U.S. DEPARTMENT OF HOMELAND SECURITY

ANNUAL PERFORMANCE REPORT FY 2023-2025

APPENDIX B | RELEVANT GAO AND OIG REPORTS

DEFENDING THE HOMELAND

20

YEARS OF DHS

The U.S. Department of Homeland Security's Annual Performance Report (APR) for FY 2023-2024 presents a summary of the Department's performance for FY 2023, with performance measure results, explanations, and targets for FY 2024-2025 included.

The APR presents summaries of the Department's performance for each DHS Mission outlined in the 2023 Quadrennial Homeland Security Review (QHSR). It also highlights key performance information, including measures and results for the Department's Objectives outlined in the QHSR.

The report further summarizes information on key initiatives in the DHS Performance Management Framework related to the Strategic Review and our Agency Priority Goals (APGs). Also included are other key management initiatives, and a summary of our performance challenges and high-risk areas identified by the DHS Office of the Inspector General (OIG) and the Government Accountability Office (GAO). The APR is consolidated to incorporate our Annual Performance Plan (APP). Appendix B provides a selection of the more significant DHS program evaluations conducted in FY 2023 by GAO and DHS OIG.

For FY 2023, the Department's Performance and Accountability Reports consist of the following two reports:

DHS Agency Financial Report | Publication date: November 15, 2023

DHS Annual Performance Report | Publication date: March 11, 2024. This report is submitted with the Department's Congressional Budget Justification.

When published, both reports will be located on our public website at: https://www.dhs.gov/performance-financial-reports

Contact Information

For more information, contact:

Department of Homeland Security
Office of the Chief Financial Officer
Office of Program Analysis and Evaluation
6595 Springfield Center Drive
Springfield VA 22150

Table of Contents

Introduction

Independent program evaluations provide vital input to the Department of Homeland Security (DHS) as they offer insight to the performance of our programs and identify areas for improvement. These evaluations are used across the Department to look critically at how we conduct operations and to confront some of the key challenges facing the Department.

This appendix provides a selection of the more significant DHS program evaluations conducted in FY 2023 by the U.S. Government Accountability Office (GAO) and the DHS Office of Inspector General (OIG). For each report, the report name, report number, date issued, summary, and a link to the publicly released report are provided.

Detailed information on the findings and recommendations included GAO reports, as well as other information about the auditor, is available on GAO's website at: U.S. Government Accountability Office (U.S. GAO)

Detailed information on the findings and recommendations of DHS OIG reports, as well as other information about the auditor, is available on DHS OIG's website at: Home | Office of Inspector General (dhs.gov)

Relevant GAO and OIG Reports by DHS Component

U.S. Customs and Border Protection (CBP)

GAO Reports

Title: Southwest Border: DHS Coordinates with and Funds Nonprofits Serving Noncitizens

Number: GAO-23-106147

Date: 4/19/2023

Summary: GAO was asked to examine the extent to which DHS had used grants or contracts to provide funds to nonprofits that provide services to noncitizens released from DHS custody. The U.S. has experienced a significant number of noncitizens arriving at the Southwest Border (SWB). GAO found that when releasing noncitizens from custody and while they wait for resolution of their immigration court cases, both CBP and ICE are able to coordinate with nonprofits that provide resources such as food, shelter, and transportation. Additionally, FEMA provides grant funding to some nonprofits that offer these services, providing more than $282 million in humanitarian relief grant funding to nonprofit and governmental organizations in FY 2019, 2021, and 2022 (no funding was appropriated to the Emergency Food and Shelter Program for humanitarian relief in FY 2020). GAO noted that DHS has not entered into any contracts with nonprofits to provide services to noncitizens after they are released from custody. GAO did not make any recommendations in this report.

Title: Customs and Border Protection: Actions Needed to Enhance Acquisition Management and Knowledge Sharing

Number: GAO-23-105472

Date: 4/25/2023

Summary: GAO was asked to review CBP's processes for planning and managing its acquisitions programs. GAO assessed the extent to which key CBP stakeholders are collaborating when planning select acquisition programs and the extent to which CBP demonstrates best practices for lessons learned when developing acquisition programs. GAO reviewed policies and guidance from a nongeneralizable sample of 10 CBP programs and found that a number of key stakeholders collaborate to manage CBP's acquisition programs. However, GAO found that CBP acquisition programs would benefit from increased formal involvement by contracting officers in developing program-level acquisition strategies. GAO also found that CBP requires programs to conduct activities that can capture lessons learned, such as post-implementation reviews, but that the programs reviewed by GAO did not consistently conduct these activities. GAO made four recommendations to CBP, including to update related guidance; formalize contracting officer involvement in program acquisition strategies; collect, analyze, and validate lessons learned; and develop a lessons learned repository for acquisitions programs. DHS agreed with these recommendations and is working to implement.

Title: DNA Collections: CBP is Collecting Samples from Individuals in Custody, but Needs Better Data for Program Oversight [Reissued with revisions on Jun. 5, 2023]

Number: GAO-23-106252

Date: 5/24/2023

Summary: GAO reviewed CBP's implementation of the DNA Fingerprint Act of 2005 and the status of CBP's DNA collection program. As noted in GAO's report, CBP has implemented a nationwide DNA collection program. CBP Office of Field Operations (OFO), which is responsible for operating U.S. Ports of Entry (POEs), and U.S. Border Patrol, which is responsible for securing the borders between POEs, have processes for collecting DNA from individuals they arrest or detain. From FY 2020 to FY 2022, CBP collected nearly 1 million DNA samples for submission to the to the Federal Bureau of Investigation (FBI) for entry into the (CODIS). CODIS enables federal, state, and local labs to exchange and compare DNA information to increase chance for leads for law enforcement. GAO found that CBP has experienced challenges with DNA collection kit shortages, resulting in some individuals in CBP custody not having their DNA collected by CBP officers and agents. However, GAO also found that CBP and FBI are taking steps to resolve this issue and ensure there is a sufficient supply of DNA collection kits moving forward. GAO also noted that CBP collects data on DNA collections across field locations but is not systematically collecting data on the reasons why they do not obtain DNA from some individuals arrested or detained under CBP's immigration enforcement authority. GAO made recommendations to OFO and Border Patrol to develop and implement a mechanism to systematically collected data on the reasons why officers and agents are not collecting DNA from individuals arrested on federal criminal charges or noncitizens detained for immigration violations. DHS concurred with the recommendations and efforts are underway to implement.

Title: Southwest Border: Additional Actions Needed to Address Cultural and Natural Resource Impacts from Barrier Construction

Number: GAO-23-105443

Date: 9/7/2023

Summary: GAO reviewed the effects that the southwest border (SWB) barrier construction has had on cultural and natural resources. CBP and the Department of Defense (DOD) installed about 458 miles of border barrier panels across the SWB between January 2017 and January 2021. GAO found that before proceeding with construction, CBP took steps to assess the potential impacts of such construction, such as soliciting input from land management agencies, Tribes, and the public. However, GAO also found that CBP relied on waivers of cultural and natural resource-related laws to expedite construction. Since the administration paused border barrier construction in January 2021, CBP has prioritized efforts to address safety hazards left at incomplete project sites, such as removing exposed rebar. In addition, CBP and the Department of Interior (DOI) have worked together to identify actions to mitigate impacts from construction on federal lands. GAO is making three recommendations, including that CBP and DOI document a joint strategy to mitigate resource impacts from barrier construction and that CBP evaluate lessons learned from its assessments of potential cultural and natural resource impacts. The agencies agreed with these recommendations and are working to implement.

OIG Reports

Title: CBP Could Do More to Plan for Facilities Along the Southwest Border

Number: OIG-23-45

Date: 8/29/2023

Summary: During FY 2022, SWB crossings surged between POEs, resulting in more than 2.3 million encounters for that fiscal year alone. OIG assessed the extent to which CBP reviewed and planned for processing and holding migrants at both temporary and permanent facilities along the SWB. Since 2019, CBP has improved its response to migrant surges by deploying temporary facilities to increase it capacity to humanely process migrants. However, OIG found that CBP did not always document its planning decisions for both temporary and permanent facilities, did not always consider alternatives before issuing contracts for temporary facilities, and did not document whether it continually reassessed the need for existing temporary facilities, including the cost-effectiveness of keeping those facilities. OIG found that these conditions occurred because CBP prioritized short-term response over long-term planning, and because CBP has not yet finalized a comprehensive policy that incorporates planning for both temporary and permanent facilities. OIG recommended that CBP finalize an already-drafted plan and establish a formal policy to address these conditions, including documenting and regularly assessing the planning and need for existing temporary facilities. DHS agreed with these recommendations and efforts are underway to implement.

Title: CBP Needs to Improve Its Video and Audio Coverage at Land Ports of Entry

Number: OIG-23-54

Date: 9/25/2023

Summary: OIG assessed how often CBP uses closed-circuit television video cameras and microphones at land POEs (or, LPOEs) to ensure the protection of the public, employees, and property. Federal and CBP standards require video surveillance systems that provide camera coverage and recording at LPOEs for physical security and to monitor operations. CBP OFO uses the Centralized Area Video Surveillance System (CAVSS) to meet this requirement. OIG found that CAVSS has periodically experienced widespread recording gaps, has instances of poor-quality video and audio, displays areas of inadequate video and audio coverage within LPOEs, and could benefit from improved privacy protections for detainees being held at LPOEs. OIG found that recording gaps were an issue primarily caused by equipment not always rebooting after the OFO Office of Information and Technology (IT) applied required network security patches and scans. Video and audio quality was sometimes reduced by outdated equipment in need of repair or replacement, limited network bandwidth and emergency back-up power supply, and an unreliable electrical grid. OIG also found instances in which video and audio coverage at certain locations did not meet requirements due to a lack of coordination when repurposing LPOE rooms and conducting facility projects, funding and infrastructure constraints, and inadequate CAVSS operator training. Further, LPOEs did not always have the required privacy protections in place for detainees. OIG made seven recommendations aimed at improving OFO's CAVSS and related processes. DHS concurred with all seven recommendations and is working to implement.

Cybersecurity and Infrastructure Security Agency (CISA)

GAO Reports

Title: Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration

Number: GAO-22-104767

Date: 10/4/2022

Summary: GAO was asked to review federal efforts to provide ransomware prevention and response assistance to state, local, tribal, and territorial (SLTT) government organizations. Specifically, GAO reviewed how federal agencies assist these organizations in protecting their assets against ransomware attacks and in responding to related incidents; organizations' perspectives on ransomware assistance received from federal agencies; and the extent to which federal agencies addressed key practices for effective collaboration when assisting these organizations. GAO identified three federal agencies that provide direct ransomware assistance—CISA, USSS, and the FBI. As noted in GAO's report, most government officials surveyed said they're satisfied with the three agencies' prevention and response efforts and had generally positive views on provided services like ransomware guidance, detailed threat alerts, quality no-cost technical assessments, and timely incident response assistance. But respondents also identified challenges related to awareness, outreach, and communication. GAO found that CISA, USSS, and the FBI have taken steps to enhance interagency coordination through existing mechanisms and demonstrated coordination on a joint ransomware website, guidance, and alerts. However, GAO found that the three agencies have not addressed aspects of six of the seven key practices for interagency collaboration in their ransomware assistance to SLTT governments. GAO made three recommendations to DHS (CISA and USSS) and the Department of Justice (FBI) to address identified challenges and incorporate key collaboration practices in delivering services to SLTT governments. The agencies concurred with GAO's recommendations and are working to implement.

Title: Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity

Number: GAO-23-105480

Date: 10/24/2022

Summary: The COVID-19 pandemic forced schools nationwide to increase their reliance on IT to deliver educational guidance to students. This made Kindergarten through grade 12 (K-12) schools more vulnerable to potentially serious cyberattacks. GAO reviewed the cybersecurity of K-12 schools to determine what is known about the impact of cyber incidents, and to what extent key federal agencies coordinate with other federal and nonfederal entities to assist K-12 schools to defend against cyber threats. GAO found that K-12 schools have reported significant educational impacts due to cybersecurity incidents, such as ransomware attacks. Cyberattacks can also cause monetary losses for targeted schools due to the downtime and resources needed to recover from incidents. Officials from state and local entities reported that the loss of learning following a cyberattack ranged from 3 days to 3 weeks, and recovery time ranged from 2 to 9 months. While the precise national magnitude of cyberattacks on K-12 schools is unknown, research organizations like Comparitech have been working to identify, study, and report on data in this area. GAO made one recommendation in the report to DHS (CISA) to develop metrics to better measure the effectiveness of K-12 cybersecurity related products and services. DHS concurred with GAO's recommendation and is working to implement. GAO also made recommendations to the Department of Education.

Title: Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices

Number: GAO-23-105327

Date: 12/1/2022

Summary: Cyber threats to critical infrastructure Internet of Things (IoT) and operational technology (OT) represent a significant national security challenge. Recent incidents—such as the ransomware attacks targeting health care and essential services during the COVID-19 pandemic—illustrate the cyber threats facing the nation's critical infrastructure. IoT generally refers to the technologies and devices that allow for the network connectivity and interaction of a wide array of "things," throughout such places as buildings, transportation infrastructure, or homes. OT are programmable systems or devices that interact with the physical environment, such as building automation systems that control machines to regulate and monitor temperature. To help federal agencies and private entities manage the cybersecurity risks associated with IoT and OT, CISA and the National Institute of Standards and Technology (NIST) have issued guidance and provided resources. Specifically, CISA has published guidance, initiated programs, issued alerts and advisories on vulnerabilities affecting IoT and OT devices, and established working groups on OT. During its review, GAO found that selected federal agencies with a lead role in their critical infrastructure sectors have reported various cybersecurity initiatives to help protect three critical infrastructure sectors with extensive use of IoT or OT devices and systems. However, GAO found that none of the selected lead agencies had developed metrics to assess the effectiveness of their efforts, nor had selected agencies conducted IoT and OT cybersecurity risk assessments. Lead agency officials noted difficulty assessing program effectiveness when relying on voluntary information from sector entities. While GAO acknowledged this challenge, GAO also made recommendations to the Department of Energy, Health and Human Services, Department of Transportation, and DHS. GAO recommended that each department establish and use metrics to assess the effectiveness of sector IoT and OT cybersecurity efforts and to evaluate sector IoT and OT cybersecurity risks. DHS concurred with the two recommendations and is working to implement.

Title: Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities

Number: GAO-23-105806

Date: 2/7/2023

Summary: Critical infrastructure provides essential functions that underpin American society such as supplying water, generating energy, and producing food. Disruption or destruction of the nation's critical infrastructure sectors could have debilitating effects. As reported by GAO, the William M. (Mac) Thornberry National Defense Authorization Act for FY 2021 expanded and added responsibilities for sector risk management agencies (SRMAs). These agencies engage with their public and private sector partners to promote security and resilience within their designated critical infrastructure sectors. GAO found that CISA—as the national coordinator for infrastructure protection—has undertaken efforts to help SRMAs implement their statutory responsibilities. However, GAO also found that SRMA officials for a majority of critical infrastructure sectors reported that additional guidance and improved coordination from CISA would help them implement their statutory responsibilities. While CISA is taking steps to address these items, GAO found that CISA has not developed milestones and timelines to complete its efforts and recommended that CISA do so. DHS concurred with the recommendation and is working to implement.

OIG Reports

Title: CISA Made Progress but Resources, Staffing, and Technology Challenges Hinder Cyber Threat Detection and Mitigation

Number: OIG-23-19

Date: 3/3/2023

Summary: In December 2020, and as the operational lead for federal cybersecurity, CISA issued an emergency directive about an advanced cyberattack that had caused a breach of SolarWinds software and federal computing networks. OIG conducted this review to determine CISA's ability to detect and mitigate cyberattacks based on lessons learned after the SolarWinds breach. Following the breach discovery in 2020, OIG notes in its report that CISA improved its ability to detect and mitigate risks from major cyberattacks. However, the breach itself revealed that CISA did not have adequate resources—backup communication systems, staff, or secure space—to effectively respond to threats. To address this, CISA is taking steps to ensure continuity, strategic workforce, and workspace allocation plans are completed in a timely fashion and meet mission needs. However, OIG also notes in its report that CISA still needs to receive all the necessary cybersecurity data from other federal agencies' dashboards and complete its plans for development of malware and data analytics capabilities. Until these efforts are completed, CISA may not always be able to effectively detect and mitigate major cyberattacks or meet the government's demand for cyber capabilities that protect federal networks and systems. OIG made four recommendations in its report to address CISA's resource needs and improve technology to enhance cyber detection and mitigation. DHS concurred with the recommendations and is working to implement.

Federal Emergency Management Agency (FEMA)

GAO Reports

Title: Disaster Contracting: Action Needed to Improve Agencies' Use of Contracts for Wildfire Response and Recovery

Number: GAO-23-105292

Date: 4/13/2023

Summary: As noted by GAO, wildfire season is getting longer, and the number of large fires is increasing, leaving more people and structures at risk. Several federal agencies share responsibility for leading wildfire response and recovery. These agencies often work with private sector contractors to obtain life-saving goods and services quickly. GAO examined how FEMA, the Forest Service, and the Bureau of Land Management (BLM) collectively obligated at least a total of $2 billion for wildfire response and recovery from FY 2018 through FY 2021. To mobilize goods and services quickly, the three selected agencies GAO studied used multiple approaches. For example, they used indefinite delivery contracts and assigned ordering officials, who can be authorized to place certain orders on behalf of the government. Each of the selected agencies also had processes in place for collecting lessons learned. However, GAO found that opportunities exist for agencies to improve ordering policies, making six recommendations in its report. DHS concurred with the recommendations and is working to implement.

Title: FEMA Disaster Workforce: Actions Needed to Improve Hiring Data and Address Staffing Gaps

Number: GAO-23-105663

Date: 5/2/2023

Summary: GAO was asked to review FEMA's hiring process and staffing gaps, including FEMA's authorities and processes for hiring and related challenges, and FEMA's disaster workforce staffing gaps and the extent to which FEMA is monitoring and evaluating its efforts to fill these gaps. As noted by GAO in its report, the demand for FEMA help has increased with more frequent and complex disasters like hurricanes, wildfires, and the COVID-19 pandemic. But FEMA has had trouble building a workforce to meet these needs. GAO found that FEMA has fallen short of its yearly staffing target since 2019—and that gap continues to grow. GAO found that FEMA aims to reduce the time it takes to hire more staff, but it doesn't have accurate data to know if its strategies are working effectively. GAO recommended in its report that FEMA document clear and consistent procedures to collect and calculate time-to-hire information; document plans to monitor and evaluate the agency's progress on hiring efforts to address staffing gaps; and develop performance measures that monitor and evaluate progress towards hiring goals. DHS concurred with the recommendations and is working to implement.

Title: Transit Security: FEMA Should Improve Transparency of Grant Decisions

Number: GAO-23-105956

Date: 7/26/2023

Summary: GAO reviewed FEMA's management of the Transit Security Grant Program and assessed how grant-funded projects enhance public transit security. FEMA’s Transit Security Grant Program is designed to help public transit agencies protect people and critical infrastructure from terrorism. Public transit agencies apply to FEMA for security improvement grants, and in its “Notice of Funding Opportunity,” FEMA discloses is process for reviewing and scoring applications. However, GAO found that FEMA did not always follow that process, favoring some lower-scoring applications in 2015-2021, raising questions about the soundness of the award decisions. GAO made four recommendations to FEMA to accurately describe all the criteria it uses to score applications in the Notice of Funding Opportunity; select applications for award in accordance with its FEMA’s publicly disclosed merit review process; incorporate cyber threats into risk assessments that help inform award decisions; and document the underlying assumptions and justifications for those risk assessments. DHS concurred with GAO's recommendations and is working to implement.

Title: Flood Insurance: FEMA's New Rate-Setting Methodology Improves Actuarial Soundness but Highlights Need for Broader Program Reform

Number: GAO-23-105977

Date: 7/31/2023

Summary: As noted by GAO in this report, FEMA’s National Flood Insurance Program (NFIP) was created with competing policy goals—keeping flood insurance affordable and the program fiscally solvent. A historical focus on affordability has led to premiums that do not fully reflect flood risk, insufficient revenue to pay claims, and, ultimately, $36.5 billion in borrowing from the Department of Treasury since 2005. In October 2021, FEMA began implementing Risk Rating 2.0, a new methodology for setting premiums for the NFIP. GAO found that the new methodology substantially improves ratemaking by aligning premiums with the flood risk of individual properties, but some other aspects of NFIP still limit actuarial soundness. GAO also found that while Risk Rating 2.0 is aligning premiums with risk, affordability concerns accompany the associated premium increases. Under the current approach, GAO found that Gulf Coast states are among those experiencing the largest premium increases. Policies in these states have been among the most underpriced, despite having some of the highest flood risks. GAO notes in its report that Risk Rating 2.0 does not yet appear to have significantly changed conditions in the private flood insurance market because NFIP premiums generally remain lower than what a private insurer would need to charge to be profitable, and certain program rules continue to impede private-market growth. GAO recommended six matters for congressional consideration, including authorizing and requiring FEMA to replace two policyholder charges with risk-based premium charges; replacing discounted premiums with a means-based assistance program that is reflected in the federal budget; addressing NFIP's current debt—for example, by canceling it or modifying repayment terms—and potential for future debt; and authorizing and requiring FEMA to revise NFIP rules hindering the private market. GAO also made five recommendations to FEMA, including that it publishes an annual report on NFIP's actuarial soundness and fiscal outlook. DHS concurred with GAO's recommendations and is working to implement.

OIG Reports

Title: FEMA Should Increase Oversight to Prevent Misuse of Humanitarian Relief Funds

Number: OIG-23-20

Date: 3/28/2023

Summary: OIG conducted this review to determine whether FEMA awarded funding provided in the American Rescue Plan Act of 2021 (ARPA) in accordance with federal law and regulations. OIG found that FEMA awarded the $110 million in humanitarian relief funds provided by ARPA to the FEMA Emergency Food and Shelter Program (EFSP) National Board to provide services to families and individuals encountered by DHS in communities most impacted by the humanitarian crisis at the SWB. OIG reviewed 18 local recipient organizations (LROs) and found that they did not always use the funds consistent with ARPA's humanitarian relief funding and application guidance. Some of the LROs were not able to provide supporting documentation for families and individuals they provided services to and the required documentation or receipts for claimed reimbursements were not always provided. OIG determined these issues occurred because FEMA relied on local boards and fiscal agents to enforce the funding and application guidance. OIG notes in its report that without additional oversight and enforcement from FEMA, LROs may continue to use provided funds for services without providing the required supporting documentation for reimbursement, increasing the risk of misuse of funds and fraud. OIG made two recommendations to FEMA to improve oversight and enforcement for similar future appropriations. DHS concurred with both recommendations and is working to implement.

Title: FEMA Did Not Effectively Manage the Distribution of COVID-19 Medical Supplies and Equipment

Number: OIG-23-34

Date: 07/19/2023

Summary: On March 19, 2020, FEMA was tasked with leading the federal response to combat the COVID-19 pandemic. FEMA was responsible for coordinating the distribution of personal protective equipment, ventilators, and medical supplies to SLTT governments. OIG conducted this audit to determine to what extent FEMA managed and distributed medical supplies and equipment in response to COVID-19. As found by OIG, although FEMA worked with its strategic partners to deliver critical medical supplies and equipment in response to COVID-19, FEMA did not effectively manage the distribution process. OIG found that FEMA did not use the Logistics Supply Chain Management System (LSCMS), its system of record for managing the distribution process, to track about 30% of the critical medical resources shipped, as required. Instead, FEMA used other tracking mechanisms, such as the Web Emergency Operations Center resource request system and spreadsheets, that did not share information with LSCMS. In addition, FEMA did not maintain delivery receipt documentation for about a third of the shipments OIG reviewed. OIG found that this occurred because FEMA was under pressure to expedite the delivery of critical medical resources and did not follow established business practices. As a result, FEMA did not have full visibility into the resources shipped and received. Since the COVID-19 pandemic began, OIG found that FEMA has evaluated its early response efforts and developed a Logistics Resource Tracker to help the National Response Coordination Center centrally track the distribution of resources. Although the new automated tool enhanced FEMA's visibility into the resources shipped and received, the tool did not always have accurate data. Without accurate data, FEMA cannot ensure it has quality information to make informed allocation decisions about where to send resources, how to evaluate performance, and how to address risk in future disaster response operations. OIG made three recommendations to help improve future operations, with which DHS concurred and is working to implement.

Office of Intelligence and Analysis (I&A)

GAO Reports

Title: Domestic Terrorism: Further Actions Needed to Strengthen FBI and DHS Collaboration to Counter Threats

Number: GAO-23-104720

Date: 2/22/2023

Summary: GAO was asked to review domestic terrorism threats, incidents, and related federal cases and charges. As part of this report, GAO assessed the extent to which the FBI and DHS I&A track domestic terrorism investigations and incidents, and the extent to which both agencies follow leading collaboration practices in their efforts to counter domestic terrorism. GAO found that from FY 2013 to FY 2021, the FBI's number of open domestic terrorism-related cases grew by 357% from 1,981 to 9,049. GAO also found that from calendar year 2010 to 2021, I&A tracked a total of 231 domestic terrorism incidents, with racially or ethnically motivated violent extremists committing the most violent incidents during that time period. GAO found that FBI and DHS generally follow leading practices for collaboration to identify and counter domestic terrorism threats, such as collaborating via headquarters staff, fusion centers, and through serving on task forces, but that the two agencies have not assessed if the agreements they have in place fully reflect how their personnel should collaborate on their shared charge of preventing domestic terrorism. Due to the rapidly evolving threat landscape, GAO found that having up-to-date, comprehensive formal agreements—and regularly assessing the effectiveness of those agreements and collaborative efforts—would enhance the two entities' collaboration and may lead to improved information to counter domestic terrorism threats. GAO made six recommendations, three each to the FBI and I&A, to assess agreements in place and evaluate collaborative efforts. DHS concurred with its recommendations from GAO and is working to implement.

Title: Capitol Attack: Federal Agencies Identified Some Threats, but Did Not Fully Process and Share Information Prior to January 6, 2021 [Reissued with revisions on Jul. 21, 2023]

Number: GAO-23-106625

Date: 2/28/2023

Summary: This GAO report is the seventh in a series regarding the events that occurred at the U.S. Capitol on January 6, 2021. In this review, GAO examined how federal agencies identified potential threats, and how they used this information to prepare for and respond to the Capitol attack. GAO found that all 10 federal agencies reviewed identified potential threats of violence before January 6, but some agencies either didn't follow their established policies or procedures for reviewing the threats or didn't share critical information with partners responsible for planning security measures. As a result of this review, GAO made 10 recommendations to five agencies to, for example, assess internal control deficiencies related to processing or sharing information. DHS concurred with the four recommendations in the report for the Department and are working to implement.

U.S. Immigration and Customs Enforcement (ICE)

GAO Reports

Title: Immigration Detention: ICE Needs to Strengthen Oversight of Informed Consent for Medical Care

Number: GAO-23-105196

Date: 10/18/2022

Summary: Within DHS, ICE is responsible for providing safe, secure, and humane confinement for detained noncitizens in the U.S. In that capacity, ICE oversees and at some detention facilities provides on-site medical care services. ICE also oversees referrals and pays for off-site medical care when services are not available at detention facilities. GAO was asked to review issues related to informed consent for medical care for noncitizens in immigration detention facilities. GAO examined the extent to which ICE has policies for obtaining informed consent for medical care, and how selected facilities oversaw implementation of those policies. GAO found that ICE has established policies for obtaining and documenting informed consent for medical care provided on-site at detention facilities. Informed consent involves the provider speaking to the patient in detail about the risks, benefits, and alternatives of individual procedures. Medical care not available at detention facilities is provided off-site at clinics, hospitals, or other facilities. ICE relies on these community providers to obtain and document informed consent for care they provide off-site. However, GAO found that ICE policies do not require facilities to collect documentation of informed consent for detained noncitizens' off-site medical care from community providers. GAO made three recommendations in this report, including that ICE require detention facilities to collect informed consent documentation from off-site providers, and then require a review of this documentation as part of its oversight mechanisms for detention facilities. DHS concurred with the recommendations and is working to implement.

Title: Immigration Detention: Actions Needed to Collect Consistent Information for Segregated Housing Oversight

Number: GAO-23-105366

Date: 10/26/2022

Summary: GAO reviewed ICE's processes for and oversight of segregated housing and ICE's collection of information on segregated housing placements; the number and characteristics of segregated housing placements from fiscal years 2017 through 2021; and the extent to which ICE receives and addresses segregated housing complaints. As noted by GAO in its report, ICE can, under certain circumstances, place detained noncitizens in segregated housing—one to two person cells separate from the general population. There were 14,581 such placements from FY 2017 to FY 2021. ICE oversees segregated housing and monitors placements involving vulnerable persons (e.g., those with medical or mental health conditions). However, GAO found that ICE relies on reports and data for these oversight activities that don't always have enough detail about the circumstances leading to a placement or indicate that a placed person is vulnerable. GAO also found that housing-related complaints to ICE increased from FY 2017 to FY 2019, but decreased from FY 2020 to FY 2021, and that ICE has taken steps to address recommendations from a 2020 GAO report which recommended that ICE conduct comprehensive analyses of detention-related complaints and require its field offices to record actions taken on and resolutions from these complaints. While ICE has made progress, GAO found that opportunities for further improvements exist. In its report, GAO recommended that ICE provide specific guidance to Enforcement and Removal (ERO) field offices for segregated housing documentation, and identify all known detained noncitizens in vulnerable populations as defined in segregated housing policy. DHS concurred with the recommendations and is working to implement.

OIG Reports

Title: ICE Has Limited Ability to Identify and Combat Trade-Based Money Laundering Schemes

Number: OIG-23-41

Date: 8/21/2023

Summary: OIG conducted this review to determine the extent to which ICE identifies and combats trade-based money laundering (TBML). In TBML schemes, criminal organizations use illicit cash to buy goods, which are imported and sold in another country. The sale proceeds are returned to the criminal organization, which completes the laundering. Criminal organizations use these trade transactions to disguise their criminal proceeds and finance terrorism and other illicit activity. OIG found that ICE has limited ability to identify and combat commodities used in of TBML schemes, such as not having automated technology to identify import commodities at high risk for TBML schemes. OIG found that funding constraints and competing priorities have hampered the development of automated capabilities to identify TBML schemes, as well as ICE's ability to staff this organizational function with the needed levels of expertise. OIG found that until ICE addresses these technology and staffing limitations, TBML-related imports will potentially continue to go undetected. OIG made two recommendations to ICE to improve efforts to combat TBML. DHS concurred with both recommendations and is working to implement.

Management Directorate (MGMT)

GAO Reports

Title: DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification

Number: GAO-23-106701

Date: 4/20/2023

Summary: This is GAO's eighth assessment of the Department's major acquisitions programs. These programs acquire systems for operations like securing the border, screening travelers, and improving disaster response. GAO found that 18 of the 25 programs reviewed were meeting their cost and schedule goals by the end of FY 2022. Additionally, and as noted by GAO in its report, COVID-19 or changes implemented to address it have affected workforce availability or led to supply chain issues for some DHS major acquisitions programs. GAO found that five of the 25 programs reviewed were seeking approval to adjust their schedule or cost baselines due to COVID-19 effects, per a July 2022 DHS memorandum to address the effects of COVID-19. Five other programs reported COVID-19 cost or schedule effects in FY 2022 but were able to manage them within their baselines. The remaining 15 programs did not report cost or schedule effects related to COVID-19. Finally, GAO found that that 7 of the programs had not identified cybersecurity risks in a memo as required by DHS. As noted by GAO, DHS' major acquisition programs increasingly rely on software and IT systems, increasing potential vulnerability to a cyberattack. GAO recommended that, as DHS updates relevant policies, it clarifies which major acquisition programs are required to have completed cybersecurity risk recommendation memorandums prior to acquisition decision events, and when exemptions apply. DHS concurred with the recommendations and is working to implement.

Title: Federal Facilities: Improved Oversight Needed for Security Recommendations

Number: GAO-23-105649

Date: 5/8/2023

Summary: GAO was asked to review the implementation of countermeasures recommended by the Federal Protective Service (FPS). In this report, GAO identified information that FPS maintains on its assessments and recommendations; identified factors that affect agencies' decisions to act on these recommendations; and examined how the Interagency Security Committee (ISC)—chaired by DHS and with participation from 66 federal agencies—assesses compliance with its security standards and countermeasures. DHS is responsible for security at federal buildings and facilities, and as GAO has previously reported, many federal agencies don't implement many of FPS' recommendations for security improvements. When GAO followed up with agency representatives, they found that most cited cost or feasibility concerns. GAO also found that while DHS requires federal agencies to self-report some information about security recommendations and the status of their implementation, DHS does not have sufficient mechanisms to help verify this information. As noted by GAO in this report, the ISC is required to oversee the implementation of appropriate countermeasures in certain federal facilities, among other responsibilities, and requires non-military executive branch agencies to self-report some information on the degree to which they comply with ISC's federal security standards. However, GAO found that ISC oversight does not verify if these agencies have implemented FPS-recommended countermeasures or documented the acceptance of risk for those countermeasures they do not implement at their facilities. GAO made two recommendations to DHS to improve its oversight ability to assess countermeasure implementation; and to identify the acceptance of risk at facilities where recommended countermeasures are not implemented. DHS concurred with GAO's recommendations and is working to implement.

Title: Law Enforcement: DHS Should Strengthen Use of Force Data Collection and Analysis

Number: GAO-23-105927

Date: 7/24/2023

Summary: Issued on May 25, 2022, Executive Order 14074 required the heads of federal law enforcement agencies, including DHS, to ensure their agencies' use of force policies reflect principles of valuing and preserving human life and meet or exceed the Department of Justice's use of force policy. As part of this report, GAO selected four DHS Components with a primary mission related to law enforcement and that employ the highest number of law enforcement officers: CBP, FPS, ICE, and the Secret Service. GAO reviewed agency directives and guidance, as well as internal and published use of force incident reports from FY 2021 and FY 2022. GAO also interviewed agency officials and officials from a nongeneralizable sample of organizations with knowledge of law enforcement use of force. GAO found that while DHS requires the four agencies reviewed to submit data on uses of force, the data submitted to DHS sometimes undercount the frequency that officers used force against subjects. For example, agencies sometimes submitted data to DHS that counted multiple reportable uses of force as a single "incident." GAO also found that while DHS officials stated that analyzing the use of force data would help guide future policy decisions, DHS had not developed a plan to analyze the data at the time of GAO's review. GAO also found that the four DHS Components have review boards to analyze uses of force from the perspective of training, tactics, policy, and equipment; identify trends and lessons learned; and propose any necessary improvements to policies and procedures. Boards that were in operation from FY 2021 to FY 2022 found that most use of force incidents they reviewed aligned with agency policy. The DHS Components assessed by GAO have applied lessons learned from reviews in various ways, such as revising policy and training. GAO made two recommendations to DHS to provide guidance on how its Components should submit data to DHS for the range of scenarios when force was used multiple times and develop and implement a plan with time frames for analyzing the use of force data its Components submit. DHS agreed with the recommendations and is working to implement.

Title: DHS Acquisitions: Opportunities Exist to Enhance Risk Management

Number: GAO-23-106249

Date: 8/24/2023

Summary: As noted by GAO in this report, DHS spends billions of dollars each year on major purchases like new Coast Guard ships and systems for screening travelers. For these programs to succeed, DHS must manage acquisition risks—potential negative effects on program cost, schedule, or performance. GAO found that the Department's acquisition risk management guidance generally follows best practices developed by GAO and others, but that there's room for improvement. GAO found that DHS was already planning to update this guidance, so GAO recommended ways the guidance can better reflect best practices—for example, by improving program communications with stakeholders. GAO made eight total recommendations to in this report, including that, as DHS updates its risk management guidance, it includes steps to enhance program communication with stakeholders, improve direction to programs on providing current risk data to leadership, and address portfolio risk management. DHS agreed with the recommendations and is working to implement.

Transportation Security Administration (TSA)

GAO Reports

Title: Aviation Security: TSA Should Assess Potential for Discrimination and Better Inform Passengers of the Complaint Process

Number: GAO-23-105201

Date: 11/7/2022

Summary: As noted by GAO in its report, TSA screened over 1.5 million airline passengers per day in 2021 as part of its mission to protect the nation's transportation systems. However, TSA has faced allegations that some of its screening practices may negatively affect certain passengers and has received discrimination complaints. In its review, GAO found that TSA has taken actions, such as establishing procedures and training, that can help to prevent the potential for discrimination in its airline passenger screening practices. However, it has not assessed the extent to which these practices may result in certain passengers being referred for additional screening more often than others. GAO also found that TSA has a process for addressing passenger complaints alleging discrimination but could improve how it informs passengers about this process. GAO is making four recommendations to TSA to collect data on passenger referrals for additional screening; conduct assessments to determine the extent to which its screening practices comply with agency non-discrimination policies; take additional actions to better inform passengers about its discrimination complaint process; and strengthen its ability to analyze discrimination complaints. DHS concurred with these recommendations and is working to implement.

U.S. Coast Guard (USCG)

GAO Reports

Title: Coast Guard: Opportunities Exist to Strengthen Foreign Port Security Assessment Program

Number: GAO-23-105385

Date: 4/18/2023

Summary: As noted in this GAO report, the U.S. Coast Guard is a multi-mission maritime military service within DHS responsible for securing the U.S. maritime transportation system. GAO conducted this review William M. (Mac) Thornberry National Defense Authorization Act for FY 2021 includes a provision for GAO to review the Coast Guard's International Port Security Program. GAO reviewed, among other things, the extent to which the Coast Guard assessed foreign port security from FY 2014 through FY 2022, shared its foreign port assessments, and coordinated capacity building efforts with relevant federal stakeholders. GAO found that since FY 2014, the Coast Guard generally met its triennial foreign port security assessment requirement before the COVID-19 pandemic led it to suspend its country assessment visits during FY 2020 and FY 2021. The program resumed its visits in May 2021. As noted by GAO in its report, the Coast Guard has faced a longstanding challenge in accessing some countries' ports to conduct assessments. In recent years, the service began using alternative approaches—such as using Coast Guard intelligence—to make determinations for some countries it has been unable to visit. However, GAO found that the program has not consistently done so. GAO also found that the program consistently documents the results of its foreign port assessments in various reports, but as of September 2022 had not disseminated its most comprehensive report (known as its annual report) to CBP and other federal agencies that may have a vested interest in receiving it. GAO made six recommendations, including that the Coast Guard document its procedures for using alternative approaches to make foreign port security assessment determinations, share its annual assessment reports with CBP and other federal agencies it identifies as having a vested interest, and establish a process with the State Department for coordinating foreign port security capacity building. DHS concurred with the recommendations and is working to implement.

Title: Coast Guard: Clarifying Emergency Policies and Assessing Needs Could Improve Unit Disaster Preparedness

Number: GAO-23-106409

Date: 7/25/2023

Summary: In this report, GAO examined the extent to which the Coast Guard has clear policies and procedures for obtaining and maintaining emergency food and water for personnel at shore-based field units, and the extent to which the Coast Guard has assessed and documented shore-based field units' needs for emergency food and water. As noted by GAO in its report, the Coast Guard's operational units in the field lead its disaster response efforts, which include rescuing persons in distress and responding to marine pollution incidents. These units are often situated along major waterways and coastlines throughout the U.S. As such, personnel stationed at these units may be vulnerable to a wide variety of natural disaster risks. GAO found that Coast Guard policies about maintaining emergency food and water for field personnel are unclear. GAO also found that while Coast Guard disaster preparedness efforts include various field unit plans and risk assessments, the agency has not comprehensively assessed and documented field units' emergency food and water needs. GAO made three recommendations, including that the Coast Guard clarifies emergency food and water requirements, clarifies procurement policies and procedures, and ensures that its field units assess and document their emergency food and water needs. DHS concurred with these recommendations and is working to implement.

Title: Coast Guard Acquisitions: Polar Security Cutter Needs to Stabilize Design Before Starting Construction and Improve Schedule Oversight

Number: GAO-23-105949

Date: 7/27/2023

Summary:

As noted by GAO in this report, the Coast Guard has stated that it does not have enough polar icebreakers to meet its missions in the Arctic and Antarctic. To address the gap, the Coast Guard is partnering with the U.S. Navy to procure three heavy polar icebreakers, known as Polar Security Cutters. The Coast Guard plans to invest at least $11.6 billion for acquisition, operations, and maintenance of these cutters. GAO was asked to review the acquisition of the Polar Security Cutter's (PSC), including steps taken in the design phase, and progress toward maintaining and extending the life of the *Polar Star*, the Coast Guard’s current and only active heavy polar icebreaker. GAO found that factors effecting progress have included issues with the original design of the new PSCs; a general lack of experience with designing and building polar icebreakers among U.S.-based designers and shipbuilders; and schedule and cost estimates that GAO found to be likely unreliable. While development of the PSCs continues, the Coast Guard intends for its sole icebreaker, the *Polar Star*, to be available until at least the second PSC is operational. GAO found that the Coast Guard has efforts underway to maintain and extend the life of the *Polar Star* and that Coast Guard assessments of the hull found it in good structural condition, but that the cutter's deteriorating electrical and propulsion systems present challenges to the Coast Guard. GAO made two recommendations, including that DHS ensures the design is sufficiently mature before the Coast Guard starts cutter construction and that DHS ensures the Coast Guard adds the third PSC delivery date into its acquisition program baseline. DHS concurred with both recommendations.

OIG Reports

Title: The United States Coast Guard Needs to Determine the Impact and Effectiveness of Its Streamlined Inspection Program

Number: OIG-23-46

Date: 8/30/2023

Summary: As noted by OIG in its report, the Coast Guard has a process to enroll vessels in the Streamlined Inspection Program (SIP) in accordance with the Code of Federal Regulations (C.F.R.). SIP aims to promote a more effective and efficient process to ensure vessels traveling in U.S. waterways comply with regulatory safety requirements. However, OIG found that less than 1% of vessels in the Coast Guard's fleet of responsibility participated in SIP during calendar year 2021. OIG also found that the Coast Guard cannot demonstrate the oversight functions it uses ensure SIP-enrolled vessels remain in continuous compliance with the C.F.R. Lastly, OIG found that since SIP's inception in 1998, the Coast Guard has not identified or assessed the program's contributions to mission success or established key performance indicators for SIP. OIG made three recommendations that, when implemented, will better enable the Coast Guard to assess the effectiveness and efficiency of the SIP program. DHS concurred with the recommendations and is working to implement.

U.S. Citizenship and Immigration Services (USCIS)

GAO Reports

Title: Immigrant Investor Program: Opportunities Exist to Improve Fraud and National Security Risk Monitoring

Number: GAO-23-106452

Date: 3/28/2023

Summary: As noted by GAO, the employment-based fifth preference (EB-5) visa category was created in 1990 to encourage foreign investors to provide capital and promote job creation in the U.S. In turn, investors and eligible family members obtain paths to citizenship. USCIS administers the program and investigates any fraud and national security concerns. GAO found that EB-5 participation declined sharply from FY 2016 to FY 2021, primarily due to fewer Chinese investors. GAO found that USCIS conducted at least one fraud or national security risk assessment on an aspect of the EB-5 program each fiscal year since 2016. In addition, USCIS has undertaken several initiatives to address overall program fraud and national security risks. These include conducting compliance reviews; increased trainings on fraud and national security indicators; and additional screening for investors linked to companies or countries of concern. However, GAO found that while USCIS collects some data on EB-5 fraud and national security concerns that it investigates, it does not have readily available data about the types and characteristics of fraud unique to the program. GAO recommended that USCIS systematically collect and track data on the different types of fraud in the EB-5 program; and develop a process to collect and assess the reasons for denying petitions and applications and terminating EB-5 Regional Centers. DHS concurred with the recommendations and is working to implement.

OIG Reports

Title: USCIS Has Generally Met Statutory Requirements to Adjudicate Asylum Applications from Paroled Afghan Evacuees

Number: OIG-23-40

Date: 8/18/2023

Summary: OIG conducted this review to assess USCIS' ability to meet statutory timelines for adjudicating asylum applications from Afghans arriving in the United States under Operation Allies Welcome (OAW). OIG found that USCIS has met OAW-specific processing timelines established by the Afghanistan Supplemental Appropriations Act of 2022 for the majority of applications that have been filed and has adjusted its operations to expedite adjudications. However, OIG notes that a surge of applications over a short period of time may strain USCIS operations given the required processing timelines and the preexisting non-OAW application backlog. OIG recommend that USCIS continue to evaluate its operations and ensure consistent compliance with statutory timelines for interviewing asylum applicants from the OAW population. DHS concurred with the recommendations and is working to implement.

U.S. Secret Service (USSS)

GAO Reports

Title: Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains

Number: GAO-23-105466

Date: 11/15/2022

Summary: As noted by GAO in this report, and given the ever-increasing cyber threat landscape, the federal government has initiatives underway intended to protect agency IT. One such initiative, a zero trust architecture, is based on the concept that no actor operating outside or within an organization's network should be trusted. The Secret Service relies heavily on the use of IT to support its protection and financial investigations mission. GAO was asked to review cybersecurity at the agency and evaluate implementation of a zero trust architecture. To implement a zero trust architecture, GAO found that the Secret Service developed an implementation with four major milestones. GAO also found that the Secret Service has completed a self-assessment on their progress towards achieving these milestones, and has made progress specifically in implementing cloud services and achieving maturity in event logging. In addition, GAO found that the Secret Service had developed a plan to implement a more advanced internet protocol, but had not fully met longstanding Office of Management and Budget (OMB) requirements for public-facing systems, though GAO also noted that several of the Secret Service's efforts are likely responsive to actions specified in OMB's zero trust strategy issued in January 2022. GAO made two recommendations to the Secret Service, including to transition to a more advanced internet protocol for its public-facing systems and to update its zero trust architecture implementation plan in accordance with the latest OMB guidance. DHS concurred with the recommendations and is working to implement.

Acronyms

APP – Annual Performance Plan

APR – Annual Performance Report

ARPA – American Rescue Plan Act of 2021

BLM – Bureau of Land Management

C.F.R. – Code of Federal Regulations

CAVSS – Centralized Area Video Surveillance System

CBP – U.S. Customs and Border Protection

CISA – Cybersecurity and Infrastructure Security Agency

CODIS – Combined DNA Index System

DHS – Department of Homeland Security

DOI – Department of Interior

EB-5 – Employment-based fifth preference

EFSP – Emergency Food and Shelter Program

ERO – Enforcement and Removal Operations

FBI – Federal Bureau of Investigation

FEMA – Federal Emergency Management Agency

FPS – Federal Protective Service

GAO – U.S. Government Accountability Office

I&A – Office of Intelligence and Analysis

ICE – U.S. Immigration and Customs Enforcement

IoT – Internet of Things

ISC – Interagency Security Committee

IT – Information Technology

LPOE – Land Port of Entry

LSCMS – Logistics Supply Chain Management System

MGMT – Management Directorate

NFIP – National Flood Insurance Program

NIST – National Institute of Standards and Technology

OAW – Operation Allies Welcome

OFO – Office of Field Operations

OIG – Office of Inspector General

OMB – Office of Management and Budget

OT – Operational Technology

POE – Port of Entry

PSC – Polar Security Cutter

QHSR – Quadrennial Homeland Security Review

SIP – Streamlined Inspection Program

SLTT – State, local, tribal, territorial

SRMA – Sector Risk Management Agency

SWB – Southwest border

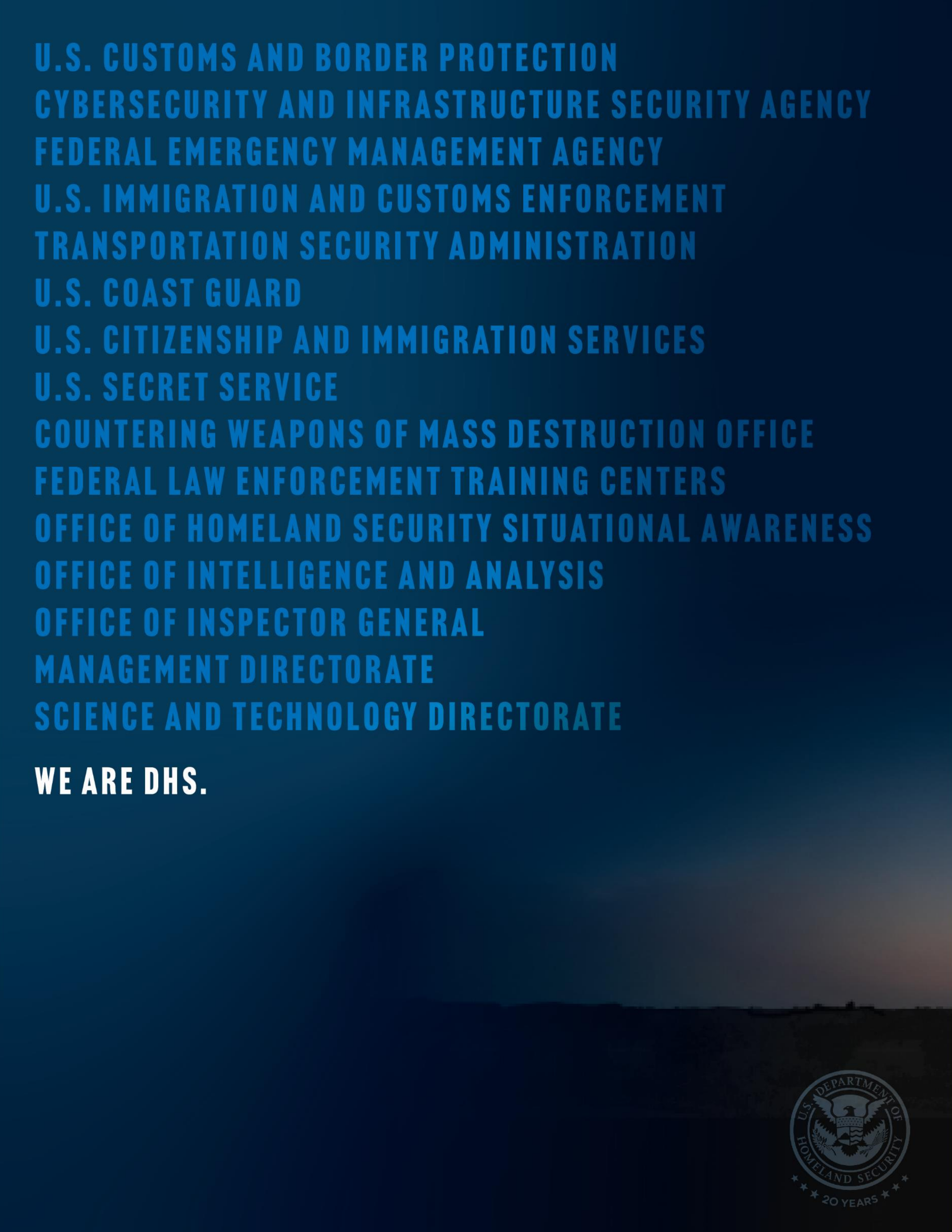
TBML – Trade-based money laundering

TSA – Transportation Security Administration

USCG – U.S. Coast Guard

USCIS – U.S. Citizenship and Immigration Services

USSS – U.S. Secret Service



U.S. CUSTOMS AND BORDER PROTECTION
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
FEDERAL EMERGENCY MANAGEMENT AGENCY
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
TRANSPORTATION SECURITY ADMINISTRATION
U.S. COAST GUARD
U.S. CITIZENSHIP AND IMMIGRATION SERVICES
U.S. SECRET SERVICE
COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE
FEDERAL LAW ENFORCEMENT TRAINING CENTERS
OFFICE OF HOMELAND SECURITY SITUATIONAL AWARENESS
OFFICE OF INTELLIGENCE AND ANALYSIS
OFFICE OF INSPECTOR GENERAL
MANAGEMENT DIRECTORATE
SCIENCE AND TECHNOLOGY DIRECTORATE

WE ARE DHS.

U.S. DEPARTMENT OF HOMELAND SECURITY
20 YEARS