U.S. DEPARTMENT OF HOMELAND SECURITY

# OFFICE OF INSPECTOR GENERAL

Testimony of

**Kristen D. Bernard, Deputy Inspector General for Audits**

and

**Erika Lang, Assistant Inspector General for Inspections & Evaluations**

before the

**Subcommittee on Oversight, Investigations, and Accountability**

**Committee on Homeland Security**

**United States House of Representatives**

**March 11, 2025**
**2:00 PM**

Chairman Brecheen, Ranking Member Thanedar, and Members of the Subcommittee:

Thank you for the opportunity to discuss the Department of Homeland Security (DHS), Office of Inspector General's (OIG) efforts to combat fraud, waste, and abuse in the Department of Homeland Security.

DHS is tasked with safeguarding our Nation from diverse and evolving threats; it operates with over 260,000 personnel and annual total budget authority of over $100 billion. OIG's mission is to promote excellence, integrity, efficiency, and accountability across the vast DHS enterprise. OIG does this by conducting independent oversight through audits, inspections, evaluations, and investigations that identify and prevent fraud, waste, abuse, and mismanagement in DHS's programs and operations.

In Fiscal Year (FY) 2024, DHS OIG identified over $7 billion in funds put to better use, over $19 million in funds recovered or deobligated through audit work, and over $53 million in recoveries, fines, restitution, and asset forfeiture from OIG investigations. We issued nearly 200 recommendations to DHS, evaluated nearly 25,000 hotline complaints, made 110 arrests, and referred over 200 cases for criminal prosecution. OIG provides a remarkable return on investment for the American taxpayer. For every taxpayer dollar invested in DHS OIG, our work returns $18.63[1] in questioned costs, funds put to better use, funds recovered or deobligated, fines, and restitutions.

As the main oversight agency for DHS, OIG has identified systemic weaknesses in border security and immigration enforcement, cybersecurity, and emergency management. Our recent audits, inspections, and investigations have exposed inadequate internal controls, insufficient program management, and inefficient resource allocation that resulted in operational vulnerabilities and financial losses.

In this testimony, OIG highlights key findings from recent reports on border security operations, cybersecurity protections, and emergency management programs that reveal significant challenges and opportunities to improve the integrity, efficiency, and effectiveness of DHS programs.

## DHS Border Security and Immigration Challenges

OIG has allocated significant resources to border security and immigration oversight. In FYs 2022-24, OIG issued 86 reports about DHS' border security challenges, including 297 recommendations to improve the ability of DHS operational components' to secure the Nation's borders and enforce immigration laws. As of today, 222 recommendations (nearly 75 percent) are closed and 75 remain open.

[1] Five-year average return on investment for FY2020-24.

Below, we highlight information from seven key reports issued during this period that specifically assessed U.S. Customs and Border Protection's (CBP) ability to prevent noncitizens from entering the United States, as well as Immigration and Customs Enforcement's (ICE) capacity to safely detain, transport, and track migrants. Based on the volume of migrants that entered the United States, our oversight work in this area focused primarily on DHS's ability to screen, manage, and track all noncitizens crossing the border at and between ports of entry. OIG's work revealed two major areas of weakness:

DHS Screening and Holding Noncitizens Entering the Country Through Ports of Entry

- OIG examined whether DHS had the ability to effectively screen and vet persons seeking admission through ports of entry. Although OIG found that DHS has technology to screen travelers at airports, DHS faced operational challenges in executing day-to-day screening operations. For example, in 2024 OIG reported[2] CBP could not biometrically confirm the identity of all persons seeking entry in vehicles at land ports of entry, nor did CBP maintain consistency in operational procedures to screen all vehicle passengers. We found multiple instances where CBP did not query all individuals at land ports of entry for derogatory information prior to allowing these non-U.S. citizens into the country.

- OIG also assessed DHS' actions[3] related to the screening process of a suspected terrorist, and the timing of an arrest after the suspected terrorist's release into the United States. In 2022, CBP missed multiple opportunities to verify that an apprehended migrant was a positive match for the terrorist watchlist before releasing the migrant into the community. This included not providing information requested by the FBI's Terrorist Screening Center, which would have confirmed the positive match. This occurred because of CBP's ineffective practices and processes for resolving inconclusive matches with the watchlist. Days later when the migrant boarded a domestic US flight, the Transportation Security Administration's normal screening resulted in an alert to the Terrorist Screening Center, leading to ICE being notified to effectuate the migrant's arrest. However, ICE faced multiple challenges planning and conducting the migrant's arrest, including delays in transferring documentation and difficulties obtaining GPS data while conducting the arrest. We issued three recommendations, which are now all closed.

- While examining DHS' ability[4] to assess risks associated with releasing noncitizens without identification into the country and allowing them to travel on domestic flights, OIG determined that CBP and ICE accepted noncitizens' self-reported biographical information in the absence of acceptable forms of identification. CBP and ICE could not

[2] (OIG-24-27), DHS Needs to Improve Its Screening and Vetting of Asylum Seekers and Noncitizens Applying for Admission into the United States (REDACTED), June 7, 2024.
[3] (OIG-23-31), CBP Released a Migrant on a Terrorist Watchlist, and ICE Faced Information Sharing Challenges Planning and Conducting the Arrest (REDACTED), June 28, 2023.
[4] (OIG-24-65), CBP, ICE, and TSA Did Not Fully Assess Risks Associated with Releasing Noncitizens without Identification into the United States and Allowing Them to Travel on Domestic Flights (REDACTED), September 30, 2024.

provide data about how many noncitizens without identification were released into the country. We issued three recommendations—including for CBP and ICE to conduct a comprehensive analysis of the risks associated with releasing noncitizens into the country without proper identification and take steps to mitigate those risks—with which the Department concurred; the recommendations remain resolved and open.

DHS Could Not Track All Migrants Released into the Country

- Between FYs 2022-24, the U.S. Border Patrol (USBP) apprehended more than 5.7 million migrants who illegally entered the United States.[5] Given this volume, OIG sought to determine whether DHS had sufficient capabilities to account for all migrants once apprehended. Over a series of four reports, OIG found that DHS did not have the systems or infrastructure to process the influx of migrants who illegally crossed the border between ports of entry. For example, in 2022 we identified[6] shortcomings with technology systems that resulted in manual methods to transfer and track migrants, which prevented DHS from having digital access to records from the point of apprehension to release or transfer. Given that thousands of migrants are transferred daily, this gap in functionality adversely affects DHS's ability to manage the high volume of apprehensions and timely transfer individuals from USBP custody. OIG also determined DHS shared information manually with the Department of Justice because systems lacked integration, and DHS personnel faced challenges from inconsistent or missing data in DHS' systems of record.

- Similarly, in 2023, we reported[7] DHS had limited ability to track migrants' post-release addresses, as more than 177,000 illegal migrant records were either missing, invalid for delivery, or not legitimate residential locations. In 2024, we reported[8] ICE was unable to locate more than 32,000 unaccompanied migrant children (UCs) who did not appear as scheduled for immigration court proceedings, nor did ICE always inform the U.S. Department of Health & Human Services' Office of Refugee Resettlement when UCs failed to appear in court. OIG found that ICE did not serve a Notice to Appear on more than 291,000 UCs.

- Finally, OIG assessed[9] CBP and ICE processes for detaining and removing inadmissible travelers arriving at a particular international airport. Between FYs 2021-23, CBP released at least 383 inadmissible travelers from custody at the international airport because it

[5] https://www.cbp.gov/newsroom/stats/southwest-land-border-encounters, filtered for FY 2022, 2023, 2024 and U.S. Border Patrol.
[6] (OIG-22-66), DHS Technology Systems Do Not Effectively Support Migrant Tracking at the Southwest Border, September 9, 2022.
[7] (OIG-23-47), DHS Does Not Have Assurance That All Migrants Can be Located Once Released into the United States (REDACTED), September 6, 2023.
[8] (OIG-24-46), Management Alert - ICE Cannot Monitor All Unaccompanied Migrant Children Released from DHS and U.S. Department of Health and Human Services' Custody, August 19, 2024.
[9] (OIG-24-30), CBP and ICE Did Not Have an Effective Process for Detaining and Removing Inadmissible Travelers at an International Airport (REDACTED), June 12, 2024.

could not transfer them to ICE, detain them at the airport, or fly them to another airport. CBP also did not have an effective process to determine which inadmissible travelers failed to return for their removal flights—a population that constituted 44% (168) of inadmissible travelers—and thus did not consistently transfer their cases to ICE for removal proceedings. We made three recommendations, which are all now closed.

DHS Border Security Operations During Operation Allies Welcome

The scope of our border security audit and inspection work has expanded in recent years to include potential vulnerabilities due to exigent circumstances. For example, OIG published six reports related to the resettlement of individuals evacuated from Afghanistan as part of Operation Allies Welcome (OAW); this involved the resettlement of approximately 97,000 evacuees in American communities beginning in September 2021.

- OIG assessed[10] the extent to which DHS screened, vetted, and inspected evacuees arriving as part of OAW and determined CBP did not always have critical data to properly vet Afghan evacuees. Information used to vet evacuees in government databases was sometimes inaccurate, incomplete, or missing. In addition, CBP permitted 35 Afghan evacuees to board a flight without being cleared to travel and did not collect biometrics from 1,299 evacuees prior to their travel to the United States. As a result, DHS paroled at least two evacuees into the United States who posed a risk to national security and the safety of local communities and may have admitted or paroled more individuals of concern.

- OIG reviewed[11] DHS' efforts to track evacuees who independently departed U.S. military bases and how these "independent departures" affected immigration status. Approximately 11,700 Afghan evacuees departed U.S. military bases, or safe havens, without assistance from resettlement agencies. OIG's review found the Unified Coordination Group (UCG)—the entity tasked with coordinating resettlement efforts—struggled to track OAW independent departures evacuees and had difficulties documenting when independent departures occurred. Finally, the UCG did not attempt to locate all evacuees who independently departed safe havens to verify their compliance with parole conditions.

- In assessing[12] DHS's identification and resolution of potentially derogatory records for OAW parolees, OIG found that CBP, U.S. Citizenship and Immigration Services (USCIS),

[10] (OIG-22-64), DHS Encountered Obstacles to Screen, Vet, and Inspect All Evacuees during the Recent Afghanistan Crisis (REDACTED), September 6, 2022.
[11] (OIG-22-79), The Unified Coordination Group Struggled to Track Afghan Evacuees Independently Departing U.S. Military Bases, September 29, 2022.
[12] (OIG-24-24), DHS Has a Fragmented Process for Identifying and Resolving Derogatory Information for Operation Allies Welcome Parolees, May 6, 2024.

and ICE's interconnected processes for identifying and resolving derogatory information for OAW parolees was fragmented. OIG identified USCIS enforcement action gaps for parolees who were denied immigration benefits; specifically, USCIS would not initiate removal proceedings against an OAW parolee or terminate parole when it denied a benefit application due to derogatory information. OIG also determined that no one in DHS had responsibility for monitoring parole expiration for OAW parolees or taking any related action, such as initiating removal proceedings, when derogatory information about a parolee was discovered.

- OIG also reviewed DHS' overall management of OAW to determine if there were any deficiencies or best practices. We found that DHS met processing timelines[13] for the limited number of asylum applicants from the OAW population. However, DHS did not have a structure to support its own volunteers for unfunded operations such as OAW,[14] and the lack of direct funding and absence of clear authority for UCG leadership affected the UCG's coordination of the OAW resettlement process.[15] In total, DHS OIG made 14 recommendations related to OAW. Currently, five recommendations are closed, eight recommendations are resolved and open, and one recommendation, with which the Department did not concur, remains unresolved and open.

Unannounced Inspections of CBP and ICE Facilities

OIG continues to conduct unannounced inspections of both CBP short-term holding facilities and ICE detention facilities, as mandated by Congress in 2019. CBP is responsible for apprehending migrants and detaining them for a short period, typically not to exceed 72 hours, while ICE is responsible for long-term detention. OIG's inspections of CBP and ICE facilities evaluate the Department's compliance with applicable detention standards to ensure they meet federal requirements regarding the safety, well-being, and care of detainees in custody. We use a risk-based, data-driven methodology to determine which facilities to inspect, based on prior inspections, location, size, facility type, DHS OIG Hotline complaints, and historical and current apprehension numbers. Our inspections help ensure facilities comply with standards; improve the efficiency of detention operations; and mitigate risks to the health, welfare, and safety of detainees and DHS personnel.

- OIG issued 16 reports regarding CBP short-term holding facilities from FYs 2022-24, covering 93 USBP and Office of Field Operations facilities. Within those 16 reports, OIG made 39 recommendations to improve the conditions of detainees in detention. Some of

[13] (OIG-23-40), USCIS Has Generally Met Statutory Requirements to Adjudicate Asylum Applications from Paroled Afghan Evacuees, August 18, 2023.
[14] (OIG-22-54), DHS Did Not Adequately or Efficiently Deploy Its Employees to U.S. Military Installations in Support of Operation Allies Welcome, July 27, 2022.
[15] (OIG-22-78), The DHS Unified Coordination Group for Operation Allies Welcome Coordinated Afghan Resettlement but Faced Challenges in Funding And Authority, September 29, 2022.

OIG's most significant recommendations have addressed meeting standards for time in custody, overcrowding, managing detainees with contagious diseases, and handling detainee property. DHS has taken corrective action to close 36 of the 39 recommendations.

- In the same period, OIG issued 13 reports and one management alert related to 13 ICE detention facilities. Within those 14 reports, we made 111 recommendations to improve the conditions of detainees in detention. Generally, areas of non-compliance included environmental health and safety, the use of special management units, staff-detainee communication, dental and chronic care, medical staffing shortages, and grievance systems. We also found that ICE paid approximately $86 million for unused bedspace under contracts in which ICE guarantees minimum payments to detention facility contractors or state and local governments, paying for bed space regardless of use. ICE has taken corrective action to close 106 of the 111 recommendations.

## Cybersecurity Oversight

Cyberspace has become the most active threat domain in the world and a dynamic threat to U.S. security. In 2023, federal agencies reported nearly a 10 percent increase of cybersecurity incidents with over 32,000 total incidents Federal Government-wide.[16] DHS's vast and complex information technology (IT) environment includes more than 800 unique IT systems that process and maintain critical and sensitive mission-related data pertaining to counterterrorism, border security, law enforcement, and critical infrastructure, among other areas. This scale and level of potential exposure requires continuous monitoring and action to ensure cybersecurity threats are identified and remediated timely. Such protections are vital to secure the Departments' systems and information from domestic and foreign adversaries who may wish to exploit vulnerabilities to gain access.

OIG's role is to ensure DHS cyber defenses are adequate to identify, prevent, and mitigate threats. OIG uses a multidisciplinary IT oversight approach with IT auditors leading assessments of management controls, cybersecurity experts providing targeted technical expertise, and technical testing tools to perform real time assessments of system controls to detect weaknesses. OIG's technical testing tools include vulnerability and configuration scans of component workstations, servers, domain controllers, databases, and applications to identify system vulnerabilities and verify settings are correctly implemented.

OIG collaborates closely with DHS officials to maintain awareness of key cybersecurity challenges and priorities, which informs our risk-based approach for selecting the audits to address the Department's most pressing cybersecurity risks and challenges. DHS OIG adds value to the Department by sharing the results of its technical testing to uncover IT security vulnerabilities in real time. Over the past three years, OIG has identified more than 4,000

[16] (FY23-FISMA-Report), Office of Management and Budget, Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2023.

security vulnerabilities, allowing DHS to quickly address vulnerabilities and weaknesses that could potentially be exploited by adversaries.

Since FY 2021, OIG has issued 16 reports containing a total of 99 recommendations aimed at bolstering the Department's cybersecurity protections for systems, networks, and mobile device security.

System and Mobile Device Security Oversight Work

We conducted technical assessments[17] to test security controls of several mission critical systems across CBP, ICE, FEMA, and TSA, finding that additional steps are needed to ensure these sensitive systems are adequately secured. For example, we identified hundreds of workstations that were not receiving security patches to address critical and high vulnerabilities for more than six months and those that were missing the DHS required settings needed to ensure effective system security.

We found significant shortcomings at each of the three DHS Components—USCIS, FEMA, and ICE—we assessed for proper controls[18] to prevent unauthorized access to data and systems. Based on our test samples across these audits, on average 64 percent of the personnel who had either left DHS or transferred to a new position continued to have access to Department systems and information beyond their last day. We also identified hundreds of users who held inappropriate access to privileged accounts—such as administrators with broad and/or special access to system data—with no mission need for their level of access.

OIG completed assessments of mobile device security practices at ICE and FEMA,[19] in which we found weak security practices such as employees installing high risk applications from companies banned by the government and mobile devices that were not wiped even though they were lost, stolen, or taken abroad without appropriate permission. As a result, mobile devices and the sensitive information they contain may be at a higher risk of unauthorized access and more susceptible to cyberattacks.

As we plan our work for Fiscal Year 2026 and beyond, DHS OIG will utilize red team and penetration testing—methods in which OIG conducts a simulated and nondestructive cyberattack— to further enhance our oversight work. We will also employ penetration testing

[17] (OIG-23-43), CBP Implemented Effective Technical Controls to Secure a Selected Tier 1 High Value Asset, August 23, 2023; (OIG-23-44), Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset, August 28, 2023; (OIG-24-53), ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems, September 17, 2024; (OIG-25-08), Cybersecurity System Review of a Selected High Value Asset at CISA, January 15, 2025.

[18] (OIG-22-65), USCIS Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information, September 7, 2022; (OIG-23-16), FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information, February 15, 2023; (OIG-23-33), ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information, July 19, 2023.

[19] (OIG-24-61), ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information, September 26, 2024; (OIG-23-32), FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access, July 7, 2023.

attack methods such as phishing exercises, password cracking, theft of credentials, attempted unauthorized logins, unauthorized input attacks from external sources, malicious payload deployment, identity spoofing to gain trusted access to networks and devices, and unauthorized privilege escalation to continue to ensure DHS has the necessary cybersecurity posture to prevent threats.

## Federal Emergency and Disaster Management

The past several years has been marked by record-breaking catastrophic disasters for management by FEMA, including unprecedented natural disasters and a global pandemic. FEMA has declared 238 major disaster declarations from FY 2022 through the present, such as hurricanes, floods, tornadoes, and wildfires. OIG conducted nearly 40 audits on FEMA, identifying overpayments, ineligible payments, and unsupported payments totaling approximately $12 billion. We have also identified inadequate oversight leading to $9 billion in funds put to better use. Collectively, OIG found that FEMA continues to face significant challenges in three key areas: COVID-19 pandemic response, natural disaster response, and management of other grants.

### FEMA COVID-19 Pandemic Response

Given the unprecedented level of funding provided to FEMA for America's COVID-19 response, most of OIG's FEMA audit work over the past years has related to the pandemic. As of September 2021, FEMA had received nearly $100 billion to assist the Nation in addressing the challenges of the pandemic. The size of these appropriations, coupled with the need to quickly distribute funds, signal an environment ripe for fraud.

OIG has taken a technology-enabled joint audit and investigative approach to overseeing FEMA's COVID funds and programs. OIG auditors were able to quickly identify areas of fraud, waste, and abuse for several specific programs. OIG criminal investigators led the charge against fraud by sharing information on known fraud schemes for similar programs, such as COVID-19 unemployment insurance fraud. OIG's data scientists obtained data sets from partner agencies to conduct in-depth computer matching efforts to support audits.

OIG conducted robust oversight on FEMA's management of COVID-19 assistance programs across 14 audit reports over the past three years. We highlight reports below to illustrate some of the weaknesses in FEMA's management of COVID-19 funding which led to $12 billion in questioned costs and $1.5 billion in funds put to better use.

- In 2022, OIG found that FEMA's Lost Wage Assistance (LWA) program[20] launched the program for state workforce agencies to provide unemployment insurance without first

[20] (OIG-22-28), Management Alert – Reporting Suspected Fraud of Lost Wages Assistance, February 28, 2022; (OIG-22-69), FEMA Did Not Implement Controls to Prevent More than $3.7 Billion in Improper Payments from the Lost Wages Assistance Program, September 16, 2022; (OIG-22-73), More than $2.6 Million in Potentially Fraudulent LWA Payments Were Linked to DHS Employees' Identities, September 27, 2022.

setting clear guidance or controls to mitigate the risk of improper payments. Instead, FEMA relied on state insurance programs to determine eligibility and distribute the funding, resulting in more than $3.7 billion in improper payments. We issued a management alert and two audit reports on this subject containing a total of 15 recommendations to improve FEMA's management of its federal assistance programs and to recover improper payments; 5 recommendations remain open and unresolved.

- OIG in 2022 also found[21] that FEMA did not have effective controls over the Funeral Assistance Program, resulting in over $26 million in ineligible or unallowable funeral expenses. We issued an alert to recommend FEMA immediately establish guardrails for reimbursement expenses and cost exceptions and later issued a final report including six recommendations to improve FEMA's oversight of the funeral assistance program. Two recommendations are open; one is unresolved.

- In 2023, OIG assessed FEMA's oversight of the distribution of COVID-19 medical supplies and equipment. We found[22] that FEMA did not effectively manage the distribution process, nor did it provide sufficient oversight of Project Airbridge, a COVID-19 initiative to reduce shipping times. As a result, FEMA did not have full visibility into the resources shipped and received, hindering its ability to make informed decisions. FEMA may have also paid unnecessary transportation costs and the projects $238 million may have been better spent on COVID-19 initiative. We issued five recommendations to improve FEMA's oversight of future public/private partnerships, all are open and resolved.

- In January 2025, we reported[23] FEMA did not have sufficient oversight over COVID-19 emergency protective measures public assistance funding. FEMA over-obligated at least $1.5 billion in funds for one state's medical staffing grant and did not determine the cost allowability of the $8.1 billion in funds drawn down by the state. Additionally, we reviewed a sample of 20 other grants and identified approximately $32.8 million in improper payments. We issued seven recommendations for FEMA to improve oversight, four remain open and resolved.

COVID-19 Fraud Investigations

In 2021, OIG established a dedicated COVID-19 Fraud Unit (CFU) to focus solely on identifying and investigating fraud related to COVID-19. Due to the large scope of the potential fraud, OIG utilized data analytics to identify large, organized fraud schemes – some of which resulted in millions of dollars being distributed to fraudsters. Our investigations have

[21] (OIG-22-36), Management Alert - FEMA's COVID-19 Funeral Assistance Operating Procedures Are Inconsistent with Previous Interpretation of Long-Standing Regulations for Eligible Funeral Expenses, April 13, 2022; (OIG-23-42), Ineffective Controls Over COVID-19 Funeral Assistance Leave the Program Susceptible to Waste and Abuse, August 22, 2023.
[22] (OIG-23-14), FEMA Did Not Provide Sufficient Oversight of Project Airbridge, February 7, 2023; (OIG 23-34), FEMA Did Not Effectively Manage the Distribution of COVID-19 Medical Supplies and Equipment, July 19, 2023.
[23] (OIG-25-13), FEMA's Insufficient Oversight of COVID-19 Emergency Protective Measures Grants Led to Over $8.1 Billion in Questioned Costs and $1.5 Billion in Over-obligated Funds, January 30, 2025.

identified instances in which recipients, through fraud, received payments that they were not eligible for under the Disaster Relief Fund.

Since the beginning of the pandemic, OIG has received over 8,800 complaints and opened over 600 investigations into COVID-19 fraud. To date, our investigations have resulted in more than 200 indictments, 50 criminal Bills of Information, 162 convictions, and nearly $49 million in recoveries. A sample of OIG significant cases in this area include:

- A New Jersey man was sentenced to six years and nine months in prison and was ordered to pay $4.2 million in restitution for two related COVID-19 fraud cases; one case alleged wire fraud and aggravated identity theft in California and the other case alleged wire fraud in New Jersey. The perpetrator executed a scheme to defraud the California Employment Development Department (EDD) by filing at least 78 fraudulent unemployment insurance claims with EDD, seeking Pandemic Unemployment Assistance and other benefits under the CARES Act. The scheme sought over $2.5 million in unemployment insurance benefits and caused EDD and the United States to incur actual losses exceeding $900,000. The perpetrator also executed a scheme to defraud the Small Business Administration by fraudulently receiving $1.28 million in Economic Injury Disaster Loans funds and withdrawing over $777,000.

- A Georgia woman was sentenced to 12 years in prison for her role in a scheme to defraud the Georgia Department of Labor (GaDOL) out of tens of millions of dollars in benefits meant to assist unemployed individuals during the COVID-19 pandemic. The scammer and her co-conspirators caused more than 5,000 fraudulent unemployment insurance claims to be filed with GaDOL, resulting in at least $30 million in stolen benefits.

- DHS OIG and FBI Phoenix's Violent Street Gang Task Force investigated the Arizona Mexican Mafia (AMM) for COVID pandemic unemployment assistance (PUA) fraud after developing information that AMM prison inmates were engaged in PUA fraud along with other criminal activities, e.g., illegal drugs and stolen property. The AMM is one of the most violent street gangs in Arizona; it exerts significant influence over most Arizona Department of Corrections prison yards. The estimated fraud loss included over $1 million in unemployment benefit payments and nearly $2 million in money laundering activities. Thirty members and/or associates of the gang were indicted on multiple felony charges including fraudulent schemes, conspiracy, money laundering, and participating in a criminal syndicate.

<u>FEMA Management of Disaster Response Programs</u>

DHS OIG will continue robust oversight of FEMA's management of disaster response programs, including the individual assistance program, disaster closeout process, and Puerto Rico's recovery to Hurricane Maria. Over the past three years, 10 audits resulted in nearly $500,000 in questioned costs and over $7 billion in funds put to better use.

- OIG reported in 2022[24] that FEMA did not effectively manage the Individual Assistance Disaster Case Management Program following Hurricane Maria. FEMA did not properly monitor cooperative agreements to ensure non-profit organization were using accounting methods in accordance with Federal requirements. FEMA made advance payments totaling $6.4 million to six nonprofit organizations based on estimates, without reconciling the payments with actual costs. Additionally, FEMA lacked supporting documentation for eight nonprofit organizations totaling $10.7 million. These reports contained three recommendations to improve the programs and management of funds; one is open and resolved and two are closed.

- We recently reported[25] on FEMA's efficiency in closing out disaster declarations for grant programs awarded in 2012 or earlier. We identified 26 programs that remained open beyond their period of performance, totaling nearly $9.4 million in unliquidated funds. FEMA also extended 41 program periods of performance or closeout liquidation periods without detailed and documented justification, delaying project closures by up to 16 years. The 41 programs represent more than $7 billion in unliquidated funds that could potentially be returned to the Disaster Relief Fund. The report contained two recommendations to improve FEMA's closeout of declared disasters, both remain open with one resolved and the other unresolved.

FEMA Grants Management

OIG continues to oversee FEMA's management of its grants and programs. We issued 10 audit reports on these topics, including a review of Humanitarian Relief Funds, the Hazard Mitigation Grant Program, and information technology. Our work assessing FEMA's grants management led to $26 million in questioned costs and $180 million in funds put to better use.

- In 2022 we looked at FEMA's oversight of its Hazard Mitigation Grant program (HMGP) property acquisitions and reported[26] FEMA did not provide assurance that projects were awarded equitably. Grant program officials regularly granted states more funds than needed to complete projects, did not always deobligate unused funds promptly, and did not use Strategic Funds Management, an incremental funding process, as required. We estimate that FEMA could put about $135 million to better use if it strengthens its HMGP project management. We made 4 recommendations to strengthen FEMA's property acquisition activities, and all recommendations are open and resolved.

[24] (OIG-22-77), FEMA Did Not Effectively Manage Disaster Case Management Program Funds in Support of Hurricane Maria Recovery Services, September 29, 2022.
[25] (OIG-24-45), FEMA's Inadequate Oversight Led to Delays in Closing Out Declared Disasters, August 14, 2024.
[26] (OIG-22-46), FEMA Needs to Improve Oversight and Management of Hazard Mitigation Grant Program Property Acquisitions, June 22, 2022.

- Also in 2022, we reported[27] on improvements FEMA could implement to better manage the Emergency Food and Shelter Program to ensure individuals receive aid in a timely manner and that program funding is used in accordance with Federal requirements. From FYs 2017-2020, the Board did not spend about $58 million of the $560 million (10.4 percent) in appropriated grant funds. We made 10 recommendations to improve oversight of the Emergency Food and Shelter Program, FEMA nonconcurred with 3 recommendations. Of those recommendations, 5 are closed and 5 are open and resolved.

- Finally, in 2023 we reported[28] that FEMA should increase oversight to prevent misuse of humanitarian relief funds. We reviewed $12.9 million from 18 local recipient organizations and determined FEMA did not support the $7.4 million in funding provided to them. Additionally, FEMA was unable to provide documentation for families and individuals to whom they provided services. We made 2 recommendations to improve oversight and enforcement for similar future appropriations. One recommendation is closed, and one is open but resolved.

OIG continues to monitor FEMA's disaster response operations and has ongoing audit work to evaluate FEMA's management of claims for the Hermit's Peak/Calf Canyon fires, and adherence to applicable policies when determining community trends that impact disaster survivor assistance for Hurricanes Irene and Milton. We also have work planned to assess FEMA's response to the 2023 wildfire in Lahaina, Hawaii, and recent wildfires in Southern California.

## Access to Information

The Inspector General Act of 1978, as amended, established Offices of Inspector General as "independent and objective" units in departments and large agencies. The Inspector General Empowerment Act of 2016 further protected Inspectors General by confirming that all IGs are entitled to "full and prompt access to agency records" to ensure IGs can conduct their reviews in an efficient manner. This law also allowed IGs to match data across agencies to help uncover wasteful spending and enhance the public's access to information about misconduct among senior government employees.

Beginning with OIG's Semi-Annual Report to Congress (SAR) for the period ending September 30, 2021, and continuing with every subsequent SAR, OIG has documented DHS delays or denials in providing requested information in accordance with the law. These delays and denials have adversely impacted our ability to provide Congress and the public objective and timely oversight of the Department's operations and programs.

Since 2021, OIG has reported 33 delays and 35 denials of access to information by the Department. Examples include:

---

[27] (OIG-22-56), FEMA Needs to Improve Its Oversight of the Emergency Food and Shelter Program, August 10, 2022.
[28] (OIG-23-20), FEMA Should Increase Oversight to Prevent Misuse of Humanitarian Relief Funds, March 28, 2023.

- CBP on three occasions denied OIG access to BorderStat, citing concerns that the OIG would have access to data outside the scope of the announced audit. BorderStat contains data from multiple data sources, such as anti-terrorism matches, cargo processing rates, and passenger processing rates. Most recently, CBP denied our request despite being unable to provide the OIG with a complete set of data to support an ongoing audit.

- FEMA routinely denies OIG requests for access to certain databases citing similar concerns regarding scope. In a recent audit, the FEMA data analytics team was unable to provide the OIG with complete datasets due to the complexity of the FEMA GO database, forcing the OIG to make multiple requests for data extracts. This resulted in a 114-calendar day delay before the OIG received complete data.

- For over three years OIG has been denied access to the DHS Integrated Security Management System (ISMS), run by the Office of the Chief Security Officer, which houses key information on DHS personnel (contractors and staff) related to security processing, such as background and clearance information. Because this is a system of record for key data elements that do not exist elsewhere in DHS, its data is critical for several ongoing OIG reviews. Additionally, access to ISMS is necessary for OIG to perform adequate oversight of DHS's security clearance and adjudication processes, which are integral to the safe, effective functioning of the Department.

## Conclusion

Eliminating fraud, waste, and abuse is not just about recovering lost funds; it is about ensuring that taxpayer dollars are used effectively in the first place. As evidenced through the robust portfolio of reports and investigations highlighted in this testimony, OIG has worked diligently to improve efficiency and effectiveness of the Department of Homeland Security.

OIG can perform this important work due to its independent posture; we conduct objective, non-partisan, and credible oversight, that has identified critical vulnerabilities within the Department, resulted in the recovery of millions of taxpayer dollars, and yielded actionable recommendations to strengthen accountability and efficiency in DHS programs and operations.

We appreciate your support and remain committed to working with Congress, this Subcommittee, DHS leadership, and other stakeholders to promote transparency, efficiency, and accountability throughout the Department.