters |
| Tahani Afaneh | Assistant Chief Counsel | Litigation Technology and Support, Office of Chief Counsel, U.S. Customs and Border Protection (CBP) |
| Amy Bennett | Director of Communications | Office of Privacy |
| Lauren Bernstein | Associate Counsel | Regulatory and Verification Law Division, United States Citizenship and Immigration Services (USCIS), Office of Chief Counsel (OCC) |
| Roger Brown | Deputy Chief Human Capital Officer | Office of the Chief Human Capital Officer (OCHCO) |
| Cynthia Burdette | Acting Deputy Assistant Commissioner | Office of Public Affairs (OPA), CBP |
| Philip Busch | Senior Legal Advisor | USCIS OCC |
| Jeffrey Carter | Acting Assistant Commissioner | OPA, CBP |
| Shvonne Chappell-Kirby | Chief of Staff | Office of Privacy, USCIS |
| Bryan Christian | Chief of Office of Access and Information Services | External Affairs Directorate, USCIS |
| Vashon Citizen | Chief of the Digital Services Division | Office of Access and Information Services, USCIS |
| Kenneth N. Clark | Assistant Director | Office of Information Governance and Privacy, Immigration and Customs Enforcement (ICE) |
| Mason Clutter | Senior Policy Advisor to Chief Privacy Officer | Office of Privacy, DHS Headquarters |
| Christine Montani Cyr | Director of Enterprise Analytics and Chief Data Officer | Federal Emergency Management Agency (FEMA) |
| Jennifer Daskal | Deputy General Counsel | Office of General Counsel, DHS Headquarters |

| | | |
|----------------------|---|--|
| Shannon K. DiMartino | Technology Oversight Branch Chief | Office of Privacy, USCIS |
| Lynn Parker Dupree | Former - Chief Privacy Officer and Chief FOIA Officer | Office of Privacy, DHS Headquarters |
| Marsha Espinosa | Assistant Secretary | Office of Public Affairs, DHS Headquarters |
| Elizabeth Gaffin | Associate Counsel | Regulation and Verification Law Division, OCC, USCIS |
| Monica Generous | Director | Human Capital Accountability, Human Capital Policy and Programs, OCHCO |
| Ricou Heaton | Deputy Associate Chief Counsel | Information Law Branch (LB), FEMA |
| Rachelle Henderson | Chief Information Officer | Office of the Chief Information Officer, ICE |
| James Holzer | Deputy Chief Privacy Officer | Office of Privacy, DHS Headquarters |
| Mike Horton | Chief Data Officer | Office of the Chief Information Officer, DHS Headquarters |
| Patrick Howard | Branch Chief | FOIA Division, Privacy and Diversity Office, Office of the Commissioner, CBP |
| Eric Hysen | CIO & Senior Official Performing the Duties of the Deputy Under Secretary for Management | Office of the Chief Information Officer, DHS Headquarters |
| Alexander Jacobs | Senior Director | Homeland Security Advisory Council |
| Kimya Lee | Deputy Chief Human Capital Officer | OCHCO |
| Quan Long | Deputy Chief | Commercial and Administrative Law Division, OCC |
| Marian Manlove | Acting Executive Director | Human Capital Policy and Programs, OCHCO |
| Tammy M. Meckley | Associate Director | Immigration Records and Services Directorate, USCIS |
| Jonathan E. Meyer | General Counsel | Office of General Counsel, DHS Headquarters |
| Teri Miller | Freedom of Information Act Officer | Transportation Security Administration |

| | | |
|-----------------------|--|---|
| Jeffrey Mitchell | Attorney-Advisor | Office of the Chief Information Officer, DHS Headquarters |
| Bitta Mostofi | Senior Advisor | Customer Experience, Office of the USCIS Director |
| Shiraz Panthaky | Chief | Government Information Law Division, Office of the Principal Legal Advisor, ICE |
| Catrina Pavlik-Keenan | Deputy Chief FOIA Officer | Office of Privacy, DHS Headquarters |
| Elizabeth Puchek | Chief Data Officer | Office of the Chief Data Officer, USCIS |
| Eric Reid | Senior Advisor | Human Capital Policy and Programs, OCHCO |
| Jason Robertson | DHS Assistant General Counsel for Administrative Law | DHS Office of General Counsel (OGC) |
| Rebekah A. Salazar | Executive Director | Privacy and Diversity Office, Office of the Commissioner, CBP |
| Stephanie Sawyer | Assistant General Counsel | Labor and Employment Law, Office of General Counsel |
| Carrie McCuin Selby | Associate Director | External Affairs Directorate, USCIS |
| Scott Shuchart | Counselor to the Director | ICE |
| Stacy Smith | Assistant Director | ICE Inspections, Office of Professional Responsibility |
| Tadgh Smith | Deputy Assistant Director | Law Enforcement Systems and Analysis, USCIS |
| Marie Trottier | Outreach and Engagement Program Manager and Tribal Affairs Liaison | Transportation Security Administration |
| Joshua Stanton | Deputy Chief Counsel for General Law | Office of Chief Counsel, FEMA |
| Alexandra Travis | Chief Administrative Officer | Mission Support, FEMA |
| Angela Y. Washington | Chief | Office of Privacy, USCIS |
| MaryKate Whalen | Principal Deputy Chief Counsel | Transportation Security Administration |