Federal Housing Finance Agency
Office of Inspector General

Semiannual Report to Congress

April 1, 2026, through September 30, 2026



Table of Contents

Message from the Acting Principal Deputy Inspector General, Performing the Duties of the Inspector General 1

Snapshot of OIG Accomplishments 3

OIG's Oversight 4

- Overview 4
- OIG's Risk-Based Oversight Strategy 4
  - Management and Performance Challenges 4

Investigative Activity 6

- Significant Cases 7
  - Updated Results for Previously Reported Investigations 13
- Criminal Investigative Results 15
  - Loan Origination Schemes 15
  - Fraud Affecting the Enterprises, the FHLBanks, or FHLBank Member Institutions 18
  - Multifamily Schemes 21
  - Short Sale Schemes 22
  - Fraud Affecting the FHLBanks, or FHLBank Member Institutions as a Result of (or Related to) the CARES Act PPP 23
  - Closed Case Summaries 25
- OIG Summary of Investigative Statistics, Including Matters Referred to Prosecutive Authorities, for the Period April 1, 2026, through September 30, 2026 27

OIG's Oversight of FHFA's Programs and Operations During This Reporting Period 28

- Office of Audits 28
- Office of Evaluations 28

Reports and Recommendations 29

- Enterprises 29
- FHLBank System 30
- Agency Operations 30
- FHFA Restrictions on Access to Information Sought by the Office of Evaluations 31

Recommendations 33

Peer Reviews 51

OIG Peer Review Results 51

Outstanding Recommendations from Any Peer Review of OIG 51

Peer Reviews Conducted by OIG and Outstanding Recommendations 51

Communication and Outreach 52

Congress 52

Hotline 52

Coordinated Oversight Activities and Professional Organizations 52

Law Enforcement Outreach 53

Other Inspector General Act Reporting Requirements 54

Review of Legislation and Regulations 54

Monetary Benefits 54

Prior Management Decisions 55

Federal Financial Management Improvement Act of 1996 55

Investigations into Allegations of Employee Misconduct and Whistleblower Retaliation 55

Challenges to OIG Independence and Access to Necessary Agency Information 56

IG Act Information Concerning Reports 57

Index of Information Required by the Inspector General Act 57

Message from the Acting Principal Deputy Inspector General, Performing the Duties of the Inspector General

I am pleased to present this Semiannual Report to Congress summarizing the activities of the Federal Housing Finance Agency (FHFA or Agency) Office of Inspector General (OIG) for the six-month reporting period from April 1, 2026, through September 30, 2026. This report highlights OIG's work fulfilling its statutory mission to promote the economy, efficiency, and effectiveness of FHFA, and prevent and deter fraud, waste, and abuse in the Agency's programs and operations and those of the entities it regulates.

Our oversight focused on mandated work and areas of greatest risk to FHFA and the entities it oversees: Fannie Mae and Freddie Mac (the Enterprises), the Federal Home Loan Bank System, and U.S. Financial Technology, LLC. In our audits, we addressed information systems security at the Agency and the FHLBanks, the Agency's Suspended Counterparty Program, and multifamily credit risk at the Enterprises. We issued timely, evidence-based reports with actionable recommendations to enhance safeguards, improve operations, and protect taxpayer interests.

This reporting period, OIG's investigative work contributed to over $29 million in monetary impacts – including criminal restitution, fines, special assessments, and forfeitures – continuing our trend of results-driven outcomes. OIG advanced its investigative mission by partnering closely with federal, state, and local law enforcement to disrupt sophisticated mortgage-related fraud schemes, hold wrongdoers accountable, and deter misconduct affecting mortgages owned or guaranteed by the Enterprises. Defendants in numerous OIG-supported investigations received substantial prison sentences and were ordered to pay restitution, forfeiture, fines, and assessments. Our cases reflect the complexity of the schemes uncovered, to include fraud in multifamily loans, fraudulent short sales, and fraudulent loan applications under the Coronavirus Aid, Relief, and Economic Security (CARES) Act. These schemes harmed numerous victims – including banks and individuals – and resulted in substantial losses to the Enterprises.

While OIG remains committed to its mission, our office's ability to carry out future oversight has been severely hindered by the Agency's abrupt reduction to our fiscal year (FY) 2027 budget by

approximately 64%. This reduction slashes the $55 million estimate included in the President's Budget for FY 2027. To prevent a funding shortfall, we must shut down our national criminal enforcement program, reduce our mission-critical workforce, and eliminate other areas of important oversight such as our Office of Evaluations, among other cost savings efforts. We describe these efforts as part of this Semiannual Report.

James Hodge
Acting Principal Deputy Inspector General,
Performing the Duties of the Inspector General /s/

October 30, 2026

Snapshot of OIG Accomplishments

Semiannual Reporting Period
April 1, 2026–September 30, 2026

Investigative Activities:	
Indictments / Charges	46
Convictions / Pleas	43
Sentencings	24
Suspended Counterparty Referrals to FHFA	147
Investigative Monetary Results:	
Criminal Restitution	$12,153,876
Criminal Fines / Special Assessments / Forfeitures	$17,326,893
Investigations Total Monetary Results *	$29,480,769
Reports Issued	8
Recommendations Made	55
Questioned Costs	$0

* Includes court-ordered results from individual OIG investigations and joint investigations with other law enforcement organizations.

OIG's Oversight

Overview

The Housing and Economic Recovery Act of 2008 established FHFA (also known as U.S. Federal Housing) in July 2008. FHFA regulates and supervises Fannie Mae and Freddie Mac and their affiliate, U.S. Financial Technology, LLC (U.S. FinTech), as well as the Federal Home Loan Banks (FHLBanks)[1] and the FHLBanks' fiscal agent, the Office of Finance.

FHFA is responsible for ensuring that the regulated entities operate in a safe and sound manner so that they serve as reliable sources of liquidity and funding for housing finance and community investment. As of June 30, 2026, the Enterprises collectively reported more than $7.85 trillion in assets, and the FHLBanks reported approximately $1.44 trillion. FHFA also has served as the Enterprises' conservator since September 2008.

OIG's Risk-Based Oversight Strategy

FHFA's dual roles as the regulated entities' supervisor and the Enterprises' conservator present unique challenges for OIG. These dual responsibilities put FHFA in a position different from that of other federal financial regulators, and OIG structures its oversight program to examine rigorously the Agency's exercise of both responsibilities. As part of that oversight, OIG focuses its work on the areas of greatest risk to FHFA and the regulated entities through investigations, audits, evaluations, and compliance reviews.

Management and Performance Challenges

An integral part of OIG's oversight is to identify and assess FHFA's top management and performance challenges, and to align our work accordingly. We annually report to the FHFA Director our view of the Agency's most significant management and performance challenges that, if not addressed, could adversely affect FHFA's accomplishment of its mission. Our memorandum identifying those challenges for Fiscal Year (FY) 2027 is available on our website.

FHFA's most significant management and performance challenges for FY 2027 are:

- Managing risks in the Enterprises' multifamily lines of business;

[1] Collectively, the Enterprises, U.S. FinTech, and the FHLBanks are the "regulated entities." 12 U.S.C. § 4502(20).

- Managing vulnerability within FHFA's information security programs and at the regulated entities;
- Addressing human capital risk at FHFA and the Enterprises; and
- Overseeing the regulated entities' reliance on counterparties and third parties.

These challenges were repeated from FY 2026. OIG considers these challenges when planning its oversight activities. Identifying vulnerabilities in these and other areas and recommending positive, meaningful actions that the Agency could take to mitigate them and remediate identified deficiencies are important parts of our mission.

Investigative Activity

OIG's investigative mission is to prevent and detect fraud, waste, and abuse in the programs and operations of FHFA and its regulated entities. OIG's Office of Investigations executes its mission by investigating allegations of significant criminal and civil wrongdoing with the potential to affect the Agency and its regulated entities. These investigations are conducted in strict accordance with professional guidelines issued by the Attorney General of the United States and the standards established by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) for investigations, which are known as the *Quality Standards for Investigations,* commonly referred to as the "QSI."

The Office of Investigations comprises highly trained special agents and digital and investigative analysts, supported by attorney advisors in the Office of Counsel. We maximize the impact of our criminal and civil law enforcement efforts by working jointly with federal, state, and local law enforcement agencies nationwide.

The Office of Investigations is the primary federal law enforcement organization that specializes in deterring and detecting fraud perpetrated against the Enterprises, and, in some instances, cases involving financial institutions that are members of the FHLBanks. During the reporting period, OIG's investigations resulted in cumulative orders of criminal restitution, fines, special assessments, and forfeitures of over $29 million.

Fraud schemes that may fall within the Office's investigative purview include:

- Loan/Mortgage Origination – This fraud scheme typically involves the falsifying of borrowers' income, assets, employment histories, and credit profiles to make them more attractive to lenders. Offenders often employ fictitious Social Security numbers and fabricated or altered documents, such as W-2s and bank statements, to cause lenders to make loans they would not otherwise make.

- Multifamily Loans – Multifamily loan fraud relates to loans purchased by the Enterprises to finance multifamily properties.

- Short Sales – Short sales occur when a lender allows a borrower to sell his/her property for less than the debt owed. Fraudulent short sales usually involve a borrower who intentionally misrepresents or fails to disclose material facts to induce a lender to agree to a short sale.

- Loan Modification/Property Disposition – In loan modification/property disposition fraud, fraudulent actors prey on vulnerable homeowners by advertising that they can secure loan modifications if the homeowners pay significant upfront fees or take other

action that enriches the defendant. Typically, these fraudulent actors deliver little or no action, leaving homeowners in a worse position. These schemes can involve hundreds of victims.

- Real Estate Owned (REO) Homes – These homes represent collateral seized to satisfy unpaid mortgage loans. REO inventory has sparked many different schemes either to defraud the Enterprises—using contractors to secure, maintain and repair, price, and ultimately sell their properties—or to defraud individuals seeking to purchase REO properties from the Enterprises.

- Condo Conversion and Builder Bailout – Sellers or developers in these fraud schemes wrongfully conceal from prospective lenders the incentives they have offered to investors and the true value of the properties. The lenders, acting on this misinformation, make loans that are far riskier than they have been led to believe. Such loans often default and go into foreclosure.

- Adverse Possession/Distressed Property – These fraud schemes use illegal adverse possession (also known as "home squatting") or fraudulent documentation to control distressed homes, foreclosed homes, and REO properties. In distressed property schemes, perpetrators falsely purport to assist struggling homeowners seeking to delay or avoid foreclosure. Violators use fraudulent tactics, such as filing false bankruptcy petitions, while collecting significant fees from the homeowners.

- Coronavirus Disease 2019 (COVID) Paycheck Protection Program (PPP) Loans under the CARES Act – Fraud perpetrated against these programs includes schemes where FHLBank member banks are victimized by the submission of PPP applications with false and misleading statements about a company's business operations and payroll expenses. These applications often include supporting documentation that is fabricated or altered, such as false federal tax filings and employee payroll records, to cause loan approval.

A summary of publicly reportable investigative outcomes is included in the Criminal Investigative Results section.

Significant Cases

Our investigations are complex and often span multiple years. This section details significant case events during this semiannual period and material updates for investigations that have been highlighted in previous reporting periods.

Real Estate Investor Pleaded Guilty in $229 Million Origination Fraud Scheme, New Jersey

On May 21, 2026, in the District of New Jersey, Mordichai Weiss pleaded guilty to conspiracy to commit wire fraud for his role in a loan origination fraud scheme that included multifamily properties.

According to documents filed in this case and statements made in court, Weiss conspired with others to deceive lenders into issuing multifamily and commercial mortgage loans in amounts they otherwise would not have approved. Weiss and his conspirators submitted falsified documents to lenders, including altered bank records and fraudulent settlement statements, to misrepresent the true purchase prices of the properties.

In one multifamily transaction, Weiss agreed to purchase an apartment complex in Texas for approximately $66.9 million. Weiss and others provided the lender with a fraudulent purchase agreement reflecting a price of $97.8 million. That inflated figure was repeated across multiple falsified documents submitted in support of the loan. The lender approved and funded a loan of approximately $68.5 million, on which Weiss later defaulted.

Weiss obtained over $229 million in loans from multiple financial institutions through this scheme. Ultimately, he defaulted on the loans, or the loan balances substantially exceeded the value of the underlying collateral, resulting in over $94 million in losses to lenders, including Fannie Mae and Freddie Mac.

Attorney Sentenced in Mortgage Fraud Scheme, Maryland

On June 23, 2026, in the District of Maryland, Jacob Rappaport was sentenced to 15 months in prison and ordered to pay $16,250 in forfeiture for his role in a mortgage fraud scheme involving multifamily and single-family properties.

According to court records, Rappaport, along with Alexander Schultz, co-owner of Limitless Management, LLC (Limitless), a company that bought, sold, and managed real estate, and others conspired to submit false and fictitious information on loan applications to obtain mortgages on multifamily and single-family properties.

A previous semiannual report highlighted the fraudulent multifamily and single-family transactions executed by Schultz and Limitless. Rappaport prepared the contracts for the fraudulent multifamily transaction, which led the lender to believe that the sales price was higher, and the property had inflated equity. Freddie Mac ultimately acquired the fraudulent loan. Rappaport also utilized his attorney trust account to facilitate the return of $2 million in illicit proceeds in the form of “show money” to another conspirator for the fraudulent single-family transactions.

In January 2024, Schultz pleaded guilty to conspiracy to commit bank fraud for his role in this scheme and is awaiting sentencing.

Former Certified Residential Appraiser Sentenced in Fraud Scheme, Texas

On June 24, 2026, in the Eastern District of Texas, Armando Martinez was sentenced to 240 months in prison, five years of supervised release, and ordered to pay $157,529 in restitution for his role in a bank fraud scheme.

According to court records, Martinez, director of Martinez and Associates Appraisal Group, Inc., was a certified residential appraiser until his license was revoked by the Florida Real Estate Appraisal Board. Martinez, through his company, continued to offer appraisal services to mortgage companies and other financial institutions. He prepared false and fraudulent appraisal reports using the name and license number of an unwitting appraiser and directed others to take interior and exterior photos of properties for which he never conducted appraisals. Martinez also altered the insurance certificate for his company to deceive lenders that his company carried suitable liability insurance and issued invoices to the lenders seeking, and receiving, payment for false and fraudulent appraisal reports.

Business Owner Pleaded Guilty in Short Sale Fraud Scheme, California

On September 15, 2026, in the Central District of California, Bruce Majeski pleaded guilty to bank fraud and conspiracy to commit bank fraud for his role in a short sale fraud scheme that caused loss to the Enterprises.

According to court records, Majeski and others, through various business entities, would pitch distressed homeowners a way to sell their home through a short sale while retaining the ability to remain in their home through a lease-back, as well as the ability to repurchase their home through an option-to-buy agreement. Majeski and others would communicate with banks and mortgage lenders on behalf of the homeowners to facilitate the short sale transaction.

Majeski and others signed or caused to be signed documents transmitted to banks and lenders falsely representing that there were no agreements between the buyer and seller to allow the seller to remain in the property or to repurchase the property.

Former Real Estate Agent Pleaded Guilty in Origination Fraud Scheme, New York

On September 1, 2026, in the Southern District of New York, Henry Andrixon pleaded guilty to bank fraud for his role in a loan origination fraud scheme.

According to court documents, Andrixon engaged in a scheme to submit false and fraudulent mortgage loan applications to at least eight different lenders. The applications contained materially false statements, including employment information, to induce lenders to issue

mortgage loans. Andrixon was paid a fee for his services by borrowers and sometimes received a referral fee from a real estate broker.

Andrixon secured more than 50 mortgages totaling over $17 million based on materially false information.

Former Bank President and Business Owners Pleaded Guilty in Bank Fraud Scheme, Oklahoma

During this reporting period, in the Western District of Oklahoma, Danny Seibel pleaded guilty to bank fraud in connection with a bank fraud scheme.

According to court records, Seibel worked for the First National Bank of Lindsay (FNBL), a FHLBank member bank, since 1993 in a variety of positions. At the time of his termination in September 2024, Seibel served as the Bank's president and chief executive officer.

Seibel issued loans to friends, neighbors, and other borrowers, that were never repaid or Seibel never recorded any payments. Additionally, he falsified bank records in relation to the loans he approved or oversaw to give the appearance that the loans were performing. Seibel would also falsely state the purpose of some of the loans he issued, claiming the loans were for real estate improvements, vehicles, or equipment. Instead, the proceeds were used to repay portions of other loans, to gamble, or for day-to-day expenses.

Cody Cordell, an associate of Seibel and a FNBL client, pleaded guilty to conspiracy to commit bank fraud in connection with this scheme. Cordell owned a trucking company and other businesses. Seibel issued loans to Cordell that were never repaid or payments were never recorded. Seibel then entered false information into bank records regarding some of the loans he made to businesses associated with Cordell.

Further, Shaun Christian, also a Seibel associate and a FNBL client, pleaded guilty to conspiracy to commit bank fraud and money laundering. Christian owned several automotive businesses and Seibel issued loans to Christian that were never repaid or payments were never recorded. Seibel then entered false information into bank records regarding some of the loans he made to businesses associated with Christian.

In October 2024, FNBL failed and the Office of the Comptroller of the Currency appointed the Federal Deposit Insurance Corporation as the receiver.

Loan Officers Pleaded Guilty in Large-Scale Origination Fraud Scheme, New Jersey

In the summer of 2026, in the District of New Jersey, two loan officers pleaded guilty for their roles in a large-scale mortgage fraud scheme that included hundreds of loans purchased by the Enterprises.

Christopher Gallo pleaded guilty to conspiracy to commit bank fraud, while Mehmet Elmas pleaded guilty to conspiracy to commit bank fraud, bank fraud, and making false statements on a loan application.

According to court records, Gallo and Elmas were employed by a privately owned licensed residential mortgage lending business. Gallo and Elmas used their positions to engage in a scheme to falsify documents to fraudulently obtain mortgage loans.

The defendants routinely misled lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Additionally, they submitted loan applications falsely stating listed borrowers as primary residents of properties when those properties were intended to be used as rental or investment properties.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers or the financial condition of homeowners' associations to facilitate mortgage loan approval. In a five-year period, the conspirators originated more than $3 billion in loans.

Business Owner and Tax Preparer Pleaded Guilty in Origination Fraud Scheme, North Carolina

During this reporting period, in the Western District of North Carolina, Gregory Harris and Timothy Ingram both pleaded guilty to conspiracy for their roles in a loan origination fraud scheme.

According to court records, Harris was the owner of Mass Marketing Financial Services, LLC, dba Rent Busters ("Rent Busters"), a debt repair service and mortgage loan consulting business. Harris, through Rent Busters, acted as a third-party intermediary or consultant hired by borrowers to assist with obtaining mortgage loans. Harris conspired with tax preparer Timothy Ingram and a loan officer to submit false and fraudulent loan applications to induce mortgage lenders to fund mortgages.

Harris and others referred prospective borrowers to a loan officer to assist them in applying for mortgage loans. Harris would then direct the borrower to Ingram to assist with preparing fraudulent tax returns. Harris and others provided Ingram with borrowers' financial information and directed him to prepare tax returns that showed sufficient income for unqualified borrowers to qualify for loans, which Ingram did. Ingram also prepared and signed certified public accountant (CPA) letters attesting to certain aspects of the borrowers' financial information which were submitted in support of fraudulent loan applications. Ingram was not a CPA.

Former Investment Advisor Sentenced in PPP Fraud Scheme, Florida

On June 25, 2026, in the Middle District of Florida, Jared Eakes was sentenced to 78 months in prison, five years of supervised release, and ordered to pay over $5 million in restitution and $7 million in forfeiture for his role in a scheme to submit false loan applications to obtain PPP loans from lenders that included FHLBank member banks.

According to court documents, Eakes created and controlled corporate entities purportedly engaged in investment management, consulting, and other services, as well as related corporate bank accounts. Eakes used some of these entities and accounts to fraudulently obtain PPP loans for over $4.7 million. Eakes submitted multiple fraudulent PPP loan applications on behalf of various entities containing materially false statements and misrepresentations to include false tax records in support of the loan applications. The applications also contained a certification that the PPP funds would be used to "retain workers and maintain payroll or make mortgage interest payments, lease payments, and utility payments" on behalf of the applying entity. However, the PPP loan proceeds were deposited into Eakes-controlled bank accounts and the funds were used for his own personal enrichment to include stock trading.

A Trial Conviction and Two Guilty Pleas in COVID Relief Fraud Scheme, Florida

On August 18, 2026, in the Southern District of Florida, after a five-day trial, a federal jury convicted James Compere of conspiracy to commit wire fraud, wire fraud, false statements to the Small Business Administration, and conspiracy to commit money laundering for his role in a scheme to submit false loan applications to obtain PPP loans and Economic Injury Disaster Loans (EIDL) from lenders that included FHLBank member banks.

According to court records, Compere, along with Reginald Compere and Yasmeen Ebanks, submitted false and fraudulent PPP and EIDL loan applications on behalf of conspirator-controlled purported businesses. The fraudulent applications generally misrepresented revenue, monthly payroll, and numbers of employees and were supported by falsified documents including tax documents.

Reginald pleaded guilty to conspiracy to commit wire fraud, wire fraud, and false statements to the Small Business Administration while Ebanks pleaded guilty to conspiracy to commit wire fraud in July 2026.

Updated Results for Previously Reported Investigations

Former Bank Chief Financial Officer Sentenced in Bank Fraud Scheme, Nebraska

On July 13, 2026, in the District of Nebraska, Aaron Luneke was sentenced to 36 months in prison and five years of supervised release for his role in a bank fraud scheme that victimized multiple FHLBank member banks.

Luneke's specific scheme and jury trial conviction for bank fraud were reported in the preceding semiannual report.

Public Official and Conspirator Sentenced in Short Sale Fraud Scheme, New Jersey

On June 1, 2026, in the District of New Jersey, a sitting councilman and his conspirator were sentenced for their roles in a short sale fraud scheme which caused a loss to Fannie Mae.

Nathaniel Anderson was sentenced to 12 months and one day in prison, three years of supervised release, and ordered to pay $221,862 in restitution, jointly and severally. Chrisone Anderson was sentenced to time served, three years of supervised release including eight months of home confinement, and ordered to pay $221,862 in restitution, jointly and severally.

The preceding semiannual report featured the Andersons' fraud scheme and their jury trial convictions for conspiracy to commit wire fraud affecting a financial institution, bank fraud, and false statements on a loan application.

Bank Fraud Investigation Yields Additional Results, Texas

Previous reporting periods have highlighted the achieved results of investigating a bank fraud scheme in the Southern District of Texas that encompassed numerous loans totaling more than $60 million with at least $40 million in fraudulent proceeds and multiple victims including FHLBank member banks. The overall scheme involved the preparation and submission of fraudulent loan applications that contained false and fraudulent information supported by false or fictitious income tax returns, financial statements, bank account statements, and equipment invoices.

During this reporting period the following results were realized:

- Business owner Jennifer Williams was sentenced to 12 months and one day in prison, three years of supervised release, and ordered to pay over $6 million in restitution, jointly and severally.
- Business owner Kazem Younes pleaded guilty to conspiracy to commit bank fraud.

- Certified public accountant Jolson Wu pleaded guilty to conspiracy to commit bank fraud.
- Loan officer Siupo Mo was charged by indictment with conspiracy to commit bank fraud and bank fraud, and his prosecution is ongoing.

Business Owner Sentenced in COVID Relief Fraud Scheme, Florida

On July 10, 2026, in the Middle District of Florida, Stephen Gurba was sentenced to 30 months in prison, three years of supervised release, and ordered to pay over $1 million in restitution in connection with a COVID relief fraud scheme.

The aspects of the fraud scheme and Gurba's conviction by a federal jury of wire fraud, aggravated identity theft, and making a false statement to a financial institution were highlighted in the preceding semiannual report.

Criminal Investigative Results

Below are individuals sentenced, convicted, or charged during the reporting period, grouped by fraud category.

Loan Origination Schemes

Former Certified Residential Appraiser Sentenced in Bank Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Armando Martinez	Former Residential Appraiser	Sentenced to 240 months in prison, five years of supervised release, and ordered to pay $157,529 in restitution.	Eastern District of Texas

Conspirator Sentenced in Multi-Layered Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Luis Belevan	Participant	Sentenced to 60 months in prison, three years of supervised release, and ordered to pay $335,235 in restitution, joint and several.	Southern District of Texas

Restitution Ordered in Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Edward Fitzgerald	Financial Advisor	Ordered to pay $2,327,497 in restitution, joint and several.	Eastern District of Virginia
Roberta Dawson	Loan Officer	Ordered to pay $2,285,861 in restitution, joint and several.	Eastern District of Virginia
Jack Dawson II	Participant	Ordered to pay $321,240 in restitution, joint and several.	Eastern District of Virginia

Conspirator Sentenced and Two Guilty Pleas in Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Kimberly Williams	Participant	Pleaded guilty to conspiracy to commit bank fraud.	Middle District of Florida
Kenneth Blair	Participant	Sentenced to 30 months in prison, five years of supervised release, and ordered to pay $178,059 in restitution and $15,475 in forfeiture.	Middle District of Florida
Kenneth Blair	Participant	Pleaded guilty to bank fraud (second guilty plea).	Middle District of Florida

Purported Business Owner Pleaded Guilty in Loan Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Joshua Batista	Participant	Pleaded guilty to making false statements to a financial institution.	Middle District of Florida

Loan Officer Pleaded Guilty in Connection with Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Jason Morales (Mantis)	Loan Officer	Pleaded guilty to bank fraud.	Middle District of Florida

Title Company Owner Pleaded Guilty in Loan Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Michael Saracco	Title Company Owner	Pleaded guilty to wire fraud.	Middle District of Florida

Individual Pleaded Guilty in Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Kiomy Torres	Participant	Pleaded guilty to conspiracy to commit bank fraud.	Middle District of Florida

Loan Officers Pleaded Guilty in Large-Scale Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Christopher Gallo	Loan Officer	Pleaded guilty to conspiracy to commit bank fraud.	District of New Jersey
Mehmet Elmas	Loan Officer	Pleaded guilty to conspiracy to commit bank fraud, bank fraud, and making false statements on a loan application.	District of New Jersey

Conspirator Pleaded Guilty in "Shotgun" Mortgage Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Jorge Flores	Participant	Pleaded guilty to conspiracy to commit bank fraud and bank fraud.	District of New Jersey

Former Real Estate Agent Pleaded Guilty in Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Henry Andrixon	Former Real Estate Agent	Pleaded guilty to bank fraud.	Southern District of New York

Business Owner and Tax Preparer Pleaded Guilty in Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Gregory Harris	Business Owner	Pleaded guilty to conspiracy.	Western District of North Carolina
Timothy Ingram	Tax Preparer	Pleaded guilty to conspiracy.	Western District of North Carolina

Conspirator Pleaded Guilty in Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Tanya Pierre	Participant	Pleaded guilty to conspiracy to commit bank and wire fraud.	District of Massachusetts

Conspirators Charged in Mortgage Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Cleophus Turner	Loan Officer	Charged by indictment with conspiracy to provide false statements to a mortgage lending business and false statements on a loan application.	Northern District of Texas
Maurice Gardner	Document Preparer	Charged by indictment with conspiracy to provide false statements to a mortgage lending business.	Northern District of Texas
Shawna Porter (Randall)	Former Real Estate Agent	Charged by indictment with conspiracy to provide false statements to a mortgage lending business and false statements on a loan application.	Northern District of Texas
Julie Shoumbert	Document Preparer	Charged by indictment with conspiracy to provide false statements to a mortgage lending business.	Northern District of Texas

Fraud Affecting the Enterprises, the FHLBanks, or FHLBank Member Institutions

Conspirator Sentenced in Loan Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Rajendra Parikh	Business Owner	Sentenced to 24 months in prison, three years of supervised release, and ordered to pay $6,010,655 in restitution, joint and several, and $6,000,000 in forfeiture.	District of Maryland

Four Sentenced and One Charged in Loan Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Francisco Granati Poloni	Participant	Sentenced to 48 months in prison and three years of supervised release.	Southern District of Florida
Yuri Rondon Diaz	Participant	Sentenced to 42 months in prison and four years of supervised release.	Southern District of Florida
Fairuz Manun	Participant	Sentenced to time served and four years of supervised release, including 12 months of home confinement, and ordered to pay $30,000 in restitution, joint and several.	Southern District of Florida
Eduardo Ojeda	Participant	Sentenced to time served and four years of supervised release, including nine months of home confinement, and ordered to pay $111,376 in restitution, joint and several.	Southern District of Florida
Jackson Ortuño	Participant	Charged by information with conspiracy.	Southern District of Florida

Former Bank Chief Financial Officer Sentenced in Bank Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Aaron Luneke	Chief Financial Officer	Sentenced to 36 months in prison and five years of supervised release.	District of Nebraska

Bank Officials Charged in Bank Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
John Dubray III	Participant	Charged by indictment with conspiracy to commit bank fraud, bank fraud, embezzlement, and bank bribery.	District of Nebraska
Jill Dubray	Participant	Charged by indictment with conspiracy to commit bank fraud and bank fraud.	District of Nebraska

Conspirators Sentenced in Nationwide Short-Term Rental Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Shray Goel	Participant	Sentenced to 12 months and one day in prison, three years of supervised release, and ordered to pay a $15,000 fine.	Central District of California
Shaunik Raheja	Participant	Sentenced to one year of probation.	Central District of California

Business Owner Charged in Multimillion-Dollar Bank Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Mahender Makhijani	Business Owner	Charged by indictment with bank fraud and making false statements on a loan application.	Central District of California

Conspirator Sentenced in Bank Account Takeover Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Jaquain Fitzgerald	Participant	Sentenced to 26 months in prison, five years of supervised release, and ordered to pay $34,812 in restitution and $6,000 in forfeiture.	Middle District of Florida

A Sentencing, Two Guilty Pleas, and One Charged in Bank Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Jennifer Williams	Business Owner	Sentenced to 12 months and one day in prison, three years of supervised release, and ordered to pay $6,383,204 in restitution, joint and several.	Southern District of Texas
Jolson Wu	Certified Public Accountant	Pleaded guilty to conspiracy to commit bank fraud.	Southern District of Texas
Kazem Younes	Business Owner	Pleaded guilty to conspiracy to commit bank fraud.	Southern District of Texas
Siupo Mo	Banker/Loan Officer	Charged by indictment with conspiracy to commit bank fraud and bank fraud.	Southern District of Texas

Former Bank CEO and Business Owners Pleaded Guilty in Bank Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Danny Seibel	Bank President	Pleaded guilty to bank fraud.	Western District of Oklahoma
Cody Cordell	Business Owner	Pleaded guilty to conspiracy to commit bank fraud and felon in possession of firearms.	Western District of Oklahoma
Shaun Christian	Business Owner	Pleaded guilty to conspiracy to commit bank fraud and money laundering.	Western District of Oklahoma

Multifamily Schemes

Attorney Sentenced in Multifamily Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Jacob Rappaport	Attorney	Sentenced to 15 months in prison and ordered to pay $16,250 in forfeiture.	District of Maryland

Real Estate Investor Pleaded Guilty in $229 Million Origination Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Mordichai Weiss	Real Estate Investor	Pleaded guilty to conspiracy to commit wire fraud.	District of New Jersey

Business Owner Charged in Two Loan Fraud Schemes			
Defendant	**Role**	**Most Recent Action**	**District**
Rodney Rosenstein	Business Owner	Charged by indictment with conspiracy to commit bank fraud and conspiracy to make false statements to influence a mortgage lending business.	District of Arizona

Two Pleaded Guilty in Real Estate Investment Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Nam Phan	Participant	Pleaded guilty to conspiracy to commit wire fraud.	Northern District of California
Mark Hanf	Participant	Pleaded guilty to conspiracy to commit wire fraud and money laundering.	Northern District of California

Short Sale Schemes

Public Official and Conspirator Sentenced in Short Sale Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Nathaniel Anderson	Participant	Sentenced to 12 months and one day in prison, three years of supervised release, and ordered to pay $221,862 in restitution, joint and several.	District of New Jersey
Chrisone Anderson	Participant	Sentenced to time served, three years of supervised release including eight months home confinement, and ordered to pay $221,862 in restitution, joint and several.	District of New Jersey

Business Owner Pleaded Guilty in Short Sale Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Bruce Majeski	Business Owner	Pleaded guilty to conspiracy to commit bank fraud and bank fraud.	Central District of California

Individual Pleaded Guilty in Short Sale Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Stephanie Smith (Parks)	Participant	Pleaded guilty to providing false documentation in connection with mortgage loans insured by the U.S. Department of Housing and Urban Development.	Eastern District of Texas

Fraud Affecting the FHLBanks, or FHLBank Member Institutions as a Result of (or Related to) the CARES Act PPP

Former Investment Advisor Sentenced in PPP Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Jared Eakes	Former Investment Advisor	Sentenced to 78 months in prison, five years of supervised release, and ordered to pay $5,101,200 in restitution and $7,340,742 in forfeiture.	Middle District of Florida

Business Owner Sentenced in COVID Relief Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Stephen Gurba	Business Owner	Sentenced to 30 months in prison, three years of supervised release, and ordered to pay $1,160,488 in restitution.	Middle District of Florida

One Pleaded Guilty and Three Charged in Connection with COVID Relief Fraud			
Defendant	**Role**	**Most Recent Action**	**District**
Rafael Romero	Participant	Pleaded guilty to wire fraud and making a false statement on a loan application.	Middle District of Florida
Yan Daniel Inclan Hernandez	Participant	Charged by indictment with wire fraud and making a false statement on a loan application.	Middle District of Florida
Felix Polanco	Participant	Charged by indictment with wire fraud.	Middle District of Florida
Gina Enciso	Participant	Charged by indictment with wire fraud and making a false statement on a loan application.	Middle District of Florida

Business Owner Sentenced in COVID Relief Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Hallan Felix Iff	Business Owner	Sentenced to 21 months in prison, three years of supervised release, and ordered to pay $2,502,610 in restitution and forfeiture.	Southern District of Florida

One Sentenced and One Charged in COVID Relief Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Francisco Macaya	Participant	Sentenced to six months in prison, two years of supervised release, and ordered to pay $130,500 in restitution.	Southern District of Florida
Michael Medina	Participant	Charged by indictment with conspiracy to commit wire fraud and wire fraud.	Southern District of Florida

Two Pleaded Guilty and One Found Guilty in COVID Relief Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Reginald Compere	Participant	Pleaded guilty to conspiracy to commit wire fraud, wire fraud, and false statements to the Small Business Administration.	Southern District of Florida
Yasmeen Ebanks	Participant	Pleaded guilty to conspiracy to commit wire fraud.	Southern District of Florida
James Compere	Participant	Convicted by a federal jury of conspiracy to commit wire fraud, wire fraud, false statements to the Small Business Administration, and conspiracy to commit money laundering.	Southern District of Florida

Business Owner Pleaded Guilty in COVID Relief Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Anthony Alexander	Business Owner	Pleaded guilty to conspiracy to unlawfully produce and transfer identification documents.	District of Maryland

Purported Business Owner Found Guilty in Multimillion-Dollar COVID Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Nikenson Jean Mathurin	Participant	Convicted by a federal jury of wire fraud and money laundering.	District of New Jersey

Conspirator Charged in Multimillion-Dollar COVID Relief Fraud Scheme			
Defendant	**Role**	**Most Recent Action**	**District**
Jamal Al Shboul	Participant	Charged by indictment with conspiracy to commit wire fraud and wire fraud.	Southern District of Texas

Closed Case Summaries

The Office of Investigations closed eight significant criminal investigations during this reporting period. The criminal investigations resulted in 15 convictions, sentences totaling more than 40 years in prison, and more than $16 million in restitution and forfeiture.

The schemes perpetrated in these cases included: loan origination fraud; multifamily loan fraud; COVID relief fraud that targeted FHLBank member banks; a condominium conversion/builder bailout conspiracy; short sale fraud; deed theft by a notary; and a title company owner who embezzled funds from real estate transactions.

Select summaries are provided below:

A real estate broker and others executed a scheme to secure mortgage loan approvals for unqualified buyers using falsified information and fictitious documents to receive real estate commission payments and cash payments from the unqualified buyers.

In another investigation, a co-chief executive officer of a commercial real estate investment firm and his co-conspirators submitted false financial documents to mortgage lending businesses for underperforming properties. The false financial documents made the properties appear more profitable than they were. This scheme led to a financial institution issuing a $481 million loan for a 43-property transaction.

We also investigated two siblings who conspired to submit eight fraudulent PPP loan applications on behalf of companies they owned or controlled. Numerous false and misleading statements were made in the applications about the companies' respective business operations and payroll expenses and were supported by fabricated documents, including falsified federal tax filings. The fraudulently obtained loan proceeds were used on personal expenses, including investments and home improvements. The government seized more than $400,000 of the more than $600,000 obtained in the fraud scheme.

In a builder bailout investigation, an attorney, real estate developers, and others conspired to defraud mortgage lenders and financial institutions by obtaining millions of dollars in fraudulent mortgages for the purchase of dozens of condominium units. As part of the scheme, the developers facilitated payment of the buyers' down payments, which were not disclosed to the lenders. Scheme participants also submitted false settlement forms, settlement statements, and

other false loan documentation to obtain more than $22 million in fraudulent mortgages on more than 60 properties. The Enterprises purchased or secured many of these mortgages and were awarded over $2.3 million in restitution.

In another case, a notary forged signatures of deceased homeowners deeding their properties to him so he could sell them to unsuspecting buyers. The Enterprises owned mortgages to several properties involved in the scheme.

Finally, in a separate investigation, a title company owner, through his business entities, collected funds from lenders, buyers, and sellers to be held in escrow and distributed in accordance with real property transactions and settlement terms. Instead, he transferred monies between escrow accounts to fund other unrelated real estate closings due to shortfalls in the destination escrow account, without the lenders' knowledge or authorization. Additionally, he diverted funds from the escrow accounts into accounts he controlled to pay for automobiles, home renovation projects, personal travel, and other expenses for personal enrichment.

OIG Summary of Investigative Statistics, Including Matters Referred to Prosecutive Authorities, for the Period April 1, 2026, through September 30, 2026

Reports; Referrals to Federal, State, and Local Prosecuting Authorities; Prosecutions; and Convictions: April 1, 2026 – September 30, 2026*	
Investigative Reports**	23
Criminal Referrals to the Department of Justice	103
Criminal Referrals to State and Local Prosecuting Authorities	8
Indictments and Informations during the Reporting Period that Resulted from Referrals to Prosecutors during Prior Reporting Periods	23
Total Indictments and Informations during the Reporting Period Resulting from OIG Referrals	46
Trials	3
Defendants Tried	3
Convictions / Pleas	43
Sentencings	24

* All criminal charges and successive actions (pleas/convictions/sentencings) are supported with documents filed with the corresponding federal or state court, including non-public (sealed) documents. All referrals made to the Department of Justice and to state prosecutors are captured within each investigative file; these actions are tabulated via a statistical report run in OIG's case management system. Criminal referrals, indictments, and information on this chart include both individuals and entities.

** For the purposes of this table, an investigative report is defined as the Report of Investigation finalized at the conclusion of an investigation, prior to case closure.

OIG's Oversight of FHFA's Programs and Operations During This Reporting Period

OIG fulfills its statutory oversight mission through three operational offices. This section discusses the oversight activities performed by two of those offices: the Office of Audits and the Office of Evaluations. Our Office of Investigations' work is discussed above in the Investigative Activity section.

Office of Audits

The Office of Audits conducts independent and objective performance audits with respect to the Agency's programs and operations. It also undertakes projects to address statutory requirements and stakeholder requests. As required by the Inspector General Act of 1978, as amended (IG Act), the Office of Audits performs its audits in accordance with *Government Auditing Standards* established by the Comptroller General of the United States, commonly referred to as generally accepted government auditing standards, or the Yellow Book. The Office of Audits also oversees certified independent public accounting firms that perform certain audits of FHFA programs and operations.

Office of Evaluations

The Office of Evaluations conducts independent and objective reviews, assessments, and analyses of FHFA's programs and operations. It also conducts compliance reviews to determine whether FHFA has effectively implemented agreed-upon corrective actions to remedy deficiencies identified in prior OIG evaluations, audits, or other reports. To assess compliance, the Office of Evaluations conducts validation testing on selected closed recommendations to confirm whether FHFA took the corrective actions. Under the IG Act, Inspectors General must adhere to the professional standards established by CIGIE. The Office of Evaluations performs its work in accordance with CIGIE's standards for inspections and evaluations, which are known as the *Quality Standards for Inspection and Evaluation*, commonly referred to as the Blue Book.

Reports and Recommendations

OIG issued eight reports during the semiannual period from April 1, 2026, through September 30, 2026:

The Office of General Counsel Provided Sufficient Oversight of the Suspended Counterparty Program But Did Not Document Certain Controls in Its Operating Procedures (AUD-2026-009, September 29, 2026)

DER Designed and Implemented Effective Oversight of the Enterprises' Multifamily Credit Risk Transfer Programs (AUD-2026-008, September 29, 2026)

FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007, September 29, 2026)

FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006, September 28, 2026)

Assessment of DBR's Oversight of the FHLBank System Corporate Governance (AUD-2026-005, September 17, 2026)

Risk Assessment of FHFA's Charge Card Programs April 1, 2025 – March 31, 2026 (OIG-RA-2026-001, September 9, 2026)

Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2026 (AUD-2026-004, July 30, 2026)

DBR's Quality Control Program Did Not Detect a Documentation Deficiency in Its Oversight of the FHLBank System's Information Security and Cybersecurity Risk Management (AUD-2026-003, May 13, 2026)

Each report is available at the links above. We summarize select reports below to highlight the important insights our body of work provides across FHFA's programs and operations, including the entities under the Agency's purview.

Enterprises

FHFA's Division of Enterprise Regulation (DER) regulates and supervises the Enterprises. During this semiannual reporting period, we assessed the Agency's effectiveness in overseeing the Enterprises' multifamily credit risk transfer (CRT) programs. The Enterprises have CRT programs for their multifamily businesses to reduce the risk of loan losses and risk to taxpayers.

The Enterprises reduce these risks by transferring credit risk (risk of losses) to sources of private capital primarily through risk sharing arrangements, and other transactions. In AUD-2026-008, we assessed whether DER designed and implemented effective oversight of the Enterprises' multifamily CRT programs. We found that DER designed and implemented effective oversight of the Enterprises' multifamily CRT programs. We made no recommendations in this report.

FHLBank System

FHFA also serves as supervisor and regulator of the FHLBank System, with these functions being performed by the Agency's Division of Federal Home Loan Bank Regulation (DBR). During this semiannual period, we assessed the Agency's oversight of the FHLBank System's activities related to corporate governance and information security and cybersecurity risk management.

Each FHLBank and the Office of Finance have a board of directors responsible for the strategic direction of the entity and senior management is responsible for implementing it. FHFA has established requirements for the boards of directors and senior management's corporate governance activities in regulation. In AUD-2026-005, we found that DBR provided sufficient oversight of the FHLBank System's corporate governance in compliance with its guidance for examination activities. As a result, we made no recommendations in this report.

As the FHLBank System relies heavily on information systems and other technology to conduct and manage business, the FHLBank System needs to protect the information technology assets and data under its control and manage cybersecurity risks - intentional and unintentional acts that may jeopardize the confidentiality, integrity, or availability of information technology assets and data. In AUD-2026-003, we found although DBR provided sufficient oversight of the FHLBank System's information security and cybersecurity risk management, we also found that DBR's quality control program did not detect and correct an instance in which the examiner analysis supporting a supervisory conclusion was not documented in the examination workpapers. We made one recommendation to address our finding. FHFA agreed to implement corrective actions in response to our recommendation.

Agency Operations

Our work includes both FHFA's oversight of the regulated entities and the Agency's internal operations. During this semiannual reporting period, we reported primarily on information security controls.

In AUD-2026-004, our contracted certified independent public accounting firm evaluated the effectiveness of the Agency's information security programs and practices, including compliance with FISMA and related information security policies, procedures, standards, and guidelines; and

responded to the FY 2025 Inspector General FISMA Reporting Metrics. The contractor found that, while the Agency complied with FISMA and related information security policies and procedures, standards, and guidelines, the Agency's information security programs and practices were not effective. To address these weaknesses, the contractor made four new recommendations to assist the Agency in strengthening its information security programs and practices and noted five open recommendations from prior audits. The Agency did not agree with the recommendations.

In another network and information security audit, AUD-2026-007, we determined FHFA's security controls were not effective in protecting its network and information systems against internal threats. We made 36 recommendations to address our findings. Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly.

FHFA uses the Enterprise Governance, Risk, and Compliance (eGRC) Cloud System, a comprehensive solution to manage risks, ensure compliance, and support oversight activities, including tracking of hotline complaints referred by the OIG. In AUD-2026-006, we determined whether FHFA effectively designed and implemented security controls for its eGRC Cloud System to manage access and protect information in accordance with federal standards and FHFA requirements. We found that FHFA's design and implementation of select security controls for its eGRC Cloud System were not fully effective. While FHFA designed and implemented some of the security controls in accordance with federal standards and FHFA requirements, we found weaknesses in other controls. As a result, we made 12 recommendations to address our findings. Agency management acknowledged receipt of the report but did not express agreement or disagreement with our recommendations. As such, management's response did not address our recommendations.

FHFA Restrictions on Access to Information Sought by the Office of Evaluations

The Office of Evaluations had anticipated issuing at least three evaluation reports regarding FHFA oversight of the Enterprises during this reporting period.[2] None of these evaluation reports, however, have been completed, due to restrictions that FHFA imposed on OIG's access to Enterprise records. To avoid an impasse that would result in escalation of the access issue to Congress, OIG chose to engage in extensive accommodation discussions with FHFA. While we

[2] Two evaluations involve a review of FHFA's oversight of Freddie Mac's and Fannie Mae's monitoring and an assessment of changes in the condition and value of multifamily properties that serve as collateral for loans in each Enterprise's multifamily portfolio. The third was a special project on the effectiveness of Fannie Mae's loan review and approval processes, including its oversight of the lenders' delegated underwriting, for six multifamily loans comprising a large portfolio that defaulted in June 2024.

have recently been given access to information sufficient to allow the evaluations to move forward, the access restrictions caused significant delay. Moreover, due to FHFA's drastic cut to our FY 2027 funding, we will be further impeded from completing for publication all three evaluation reports.

FHFA's refusal to provide Enterprise records and information that OIG requested to conduct a review was unprecedented. OIG first learned of the substantial change in the Agency's position on OIG's authority to access Enterprise records in early 2026 when FHFA questioned OIG's authority to access Enterprise records and information. OIG's Office of Counsel provided FHFA with a memorandum outlining OIG's legal authority to access Enterprise records, explaining that OIG is entitled to access "*all* records, reports, audits, reviews, documents, papers, recommendations, or other material *available to* [FHFA] which relate to [FHFA] programs and operations." 5 U.S.C. § 406(a)(1)(A) (emphasis added). Because FHFA is both the regulator and conservator of the Enterprises, all records of the Enterprises are available to the Agency. Despite several requests, FHFA never responded to the memorandum and continued to deny access to requested information stating, among other things, that it extended beyond OIG's oversight role.

In mid-August 2026, OIG reached an understanding with the Agency that we believed resolved FHFA's challenges to OIG's authority, while providing sufficient access to allow completion of the evaluation reports. However, on August 31, 2026, FHFA notified OIG for the first time that it was drastically reducing OIG's FY 2027 funding. As explained in the section addressing challenges to OIG independence and access to necessary agency information below, FHFA's cut in OIG's funding is an extreme escalation of the Agency's challenge to OIG's authority and independence.

Recommendations

The following table contains all open recommendations through the semiannual reporting period ending September 30, 2026.[3] For a list of all open recommendations, see OIG's Compendium of Unimplemented Recommendations. We currently have one open recommendation with questioned costs, unsupported costs, or funds to be put to better use by management from prior reporting periods.

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020 (AUD-2021-001-3, October 20, 2020)
FHFA should assess whether the Office of Technology and Information Management has sufficient, qualified staff to complete required updates and testing of its contingency plans in accordance with FHFA's standard and National Institute of Standards and Technology requirements, and address any resource constraints that have adversely affected the Office of Technology and Information Management's ability to carry out its contingency planning requirements.	FHFA Did Not Follow All of its Contingency Planning Requirements for the National Mortgage Database (NMDB) or its Correspondence Tracking System (CTS) (AUD-2022-003-3, December 13, 2021)
The FHFA Office of General Counsel's Designated Agency Ethics Official or Alternate Designated Agency Ethics Official should improve the Agency's existing internal controls over its employee financial disclosure process by performing and documenting technical reviews and conflict of interest analysis within 60 days of receiving employee financial disclosure reports as required by Office of Government Ethics regulations and FHFA policy.	FHFA Did Not Always Follow Federal Regulations and Its Policy for Employee Financial Disclosures During Fiscal Years 2020 and 2021 (AUD-2022-011-1, September 8, 2022)

[3] We both issued and closed fourteen recommendations this semiannual reporting period based on the Agency's rejection of those recommendations (AUD-2026-007); therefore, these recommendations do not appear in the open recommendation table.

Open Recommendation	Report Title and Date
The FHFA Office of General Counsel's Designated Agency Ethics Official or Alternate Designated Agency Ethics Official should improve FHFA's existing internal controls over its employee financial disclosure process by ensuring that employees file their financial disclosure reports timely as required by Office of Government Ethics regulations and FHFA policy.	FHFA Did Not Always Follow Federal Regulations and Its Policy for Employee Financial Disclosures During Fiscal Years 2020 and 2021 (AUD-2022-011-3, September 8, 2022)
FHFA's Chief Information Officer should develop and maintain a complete and accurate cloud system component inventory, as required by National Institute of Standards and Technology Special Publication 800-53.	FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines (AUD-2023-002-2, March 8, 2023)
FHFA's Chief Information Officer should develop and implement a solution to encrypt all data-at-rest on the cloud system as required by National Institute of Standards and Technology Special Publication 800-53.	FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines (AUD-2023-002-5, March 8, 2023)
FHFA should develop, document, and implement control activities to ensure that (a) only current FHFA employees are receiving transportation benefits, (b) no employee is improperly participating in both transportation benefit programs, (c) the Transit Benefits System has a record/certification for each employee who receives a transportation benefit, and (d) SmarTrip® cards are physically controlled. Such control activities include periodic reconciliation of approved transit subsidy recipients in the Transit Benefits System to FHFA transit subsidy recipients listed on the Washington Metropolitan Area Transit Authority Monthly Activity Reports, periodic reconciliation of approved transit subsidy recipients to active parking permit recipients, and periodic inventory counts of SmarTrip® cards registered to FHFA and undistributed parking permits. [Closed in June 2019; reopened upon results of compliance testing.]	FHFA Needs to Strengthen Controls over its Employee Transportation Benefits Programs (AUD-2018-013-1, September 25, 2018) and FHFA Did Not Effectively Implement Controls Intended to Ensure the Integrity of Its Employee Transportation Benefits Program (COM-2023-005, June 21, 2023)[4]

[4] When we reopen a recommendation, we typically will not issue a new recommendation number.

Open Recommendation	Report Title and Date
FHFA should ensure that the Transit Benefits System has accurate and up-to-date records of, and current certifications for, each FHFA employee who receives a transportation benefit. [Closed in June 2019; reopened upon results of compliance testing.]	FHFA Needs to Strengthen Controls over its Employee Transportation Benefits Programs (AUD-2018-013-2, September 25, 2018) and FHFA Did Not Effectively Implement Controls Intended to Ensure the Integrity of Its Employee Transportation Benefits Program (COM-2023-005, June 21, 2023)
FHFA's Acting Chief Information Officer should remediate past due exploitable vulnerabilities in accordance with Cybersecurity and Infrastructure Security Agency Binding Operating Directive 22-01 and the Office of Technology and Information Management Vulnerability Management Process.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023 (AUD-2023-004-3, July 26, 2023)
FHFA's Chief Information Officer should restrict user access to the folders and files on FHFA's network in accordance with least privilege principle.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-1, August 12, 2024)
FHFA's Chief Information Officer should identify and implement a solution, in coordination with vendors, to ensure that multifactor authentication is required to access FHFA's network. If there are no viable solutions, document any risk-based decisions, including compensating controls.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-7, August 12, 2024)
FHFA's Chief Information Officer should identify and implement a solution to detect and monitor the transfer of large amounts of data moving across FHFA's network.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-11, August 12, 2024)

Open Recommendation	Report Title and Date
FHFA's Chief Information Officer should identify and implement a solution to detect and prevent controlled unclassified information or personally identifiable information from being transferred outside of FHFA's network to personal accounts on email and cloud-based storage services.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-12, August 12, 2024)
FHFA's Chief Information Officer should determine whether resources can be made available to implement a data loss prevention system to prevent the exfiltration of controlled unclassified information.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-13, August 12, 2024)
FHFA's Chief Information Officer should reevaluate the former Acting Chief Information Officer's risk acceptance related to portable software programs, and implement security controls to detect and prevent users from downloading and running unapproved software on FHFA's system in accordance with National Institute of Standards and Technology and FHFA's Rules of Behavior.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-14, August 12, 2024)
FHFA's Chief Information Officer should monitor and respond to unauthorized software downloads in accordance with FHFA's Common Control Plan.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-15, August 12, 2024)
FHFA's Chief Information Officer should develop a Plan of Action and Milestones to track the remediation of past due Cybersecurity and Infrastructure Security Agency Known Exploitable Vulnerabilities in accordance with Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 22-01 and FHFA's Office of Technology and Information Management Vulnerability Management Process, Revision 2.7 (September 7, 2022). FHFA's Office of Technology and Information Management should implement compensating controls (i.e., isolating systems with un-remediated vulnerabilities) to mitigate the risk of the vulnerabilities.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-17, August 12, 2024)

Open Recommendation	Report Title and Date
FHFA's Chief Information Officer should prioritize existing Office of Technology and Information Management resources based on the Plan of Action and Milestones to ensure that Cybersecurity and Infrastructure Security Agency Known Exploitable Vulnerabilities are remediated in accordance with Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 22-01 and FHFA's Office of Technology and Information Management Vulnerability Management Process, Revision 2.7 (September 7, 2022).	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-18, August 12, 2024)
FHFA's Chief Information Officer should implement security controls to lock down Universal Serial Bus ports so that only authorized Universal Serial Bus devices are allowed.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-21, August 12, 2024)
FHFA's Chief Information Officer should perform annual testing of the contingency plan in accordance with the recovery procedures document to ensure failover and failback are conducted as planned.	FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement (AUD-2024-010-4, September 25, 2024)
FHFA's Chief Information Officer should encrypt all backup data-at-rest at FHFA's alternate site and update the existing Plan of Action and Milestones to include compensating controls until the Plan of Action and Milestones has been closed.	FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement (AUD-2024-010-6, September 25, 2024)
FHFA's Division of Enterprise Regulation (DER) should consider whether to direct Freddie Mac to file an amended Suspicious Activity Report containing a complete narrative for the case identified above, and whether to amend FHFA's examination procedures to require this step if future examinations uncover a similar issue.	Inspection: FHFA Oversight of Freddie Mac's Issuance of Suspicious Activity Reports (COM-2025-005-2, March 27, 2025)

Open Recommendation	Report Title and Date
FHFA's Office of Facilities and Operations Management Associate Director, in coordination with the Office of Human Resources Management should finalize and implement policies and procedures for the Agency's administration of the background investigations and adjudication processes for federal and contractor employees that (a) are consistent with regulations and implementation guidance issued by the United States Office of Personnel Management; (b) assigns roles and responsibilities; (c) establishes specific procedures; and (d) measures operational effectiveness criteria.	FHFA's Controls Over Background Investigations and Adjudications Were Ineffective (AUD-2025-002-1, March 28, 2025)
FHFA's Chief Information Officer should establish and implement guidance for performing National Institute of Standards and Technology Cybersecurity Framework 2.0 activities through policies and procedures.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025 (AUD-2025-004-1, July 30, 2025)
FHFA's Chief Information Officer should create a Plan of Action and Milestones to establish when the annual Disaster Recovery Procedures for FHFA Production Systems exercise will be conducted and when the new system owners will be assigned and trained on their roles and responsibilities related to FHFA General Support System, Office of General Counsel Matter Management Tracking System, and the FHFA Status Tracking and Reporting system.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025 (AUD-2025-004-5, July 30, 2025)
FHFA's Chief Information Officer should schedule and conduct an annual Disaster Recovery Procedures for FHFA Production Systems exercise for the FHFA General Support System, Office of General Counsel Matter Management Tracking System, and the FHFA Status Tracking and Reporting system, and ensure new system owners are trained to execute them.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025 (AUD-2025-004-6, July 30, 2025)

Open Recommendation	Report Title and Date
FHFA's Division of Federal Home Loan Bank Regulation should assess the extent to which Federal Home Loan Banks are relying on redacted ROEs (reports of examination) when reviewing membership applications or performing ongoing monitoring.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-1, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should clarify and reinforce Division of Federal Home Loan Bank Regulation's expectation to the Federal Home Loan Banks that they should request and receive from federal and state regulators ROEs that are not substantively redacted, and that other relevant supervisory reports should be collected when necessary.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-2, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should conduct outreach to federal financial regulators to reinforce the need for compliance with 12 U.S.C. § 1442(a)(1), which requires their production of reports, records, and information relating to the condition of any member of any Federal Home Loan Bank upon request by a Federal Home Loan Bank. As part of this outreach, make clear that such materials extend beyond ROEs, and that materials produced in response to a Federal Home Loan Bank request should be provided without substantive redactions.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-3, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should assess the extent to which restrictions on access to state-issued ROEs may hinder the Federal Home Loan Banks in making fully informed decisions when evaluating applications for membership and when making determinations to limit or deny member requests for advances in accordance with applicable FHFA regulations.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-4, September 18, 2025)

Open Recommendation	Report Title and Date
FHFA's Division of Federal Home Loan Bank Regulation should, if applicable, continue to pursue outreach with the Conference of State Bank Supervisors and state regulators to assist Federal Home Loan Banks in accessing state-issued ROEs.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-5, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should complete its assessment of the extent of weaknesses in the Federal Home Loan Banks' enforcement of members' material adverse change notification requirements, and provide guidance to Federal Home Loan Banks on best practices, such as issuing periodic reminders of notification requirements, to help ensure members' compliance with the Federal Home Loan Banks' contractual requirements.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-6, September 18, 2025)
FHFA's Chief Information Officer should restrict access to member bank submission forms and associated documents to only authenticated and authorized users.	Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data (AUD-2025-007-2, September 25, 2025)
FHFA's Chief Information Officer should establish a formal content review and approval process for all documents and content posted to public-facing websites, including checks for controlled unclassified information data.	Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data (AUD-2025-007-7, September 25, 2025)
FHFA's Chief Information Officer should remediate vulnerabilities by (a) applying all available software and firmware updates to the closed circuit television platform, (b) replacing or renewing expired website security certificates, and (c) conducting a secure code review to identify and remove hardcoded credentials or unsecure configurations.	Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data (AUD-2025-007-19, September 25, 2025)

Open Recommendation	Report Title and Date
FHFA's Division of Federal Home Loan Bank Regulation Deputy Director should ensure that the Office of Risk Analysis and Modeling evaluates its current internal model risk management practices in line with FHFA's model risk management supervisory expectations (defined in Advisory Bulletin 2013-07 and Advisory Bulletin 2022-03) and design controls to (1) periodically review and maintain its model risk inventory (to include a risk-based validation schedule), (2) engage external resources to perform independent model validations in accordance with the validation schedule, and (3) conduct model performance tracking. Further, the Office of Risk Analysis and Modeling should update and finalize its policies and procedures to reflect the internal model risk management practices adopted.	The Division of Federal Home Loan Bank Regulation Needs to Improve Controls Over Internal Model Risk (AUD-2025-009-1, September 29, 2025)
FHFA's Chief Financial Officer should ensure that all staff with invoice approval authority complete the updated training.	FHFA's Controls Over Legal Service Payments Were Generally Effective But Did Not Ensure Compliance With All Contractual Requirements (AUD-2026-001-4, February 17, 2026)
FHFA's Office of Human Resources Management Director should determine the allowability of the questioned reimbursement and stipend costs totaling $65,690 and take appropriate action including recoupment of funds.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-1, March 30, 2026)

Open Recommendation	Report Title and Date
FHFA's Office of Human Resources Management Director should strengthen compliance with applicable policies and procedures over reimbursements and stipends through targeted training of Office of Human Resources Management staff responsible for initiating, reviewing, and approving payments. Training on the requirements of Policy 113, the Duty Station Policy, and other applicable guidance should reinforce the following: a. Reimbursements must be supported by verifiable documentation of an employee's eligible job-related expenses with required, supporting documentation; b. Payments must not exceed reimbursement and stipend thresholds and must be accurate; c. Stipends should be issued exclusively to employees who meet eligibility criteria; and d. Agreements and other certifications must be properly executed and maintained.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-2, March 30, 2026)
FHFA's Office of Human Resources Management Director should develop and implement standardized controls to systematically review and verify the accuracy of out-stationed employee stipend payments for consistency across the Agency.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-3, March 30, 2026)
FHFA's Office of Human Resources Management Director should conduct periodic testing of controls over reimbursements and stipends to ensure payments are made in accordance with Policy 113 and other applicable guidance.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-4, March 30, 2026)
FHFA's Division of Federal Home Loan Bank Regulation Deputy Director should reinforce controls governing out-stationed employee stipends through periodic reminders and targeted training of officials responsible to ensure recipient eligibility, accurate payment through coordination with Office of Human Resources Management, as necessary, and maintenance of properly executed duty station agreements.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-5, March 30, 2026)

Open Recommendation	Report Title and Date
FHFA's Division of Federal Home Loan Bank Regulation Deputy Director should train Division of Federal Home Loan Bank Regulation staff responsible for initiating, reviewing, processing, and approving stipends on the requirements of Policy 113, 2021-DBR-OPB-04, the Duty Station Policy, and any procedural updates.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-6, March 30, 2026)
FHFA's Office of Human Resources Management Director should develop a centralized recordkeeping system for managing reimbursement and stipend records that allows timely and accurate retrieval of supporting documentation.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-7, March 30, 2026)
FHFA's Office of Human Resources Management Director should perform periodic checks of reimbursement and stipend documents to verify that they are accurate, complete, and have been retained for the required period of time.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-8, March 30, 2026)
FHFA's Office of Human Resources Management Director should provide supplemental, as-needed training to FHFA staff responsible for initiating, reviewing, and approving reimbursements and stipends on the requirements of FHFA's Records and Information Management Policy; FHFA's Comprehensive Records Schedule; and the National Archives and Records Administration's General Records Schedules when retaining information and documentation created under Policy 113 and any corresponding updates. This training should complement, not replace, other mandatory training.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-9, March 30, 2026)
FHFA's Enterprise Governance, Risk, and Compliance System Owner should ensure that the three privileged users are provisioned with separate standard user accounts for routine activities and use privileged accounts only when elevated access is required in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-1, September 28, 2026)

Open Recommendation	Report Title and Date
FHFA's Enterprise Governance, Risk, and Compliance system owner should review the 19 inactive user accounts on the Enterprise Governance, Risk, and Compliance Cloud System and determine if they should be disabled in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-2, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should in coordination with FHFA's Chief Information Officer, implement a mechanism to identify and disable user accounts after 35 days of application-level inactivity, in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-3, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should document procedures for sanitizing hotline complaint records when entering them into the system to ensure sensitive information is not included.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-4, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should fully sanitize the two hotline complaint records that contain sensitive information in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-5, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should remove the two hotline complaint records that were transferred to the pre-production environment in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-6, September 28, 2026)

Open Recommendation	Report Title and Date
FHFA's Enterprise Governance, Risk, and Compliance system owner should update the Enterprise Governance, Risk, and Compliance Cloud System Customer Controls document in accordance with National Institute of Standards and Technology Special Publication 800-18 to: a. Describe the 87 of 92 controls that FHFA was responsible for implementing for the production environment; b. Describe the security controls for the pre-production environment; c. Document all inherited controls and reference the FHFA System Security and Privacy Plan for the General Support System or FHFA Common Control Plan; d. Identify the system's name, security categorization, impact level, operational status, system type, and authorizing official; and e. Define the system's environment and security authorization boundary.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-7, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should reset the password of the system administrator account and ensure the new password meets the password strength requirements in accordance with the FHFA Identification and Authentication Standard.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-8, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should enable and enforce multifactor authentication for access to the pre-production environment in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-9, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should ensure that user accounts used for testing in the pre-production environment include information linking to the identity of the account owner in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-10, September 28, 2026)

Open Recommendation	Report Title and Date
FHFA's Enterprise Governance, Risk, and Compliance system owner should ensure that the contractor account includes unique identifiers in accordance with the customer responsibility matrix.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-11, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should ensure that audit logs for the pre-production environment are reviewed as needed or on a quarterly basis in accordance with the Enterprise Governance, Risk, and Compliance Cloud System Customer Controls document and National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-12, September 28, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-1, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-2, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-3, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-4, September 29, 2026)

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-5, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-6, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-7, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-8, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-10, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-11, September 29, 2026)

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-12, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-13, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-14, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-15, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-16, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-17, September 29, 2026)

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-20, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-22, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-23, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-30, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-31, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-32, September 29, 2026)

Open Recommendation	Report Title and Date
FHFA's General Counsel should document procedures for the Agency's administration of the following Suspended Counterparty Program processes: (1) performing quality checks for completeness to ensure referrals are properly tracked, verified, and processed; and (2) assessing the performance of the Suspended Counterparty Program.	The Office of General Counsel Provided Sufficient Oversight of the Suspended Counterparty Program But Did Not Document Certain Controls in Its Operating Procedures (AUD-2026-009-1, September 29, 2026)
FHFA's General Counsel should ensure incorporation of the final suspension appeals process into the overall Suspended Counterparty Program Operating Procedures is completed and communicated to Suspended Counterparty Program staff.	The Office of General Counsel Provided Sufficient Oversight of the Suspended Counterparty Program But Did Not Document Certain Controls in Its Operating Procedures (AUD-2026-009-2, September 29, 2026)

Peer Reviews

OIG Peer Review Results

Peer Review Results	Date Reported
Office of Audits: The United States Securities and Exchange Commission OIG conducted the most recent peer review of OA. OIG received an external peer review rating of pass, the highest rating an audit organization can receive.	September 3, 2025
Office of Evaluations: The United States Postal Service OIG conducted the most recent peer review of OE. OIG received an external peer review rating of pass, the highest rating under applicable peer review standards.	August 6, 2025
Office of Investigations: The most recent peer review of our investigative function was conducted by the General Services Administration (GSA) OIG. GSA-OIG issued an Opinion Letter and a Letter of Observations detailing the results of its review. In the Opinion Letter, GSA-OIG reported that OIG's system of internal safeguards and management procedures for our investigative function complied with the quality standards established by CIGIE and the applicable Attorney General guidelines. In the Letter of Observations, GSA-OIG recognized OIG for employing three "best practices" in its investigative operations.	July 5, 2023

Outstanding Recommendations from Any Peer Review of OIG

OIG has no outstanding recommendations from any peer reviews.

Peer Reviews Conducted by OIG and Outstanding Recommendations

OIG did not conduct any peer reviews during this period, and there are no outstanding recommendations from peer reviews conducted by OIG.

Communication and Outreach

OIG prioritizes outreach and engagement to communicate its mission and work to members of Congress and to the public and to actively participate in government-wide oversight community activities. We continue to forge public and private partnerships to address fraud and coordinate oversight activities.

Congress

To fulfill its mission, OIG works closely with Congress and is committed to keeping it fully apprised of our oversight of FHFA. During this semiannual reporting period, we provided information on OIG's work to congressional staff, including notification of the Agency's decision to drastically reduce OIG funding 30 days before the start of FY 2027.

Hotline

The OIG Hotline serves as a vehicle through which employees of the Agency, the Enterprises, the FHLBanks, and members of the public can report suspected fraud, waste, abuse, mismanagement, or misconduct in Agency programs and operations. The Hotline is managed by OIG's Office of Investigations, and potential criminal violations are investigated by that office. Potential civil or administrative matters are retained or referred to the appropriate OIG operating division for review and follow-up, as appropriate. During this reporting period, 3,423 discrete contacts to the Hotline were made involving tips, complaints, and referrals. This included 418 separate complaints logged by the Hotline.

For more information about OIG's Hotline, including OIG contact information, see https://www.fhfaoig.gov/report-fraud-waste-or-abuse.

Coordinated Oversight Activities and Professional Organizations

During the reporting period, OIG maintained active participation in coordinated oversight activities and professional organizations, including the following:

Council of the Inspectors General on Integrity and Efficiency

OIG actively participated in various CIGIE committees and working groups, including the Audit Committee, the Inspection and Evaluation Committee, the Investigations Committee, and the Technology Committee Artificial Intelligence (AI) working group. OIG also actively supports

CIGIE's efforts to work collaboratively with international partners to counter fraud targeting the public sector through its participation in the International Public Sector Fraud Forum (IPSFF). The IPSFF consists of representatives from the governments of Australia, Canada, New Zealand, the United Kingdom, and the United States. The Forum aims to collectively share best and leading practices in fraud risk management, specifically relating to fraud schemes that target the public sector.

Council of Inspectors General on Financial Oversight

The Council of Inspectors General on Financial Oversight (CIGFO) was created by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 to oversee the Financial Stability Oversight Council (FSOC), which is charged with identifying risks to the financial stability of the United States, promoting market discipline, and responding to emerging risks to the stability of the U.S. financial system.

OIG is a statutory member of CIGFO, along with the IGs of the Department of the Treasury, Federal Deposit Insurance Corporation, Securities and Exchange Commission, and others. By statute, CIGFO may convene working groups to evaluate the effectiveness and internal operations of FSOC.

Additionally, in accordance with the Act, CIGFO issues an annual report to FSOC and to Congress that includes: (1) a section by each member IG that highlights the concerns and recommendations of the IG based on ongoing and completed work, with a focus on issues that may apply to the broader financial sector; and (2) a summary of the general observations by the Council with a focus on measures that should be taken to improve financial oversight.

CIGFO's annual report for 2026, issued in July 2026, is available on its website.

Additionally, OIG leadership and staff serve in various significant public and private professional organizations supporting CIGIE, CIGFO, and the federal community.

Law Enforcement Outreach

Federal Bureau of Investigation (FBI) Cybercrimes Task Force

The FBI's Washington, D.C., field office spearheads a multiagency cybercrimes task force, and OIG assigns special agents to assist with task force law enforcement activities. OIG makes these assignments to help combat cybercrimes and to work in partnership with multiple federal agencies. This concerted effort helps prosecute cybercriminals and stop cyberattacks made against institutions maintaining personally identifiable information, trade secrets, and financial data.

Public Awareness of OIG's Law Enforcement Mission

During this reporting period, OIG delivered 30 fraud awareness briefings to diverse audiences to raise awareness of its law enforcement mission and fraud schemes targeting FHFA programs.

Public-Private Partnerships

Housing finance professionals are on the frontlines and often have a real-time understanding of emerging threats and misconduct. OIG speaks with officials at the Enterprises and the FHLBanks regularly to benefit from their insights. OIG also makes presentations to academic and industry groups.

Coordination Among Law Enforcement Agencies

OIG has developed ongoing and close working relationships with other law enforcement agencies, including: Department of Justice and U.S. Attorneys' offices; FBI; Department of Housing and Urban Development OIG; Federal Deposit Insurance Corporation OIG; Internal Revenue Service–Criminal Investigation; the U.S. Postal Inspection Service; Small Business Administration OIG; the U.S. Trustee Program (nationwide); Financial Crimes Enforcement Network; state attorneys general; and other federal, state, and local law enforcement agencies nationwide.

Other Inspector General Act Reporting Requirements

Review of Legislation and Regulations

OIG, through its Office of Counsel, stays up to date on all applicable proposed legislation that is publicly available or disseminated by the CIGIE Legislation Committee. When appropriate, OIG comments on enacted law or proposed legislative matters relating to FHFA's programs and operations. OIG's Office of Counsel also reviews all proposed regulations pertaining to FHFA and provides recommendations when appropriate.

Monetary Benefits

We did not have any recommendations regarding questioned costs, unsupported costs, or funds to be put to better use by management.

Prior Management Decisions

We do not have reportable information for this period regarding management decisions related to an audit, inspection, evaluation, or compliance review issued in a previous reporting period.

Federal Financial Management Improvement Act of 1996

For the semiannual reporting period ending September 30, 2026, Section 5(a)(7) of the IG Act did not apply to the Agency or OIG.[5]

Investigations into Allegations of Employee Misconduct and Whistleblower Retaliation[6]

Pursuant to the IG Act, Sections 5(a)(13), (14), (16)(B), and 5(g), OIG is required to report certain information regarding: (1) investigations involving senior government employees; and (2) government officials found to have engaged in whistleblower retaliation.

Sections 5(a)(13) and 5(g) of the IG Act require that OIG report—to the extent that public disclosure of the information is not prohibited by law (e.g., the Privacy Act of 1974)—on each investigation it conducted involving a senior government employee when allegations of misconduct were substantiated. OIG completed an administrative inquiry into an allegation that an FHFA senior leader may have altered and/or forged a supervisor's signature on multiple annual leave restoration forms. The inquiry revealed that the employee reused a supervisor's electronic signature without authorization and submitted modified documents without supervisory review or approval. The inquiry did not substantiate that the employee submitted a fabricated or misleading Microsoft Teams excerpt as part of supporting documentation. Accordingly, the matter was referred to FHFA management for administrative review and appropriate corrective or disciplinary action.

Sections 5(a)(14) and 5(g) of the IG Act require that OIG report — to the extent that public disclosure of the information is not prohibited by law — on any instance of whistleblower retaliation, including information about an official found to have engaged in retaliation. OIG does not have reportable information for this period.

Sections 5(a)(16)(B) and 5(g) of the IG Act require that OIG report — to the extent that public disclosure of the information is not prohibited by law — on each investigation it conducted

[5] This paragraph reflects the IG Act Section 5 semiannual report requirement as amended by Pub. L. No. 117-263, § 5273(2) (Dec. 23, 2022).

[6] This portion of the Semiannual Report to Congress shows the IG Act Section 5 semiannual report requirements as amended by Pub. L. No. 117-263, §§ 5235(1), 5273(2) (Dec. 23, 2022).

involving a senior government employee that is closed and was not disclosed to the public. OIG does not have reportable information for this period.

Challenges to OIG Independence and Access to Necessary Agency Information

As noted above, OIG's Office of Evaluations was unable to publish three reports this SAR period due to FHFA's refusal to provide Enterprise records and information when requested. Furthermore, on August 31, 2026 – just one month before the beginning of the fiscal year – FHFA notified OIG for the first time that it intended to reduce OIG's FY 2027 budget by approximately 64% below the funding provided to the OIG in the President's Budget for FY 2027.[7]

Upon receipt of this notice, OIG engaged in extensive dialogue with FHFA to explain and justify its budgetary requirements in the brief window of time before the fiscal year's start. The dialogue with FHFA did not alter the Agency's decision to unilaterally reduce OIG's budget.

We notified our oversight committees of the devastating consequences of FHFA's severe budget reductions to our ability to carry out our mission.[8] The unprecedented and abrupt cuts will prevent OIG from conducting meaningful oversight of FHFA going forward. The budget provided will force OIG to cut 70%-80% of its mission-critical workforce and will, at best, permit OIG to conduct only those audits that are required by statute. More meaningful audits and evaluations targeted to assess the effectiveness of FHFA programs will not be possible. Moreover, the investigative work that our specialized investigators conduct to identify, investigate, and prosecute fraud in the Enterprises will cease.

Since its inception, the OIG's funding and staffing level have been directly benchmarked to the operational budgets and staffing of the Enterprises and FHLBanks. The funding level for OIG in the President's Budget for FY 2027 directly reflects application of this benchmark. By reducing our budget by approximately 64%, FHFA has substantially degraded OIG's ability to fulfill its statutory mission and eviscerated our capacity to identify, investigate, and deter mortgage, bank, and other fraud involving the Enterprises and FHLBanks.

[7] *See* https://www.whitehouse.gov/wp-content/uploads/2026/04/oia_fy2027.pdf at p. 1207, published April 2, 2026.

[8] *See* https://www.banking.senate.gov/imo/media/doc/FHFA-OIG%20Funding%20Notification%20Letter%20to%20Congress%2009.30.26.pdf

IG Act Information Concerning Reports

During this reporting period, we did not close any inspection, evaluation, or audit without disclosing the report's existence to the public.[9]

Index of Information Required by the Inspector General Act

The IG Act provides that OIG shall, not later than April 30 and October 31 of each year, prepare semiannual reports summarizing our activities during the immediately preceding six-month periods ending March 31 and September 30.

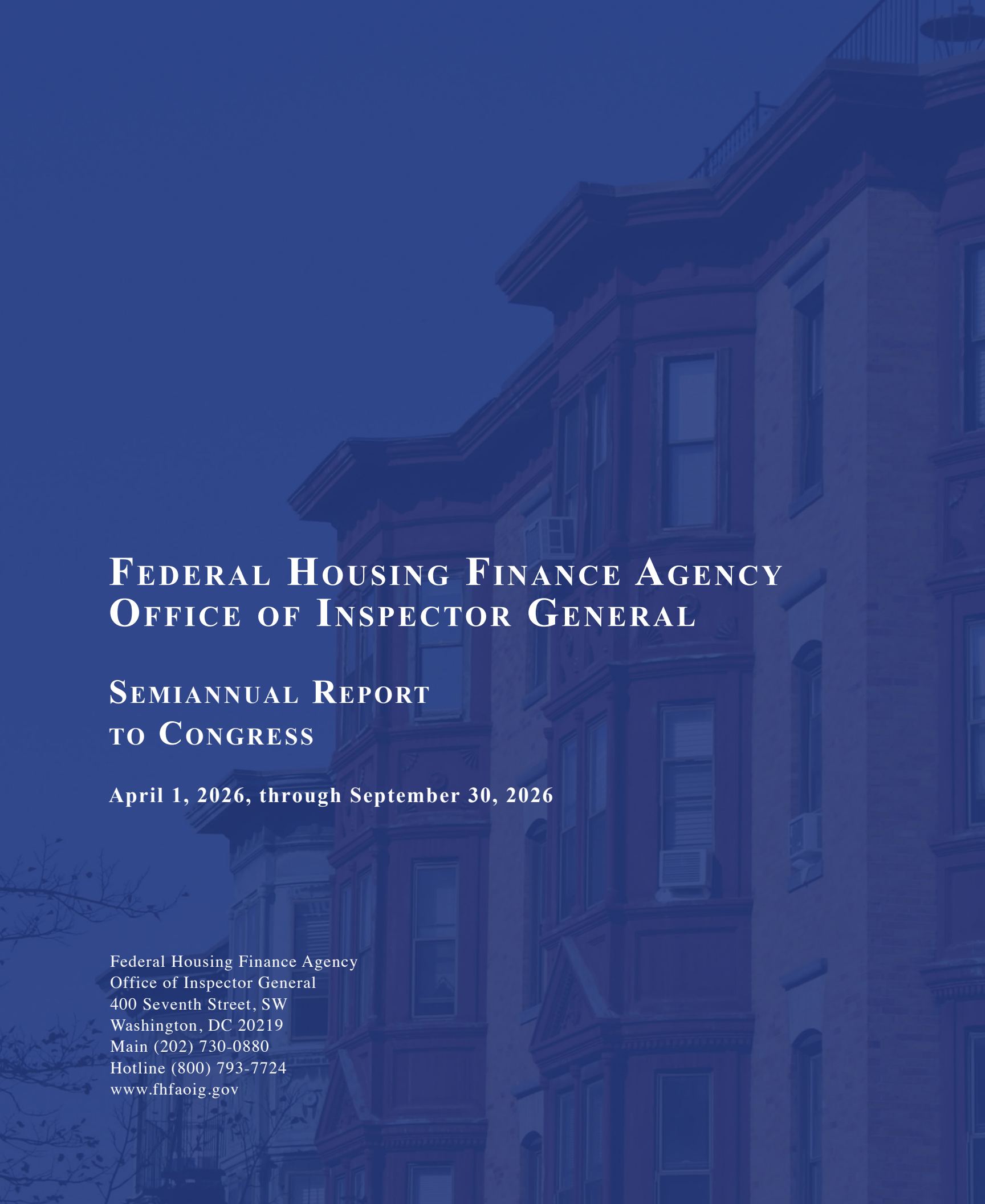
Below is a table directing the reader to the pages of this report on which various information required by the IG Act is provided.

[9] We have previously issued reports that contained information identified by OIG as non-public, privileged, or otherwise protected from disclosure under applicable law; accordingly, OIG has not publicly disclosed such contents. We have provided unredacted reports to FHFA and made them available to our Congressional oversight committees.

Source/Requirement[10]	Pages
Section 4(a)(2) – Review of legislation and regulations.	54
Section 5(a)(1) – A description of significant problems, abuses, and deficiencies relating to the administration of programs and operations of FHFA and associated reports and recommendations for corrective action made by OIG.	4-5, 28-50
Section 5(a)(2) – An identification of each recommendation made before the reporting period, for which corrective action has not been completed, including the potential costs savings associated with the recommendation.	33
Section 5(a)(3) – A summary of significant investigations closed.	25-26
Section 5(a)(4) – An identification of the total number of convictions resulting from investigations.	3, 27
Section 5(a)(5) – Information regarding each audit, inspection, or evaluation report issued, including a listing of each audit, inspection, or evaluation, and if applicable, the total dollar value of questioned costs (including a separate category for the dollar value of unsupported costs) and the dollar value of recommendations that funds be put to better use, including whether a management decision had been made.	28-32, 54
Section 5(a)(6) – Information regarding any management decision made this period with respect to any audit, inspection, or evaluation issued during a previous reporting period.	55
Section 5(a)(7) – The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	55
Section 5(a)(8) – An appendix containing the results of any peer review conducted by another IG; or the date of the last peer review if no peer review was conducted during the reporting period.	51
Section 5(a)(9) – A list of any outstanding recommendations from any peer review conducted by another IG that have not been fully implemented.	51

[10] This table shows the IG Act Section 5 semiannual report requirements as amended by Pub. L. No. 117-263, § 5273(2) (Dec. 23, 2022).

Source/Requirement	Pages
Section 5(a)(10) – A list of any peer reviews of another IG during the reporting period, including a list of any outstanding recommendations made from any previous peer review that remain outstanding or have not been fully implemented.	51
Section 5(a)(11) – Statistical tables showing, for the reporting period, the total number of: investigative reports issued; persons referred to the Department of Justice for criminal prosecution; persons referred to State and local prosecuting authorities for criminal prosecution; and indictments and criminal informations that resulted from any prior referral to prosecuting authorities.	27
Section 5(a)(12) – A description of the metrics used for developing the data for the statistical tables under the prior paragraph.	27
Section 5(a)(13) – A report on each investigation conducted by OIG where allegations of misconduct were substantiated involving a senior Government employee or senior official, including the name of the senior Government employee, if already made public by OIG, a detailed description of the facts and circumstances of the investigation, and the status and disposition of the matter.	55
Section 5(a)(14) – A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation and what, if any, consequences FHFA imposed to hold that official accountable.	55
Section 5(a)(15) – A detailed description of any attempt by FHFA to interfere with the independence of OIG, including with budget constraints designed to limit OIG's capabilities, and incidents where FHFA has resisted or objected to OIG oversight activities or restricted or significantly delayed access to information; and a summary of each report made to the FHFA head under section 6(c)(2).	56
Section 5(a)(16) – Detailed descriptions of the particular circumstances of each inspection, evaluation, and audit conducted by OIG that is closed and was not disclosed to the public; and each investigation conducted by OIG involving a senior Government employee that is closed and was not disclosed to the public.	57



Federal Housing Finance Agency
Office of Inspector General

Semiannual Report to Congress

April 1, 2026, through September 30, 2026

Federal Housing Finance Agency
Office of Inspector General
400 Seventh Street, SW
Washington, DC 20219
Main (202) 730-0880
Hotline (800) 793-7724
www.fhfaoig.gov