VII.

APPENDICES

A. Key Statistics

FDIC Actions on Financial Institutions Applications

	2021	2020	2019
Deposit Insurance	15	**18**	**15**
Approved[1]	15	18	15
Denied	0	0	0
New Branches	**493**	**430**	**548**
Approved	493	430	548
Denied	0	0	0
Mergers	**187**	**159**	**243**
Approved	187	159	243
Denied	0	0	0
Requests for Consent to Serve[2]	**47**	**79**	**87**
Approved	47	78	87
Section 19	5	11	5
Section 32	42	67	82
Denied	0	1	0
Section 19	0	0	0
Section 32	0	1	0
Notices of Change in Control	**34**	**17**	**12**
Letters of Intent Not to Disapprove	34	17	12
Disapproved	0	0	0
Brokered Deposit Waivers	**1**	**4**	**3**
Approved	1	4	3
Denied	0	0	0
Savings Association Activities[3]	**0**	**0**	**2**
Approved	0	0	2
Denied	0	0	0
State Bank Activities/Investments[4]	**25**	**31**	**20**
Approved	25	31	20
Denied	0	0	0
Conversion of Mutual Institutions	**4**	**2**	**4**
Non-Objection	4	2	4
Objection	0	0	0

[1] Includes deposit insurance applications filed on behalf of (1) newly organized institutions, (2) existing uninsured financial services companies seeking establishment as an insured institution, and (3) interim institutions established to facilitate merger or conversion transactions, and applications to facilitate the establishment of thrift holding companies.

[2] Under Section 19 of the Federal Deposit Insurance (FDI) Act, an insured institution must receive FDIC approval before employing a person convicted of dishonesty or breach of trust. Under Section 32, the FDIC must approve any change of directors or senior executive officers at a state nonmember bank that is not in compliance with capital requirements or is otherwise in troubled condition.

[3] Section 28 of the FDI Act, in general, prohibits a federally-insured state savings association from engaging in an activity not permissible for a federal savings association and requires notices or applications to be filed with the FDIC.

[4] Section 24 of the FDI Act, in general, prohibits a federally-insured state bank from engaging in an activity not permissible for a national bank and requires notices or applications to be filed with the FDIC.

Combined Risk and Consumer Enforcement Actions

	2021	2020	2019
Total Number of Actions Initiated by the FDIC	**99**	**169**	**183**
Termination of Insurance	**7**	**10**	**17**
Involuntary Termination	0	**0**	**0**
Sec. 8a For Violations, Unsafe/Unsound Practices or Conditions	0	0	0
Voluntary Termination	**7**	**10**	**17**
Sec. 8a By Order Upon Request	0	0	0
Sec. 8p No Deposits	6	8	12
Sec. 8q Deposits Assumed	1	2	5
Sec. 8b Consent and Cease-and-Desist Actions	**10**	**23**	**24**
Notices of Charges Issued	1	1	1
Orders to Pay Restitution	0	0	0
Consent and Cease and Desist Orders	8	20	18
Personal Cease and Desist Orders	1	2	5
Sec. 8e Removal/Prohibition of Director or Officer	**25**	**37**	**34**
Notices of Intention to Remove/Prohibit	4	4	1
Consent Orders	21	33	33
Sec. 8g Suspension/Removal When Charged With Crime	**0**	**0**	**0**
Civil Money Penalties Actions	**30**	**21**	**29**
Sec. 7a Call Report Penalty Orders	0	0	0
Sec. 8i Flood Act and Civil Money Penalty Orders	26	16	27
Sec. 8i Civil Money Penalty Notices of Assessment	4	5	2
Sec. 10c Orders of Investigation	**2**	**4**	**11**
Sec. 19 Waiver Orders	**24**	**74**	**64**
Approved Section 19 Waiver Orders	24	74	64
Denied Section 19 Waiver Orders	0	0	0
Sec. 32 Notices Disapproving Officer/Director's Request for Review	0	**0**	**0**
Truth-in-Lending Act Reimbursement Actions	**44**	**41**	**58**
Denials of Requests for Relief	0	0	0
Grants of Relief	0	0	0
Banks Making Reimbursement[1]	44	41	58
Suspicious Activity Reports (Open and closed institutions)[1]	**360,121**	**299,887**	**225,270**
Other Actions Not Listed[2]	**1**	**0**	**4**

[1] These actions do not constitute the initiation of a formal enforcement action and, therefore, are not included in the total number of actions initiated.

[2] The Other Actions Not Listed were, in 2021: 1 Supervisory Prompt Corrective Action Directive; in 2020: 0; in 2019: 3 Supervisory Prompt Corrective Action Directives and 1 Other Formal Action.

Estimated Insured Deposits and the Deposit Insurance Fund, December 31, 1934, through September 30, 2021[1]

Dollars in Millions (except Insurance Coverage)

		Deposits in Insured Institutions[2]				Insurance Fund as a Percentage of	
Year	Insurance Coverage[2]	Total Domestic Deposits	Est. Insured Deposits	Percentage of Domestic Deposits	Deposit Insurance Fund	Total Domestic Deposits	Est. Insured Deposits
2021	$250,000	$17,676,713	$9,577,101	54.2	$121,934.6	0.69	1.27
2020	250,000	16,339,032	9,123,046	55.8	117,896.8	0.72	1.29
2019	250,000	13,262,843	7,828,160	59.0	110,346.9	0.83	1.41
2018	250,000	12,659,406	7,525,204	59.4	102,608.9	0.81	1.36
2017	250,000	12,129,503	7,154,379	59.0	92,747.5	0.76	1.30
2016	250,000	11,693,371	6,915,663	59.1	83,161.5	0.71	1.20
2015	250,000	10,952,922	6,518,675	59.5	72,600.2	0.66	1.11
2014	250,000	10,410,687	6,195,554	59.5	62,780.2	0.60	1.01
2013	250,000	9,825,479	5,998,238	61.0	47,190.8	0.48	0.79
2012	250,000	9,474,720	7,402,053	78.1	32,957.8	0.35	0.45
2011	250,000	8,782,291	6,973,483	79.4	11,826.5	0.13	0.17
2010	250,000	7,887,858	6,301,542	79.9	(7,352.2)	(0.09)	(0.12)
2009	250,000	7,705,354	5,407,773	70.2	(20,861.8)	(0.27)	(0.39)
2008	100,000	7,505,408	4,750,783	63.3	17,276.3	0.23	0.36
2007	100,000	6,921,678	4,292,211	62.0	52,413.0	0.76	1.22
2006	100,000	6,640,097	4,153,808	62.6	50,165.3	0.76	1.21
2005	100,000	6,229,753	3,890,930	62.5	48,596.6	0.78	1.25
2004	100,000	5,724,621	3,622,059	63.3	47,506.8	0.83	1.31
2003	100,000	5,223,922	3,452,497	66.1	46,022.3	0.88	1.33
2002	100,000	4,916,078	3,383,598	68.8	43,797.0	0.89	1.29
2001	100,000	4,564,064	3,215,581	70.5	41,373.8	0.91	1.29
2000	100,000	4,211,895	3,055,108	72.5	41,733.8	0.99	1.37
1999	100,000	3,885,826	2,869,208	73.8	39,694.9	1.02	1.38
1998	100,000	3,817,150	2,850,452	74.7	39,452.1	1.03	1.38
1997	100,000	3,602,189	2,746,477	76.2	37,660.8	1.05	1.37
1996	100,000	3,454,556	2,690,439	77.9	35,742.8	1.03	1.33
1995	100,000	3,318,595	2,663,873	80.3	28,811.5	0.87	1.08
1994	100,000	3,184,410	2,588,619	81.3	23,784.5	0.75	0.92
1993	100,000	3,220,302	2,602,781	80.8	14,277.3	0.44	0.55
1992	100,000	3,275,530	2,677,709	81.7	178.4	0.01	0.01
1991	100,000	3,331,312	2,733,387	82.1	(6,934.0)	(0.21)	(0.25)
1990	100,000	3,415,464	2,784,838	81.5	4,062.7	0.12	0.15

Estimated Insured Deposits and the Deposit Insurance Fund, December 31, 1934, through September 30, 2021[1] (continued)

Dollars in Millions (except Insurance Coverage)

		Deposits in Insured Institutions[2]				Insurance Fund as a Percentage of	
Year	Insurance Coverage[2]	Total Domestic Deposits	Est. Insured Deposits	Percentage of Domestic Deposits	Deposit Insurance Fund	Total Domestic Deposits	Est. Insured Deposits
1989	100,000	3,412,503	2,755,471	80.7	13,209.5	0.39	0.48
1988	100,000	2,337,080	1,756,771	75.2	14,061.1	0.60	0.80
1987	100,000	2,198,648	1,657,291	75.4	18,301.8	0.83	1.10
1986	100,000	2,162,687	1,636,915	75.7	18,253.3	0.84	1.12
1985	100,000	1,975,030	1,510,496	76.5	17,956.9	0.91	1.19
1984	100,000	1,805,334	1,393,421	77.2	16,529.4	0.92	1.19
1983	100,000	1,690,576	1,268,332	75.0	15,429.1	0.91	1.22
1982	100,000	1,544,697	1,134,221	73.4	13,770.9	0.89	1.21
1981	100,000	1,409,322	988,898	70.2	12,246.1	0.87	1.24
1980	100,000	1,324,463	948,717	71.6	11,019.5	0.83	1.16
1979	40,000	1,226,943	808,555	65.9	9,792.7	0.80	1.21
1978	40,000	1,145,835	760,706	66.4	8,796.0	0.77	1.16
1977	40,000	1,050,435	692,533	65.9	7,992.8	0.76	1.15
1976	40,000	941,923	628,263	66.7	7,268.8	0.77	1.16
1975	40,000	875,985	569,101	65.0	6,716.0	0.77	1.18
1974	40,000	833,277	520,309	62.4	6,124.2	0.73	1.18
1973	20,000	766,509	465,600	60.7	5,615.3	0.73	1.21
1972	20,000	697,480	419,756	60.2	5,158.7	0.74	1.23
1971	20,000	610,685	374,568	61.3	4,739.9	0.78	1.27
1970	20,000	545,198	349,581	64.1	4,379.6	0.80	1.25
1969	20,000	495,858	313,085	63.1	4,051.1	0.82	1.29
1968	15,000	491,513	296,701	60.4	3,749.2	0.76	1.26
1967	15,000	448,709	261,149	58.2	3,485.5	0.78	1.33
1966	15,000	401,096	234,150	58.4	3,252.0	0.81	1.39
1965	10,000	377,400	209,690	55.6	3,036.3	0.80	1.45
1964	10,000	348,981	191,787	55.0	2,844.7	0.82	1.48
1963	10,000	313,304	177,381	56.6	2,667.9	0.85	1.50
1962	10,000	297,548	170,210	57.2	2,502.0	0.84	1.47
1961	10,000	281,304	160,309	57.0	2,353.8	0.84	1.47
1960	10,000	260,495	149,684	57.5	2,222.2	0.85	1.48
1959	10,000	247,589	142,131	57.4	2,089.8	0.84	1.47
1958	10,000	242,445	137,698	56.8	1,965.4	0.81	1.43

Estimated Insured Deposits and the Deposit Insurance Fund, December 31, 1934, through September 30, 2021[1] (continued)

Dollars in Millions (except Insurance Coverage)

		Deposits in Insured Institutions[2]				Insurance Fund as a Percentage of	
Year	Insurance Coverage[2]	Total Domestic Deposits	Est. Insured Deposits	Percentage of Domestic Deposits	Deposit Insurance Fund	Total Domestic Deposits	Est. Insured Deposits
1957	10,000	225,507	127,055	56.3	1,850.5	0.82	1.46
1956	10,000	219,393	121,008	55.2	1,742.1	0.79	1.44
1955	10,000	212,226	116,380	54.8	1,639.6	0.77	1.41
1954	10,000	203,195	110,973	54.6	1,542.7	0.76	1.39
1953	10,000	193,466	105,610	54.6	1,450.7	0.75	1.37
1952	10,000	188,142	101,841	54.1	1,363.5	0.72	1.34
1951	10,000	178,540	96,713	54.2	1,282.2	0.72	1.33
1950	10,000	167,818	91,359	54.4	1,243.9	0.74	1.36
1949	5,000	156,786	76,589	48.8	1,203.9	0.77	1.57
1948	5,000	153,454	75,320	49.1	1,065.9	0.69	1.42
1947	5,000	154,096	76,254	49.5	1,006.1	0.65	1.32
1946	5,000	148,458	73,759	49.7	1,058.5	0.71	1.44
1945	5,000	157,174	67,021	42.6	929.2	0.59	1.39
1944	5,000	134,662	56,398	41.9	804.3	0.60	1.43
1943	5,000	111,650	48,440	43.4	703.1	0.63	1.45
1942	5,000	89,869	32,837	36.5	616.9	0.69	1.88
1941	5,000	71,209	28,249	39.7	553.5	0.78	1.96
1940	5,000	65,288	26,638	40.8	496.0	0.76	1.86
1939	5,000	57,485	24,650	42.9	452.7	0.79	1.84
1938	5,000	50,791	23,121	45.5	420.5	0.83	1.82
1937	5,000	48,228	22,557	46.8	383.1	0.79	1.70
1936	5,000	50,281	22,330	44.4	343.4	0.68	1.54
1935	5,000	45,125	20,158	44.7	306.0	0.68	1.52
1934	5,000	40,060	18,075	45.1	291.7	0.73	1.61

[1] For 2021, figures are as of September 30; all other prior years are as of December 31. Prior to 1989, figures are for the Bank Insurance Fund (BIF) only and exclude insured branches of foreign banks. For 1989 to 2005, figures represent the sum of the BIF and Savings Association Insurance Fund (SAIF) amounts; for 2006 to 2021, figures are for DIF. Amounts for 1989-2021 include insured branches of foreign banks. Prior to year-end 1991, insured deposits were estimated using percentages determined from June Call and Thrift Financial Reports.

[2] The year-end 2008 coverage limit and estimated insured deposits do not reflect the temporary increase to $250,000 then in effect under the Emergency Economic Stabilization Act of 2008. The Dodd-Frank Wall Street Reform and Consumer Protection (Dodd-Frank) Act made this coverage limit permanent. The year-end 2009 coverage limit and estimated insured deposits reflect the $250,000 coverage limit. The Dodd-Frank Act also temporarily provided unlimited coverage for non-interest bearing transaction accounts for two years beginning December 31, 2010. Coverage for certain retirement accounts increased to $250,000 in 2006. Initial coverage limit was $2,500 from January 1 to June 30, 1934.

Income and Expenses, Deposit Insurance Fund, from Beginning of Operations, September 11, 1933, through December 31, 2021

Dollars in Millions

	Income					Expenses and Losses					
Year	Total	Assessment Income	Assessment Credits	Investment and Other	Effective Assessment Rate[1]	Total	Provision for Ins. Losses	Admin. and Operating Expenses[2]	Interest & Other Ins. Expenses	Funding Transfer from the FSLIC Resolution Fund	Net Income/ (Loss)
TOTAL	**$277,509.1**	**$204,998.5**	**$12,157.2**	**$84,667.8**		**$154,421.7**	**$106,142.1**	**$38,798.5**	**$9,481.2**	**$139.5**	**$123,226.9**
2021	8,153.4	7,080.2	0.0	1,073.2	0.0358%	1,705.3	(143.7)	1,842.7	6.3	0.0	6,448.1
2020	8,796.5	7,153.9	60.7	$1,703.3	0.0395%	1,691.9	(157.3)	1,846.5	2.7	0.0	7,104.6
2019	7,095.3	5,642.7	703.6	2,156.2	0.0312%	513.2	(1,285.5)	1,795.6	3.1	0.0	6,582.1
2018	11,170.8	9,526.7	0.0	1,644.1	0.0626%	1,205.2	(562.6)	1,764.7	3.1	0.0	9,965.6
2017	11,663.7	10,594.8	0.0	1,068.9	0.0716%	1,558.2	(183.1)	1,739.4	2.0	0.0	10,105.5
2016	10,674.1	9,986.6	0.0	687.5	0.0699%	150.6	(1,567.9)	1,715.0	3.5	0.0	10,523.5
2015	9,303.5	8,846.8	0.0	456.7	0.0647%	(553.2)	(2,251.3)	1,687.2	10.9	0.0	9,856.7
2014	8,965.1	8,656.1	0.0	309.0	0.0663%	(6,634.7)	(8,305.5)	1,664.3	6.5	0.0	15,599.8
2013	10,458.9	9,734.2	0.0	724.7	0.0775%	(4,045.9)	(5,659.4)	1,608.7	4.8	0.0	14,504.8
2012	18,522.3	12,397.2	0.2	6,125.3	0.1012%	(2,599.0)	(4,222.6)	1,777.5	(153.9)	0.0	21,121.3
2011	16,342.0	13,499.5	0.9	2,843.4	0.1115%	(2,915.4)	(4,413.6)	1,625.4	(127.2)	0.0	19,257.4
2010	13,379.9	13,611.2	0.8	(230.5)	0.1772%	75.0	(847.8)	1,592.6	(669.8)	0.0	13,304.9
2009	24,706.4	17,865.4	148.0	6,989.0	0.2330%	60,709.0	57,711.8	1,271.1	1,726.1	0.0	(36,002.6)
2008	7,306.3	4,410.4	1,445.9	4,341.8	0.0418%	44,339.5	41,838.8	1,033.5	1,467.2	0.0	(37,033.2)
2007	3,196.2	3,730.9	3,088.0	2,553.3	0.0093%	1,090.9	95.0	992.6	3.3	0.0	2,105.3
2006	2,643.5	31.9	0.0	2,611.6	0.0005%	904.3	(52.1)	950.6	5.8	0.0	1,739.2
2005	2,420.5	60.9	0.0	2,359.6	0.0010%	809.3	(160.2)	965.7	3.8	0.0	1,611.2
2004	2,240.3	104.2	0.0	2,136.1	0.0019%	607.6	(353.4)	941.3	19.7	0.0	1,632.7
2003	2,173.6	94.8	0.0	2,078.8	0.0019%	(67.7)	(1,010.5)	935.5	7.3	0.0	2,241.3
2002	2,384.7	107.8	0.0	2,276.9	0.0023%	719.6	(243.0)	945.1	17.5	0.0	1,665.1
2001	2,730.1	83.2	0.0	2,646.9	0.0019%	3,123.4	2,199.3	887.9	36.2	0.0	(393.3)
2000	2,570.1	64.3	0.0	2,505.8	0.0016%	945.2	28.0	883.9	33.3	0.0	1,624.9
1999	2,416.7	48.4	0.0	2,368.3	0.0013%	2,047.0	1,199.7	823.4	23.9	0.0	369.7
1998	2,584.6	37.0	0.0	2,547.6	0.0010%	817.5	(5.7)	782.6	40.6	0.0	1,767.1
1997	2,165.5	38.6	0.0	2,126.9	0.0011%	247.3	(505.7)	677.2	75.8	0.0	1,918.2
1996	7,156.8	5,294.2	0.0	1,862.6	0.1622%	353.6	(417.2)	568.3	202.5	0.0	6,803.2
1995	5,229.2	3,877.0	0.0	1,352.2	0.1238%	202.2	(354.2)	510.6	45.8	0.0	5,027.0
1994	7,682.1	6,722.7	0.0	959.4	0.2192%	(1,825.1)	(2,459.4)	443.2	191.1	0.0	9,507.2
1993	7,354.5	6,682.0	0.0	672.5	0.2157%	(6,744.4)	(7,660.4)	418.5	497.5	0.0	14,098.9
1992	6,479.3	5,758.6	0.0	720.7	0.1815%	(596.8)	(2,274.7)	614.8[3]	1,063.1	35.4	7,111.5
1991	5,886.5	5,254.0	0.0	632.5	0.1613%	16,925.3	15,496.2	326.1	1,103.0	42.4	(10,996.4)
1990	3,855.3	2,872.3	0.0	983.0	0.0868%	13,059.3	12,133.1	275.6	650.6	56.1	(9,147.9)
1989	3,494.8	1,885.0	0.0	1,609.8	0.0816%	4,352.2	3,811.3	219.9	321.0	5.6	(851.8)

Income and Expenses, Deposit Insurance Fund, from Beginning of Operations, September 11, 1933, through December 31, 2021 (continued)

Dollars in Millions

	Income					Expenses and Losses					
Year	Total	Assessment Income	Assessment Credits	Investment and Other	Effective Assessment Rate[1]	Total	Provision for Ins. Losses	Admin. and Operating Expenses[2]	Interest & Other Ins. Expenses	Funding Transfer from the FSLIC Resolution Fund	Net Income/(Loss)
1988	3,347.7	1,773.0	0.0	1,574.7	0.0825%	7,588.4	6,298.3	223.9	1,066.2	0.0	(4,240.7)
1987	3,319.4	1,696.0	0.0	1,623.4	0.0833%	3,270.9	2,996.9	204.9	69.1	0.0	48.5
1986	3,260.1	1,516.9	0.0	1,743.2	0.0787%	2,963.7	2,827.7	180.3	(44.3)	0.0	296.4
1985	3,385.5	1,433.5	0.0	1,952.0	0.0815%	1,957.9	1,569.0	179.2	209.7	0.0	1,427.6
1984	3,099.5	1,321.5	0.0	1,778.0	0.0800%	1,999.2	1,633.4	151.2	214.6	0.0	1,100.3
1983	2,628.1	1,214.9	164.0	1,577.2	0.0714%	969.9	675.1	135.7	159.1	0.0	1,658.2
1982	2,524.6	1,108.9	96.2	1,511.9	0.0769%	999.8	126.4	129.9	743.5	0.0	1,524.8
1981	2,074.7	1,039.0	117.1	1,152.8	0.0714%	848.1	320.4	127.2	400.5	0.0	1,226.6
1980	1,310.4	951.9	521.1	879.6	0.0370%	83.6	(38.1)	118.2	3.5	0.0	1,226.8
1979	1,090.4	881.0	524.6	734.0	0.0333%	93.7	(17.2)	106.8	4.1	0.0	996.7
1978	952.1	810.1	443.1	585.1	0.0385%	148.9	36.5	103.3	9.1	0.0	803.2
1977	837.8	731.3	411.9	518.4	0.0370%	113.6	20.8	89.3	3.5	0.0	724.2
1976	764.9	676.1	379.6	468.4	0.0370%	212.3	28.0	180.4[4]	3.9	0.0	552.6
1975	689.3	641.3	362.4	410.4	0.0357%	97.5	27.6	67.7	2.2	0.0	591.8
1974	668.1	587.4	285.4	366.1	0.0435%	159.2	97.9	59.2	2.1	0.0	508.9
1973	561.0	529.4	283.4	315.0	0.0385%	108.2	52.5	54.4	1.3	0.0	452.8
1972	467.0	468.8	280.3	278.5	0.0333%	65.7	10.1	49.6	6.0[5]	0.0	401.3
1971	415.3	417.2	241.4	239.5	0.0345%	60.3	13.4	46.9	0.0	0.0	355.0
1970	382.7	369.3	210.0	223.4	0.0357%	46.0	3.8	42.2	0.0	0.0	336.7
1969	335.8	364.2	220.2	191.8	0.0333%	34.5	1.0	33.5	0.0	0.0	301.3
1968	295.0	334.5	202.1	162.6	0.0333%	29.1	0.1	29.0	0.0	0.0	265.9
1967	263.0	303.1	182.4	142.3	0.0333%	27.3	2.9	24.4	0.0	0.0	235.7
1966	241.0	284.3	172.6	129.3	0.0323%	19.9	0.1	19.8	0.0	0.0	221.1
1965	214.6	260.5	158.3	112.4	0.0323%	22.9	5.2	17.7	0.0	0.0	191.7
1964	197.1	238.2	145.2	104.1	0.0323%	18.4	2.9	15.5	0.0	0.0	178.7
1963	181.9	220.6	136.4	97.7	0.0313%	15.1	0.7	14.4	0.0	0.0	166.8
1962	161.1	203.4	126.9	84.6	0.0313%	13.8	0.1	13.7	0.0	0.0	147.3
1961	147.3	188.9	115.5	73.9	0.0323%	14.8	1.6	13.2	0.0	0.0	132.5
1960	144.6	180.4	100.8	65.0	0.0370%	12.5	0.1	12.4	0.0	0.0	132.1
1959	136.5	178.2	99.6	57.9	0.0370%	12.1	0.2	11.9	0.0	0.0	124.4
1958	126.8	166.8	93.0	53.0	0.0370%	11.6	0.0	11.6	0.0	0.0	115.2
1957	117.3	159.3	90.2	48.2	0.0357%	9.7	0.1	9.6	0.0	0.0	107.6
1956	111.9	155.5	87.3	43.7	0.0370%	9.4	0.3	9.1	0.0	0.0	102.5
1955	105.8	151.5	85.4	39.7	0.0370%	9.0	0.3	8.7	0.0	0.0	96.8
1954	99.7	144.2	81.8	37.3	0.0357%	7.8	0.1	7.7	0.0	0.0	91.9
1953	94.2	138.7	78.5	34.0	0.0357%	7.3	0.1	7.2	0.0	0.0	86.9

Income and Expenses, Deposit Insurance Fund, from Beginning of Operations, September 11, 1933, through December 31, 2021 (continued)

Dollars in Millions

	Income					Expenses and Losses					
Year	Total	Assessment Income	Assessment Credits	Investment and Other	Effective Assessment Rate[1]	Total	Provision for Ins. Losses	Admin. and Operating Expenses[2]	Interest & Other Ins. Expenses	Funding Transfer from the FSLIC Resolution Fund	Net Income/ (Loss)
1952	88.6	131.0	73.7	31.3	0.0370%	7.8	0.8	7.0	0.0	0.0	80.8
1951	83.5	124.3	70.0	29.2	0.0370%	6.6	0.0	6.6	0.0	0.0	76.9
1950	84.8	122.9	68.7	30.6	0.0370%	7.8	1.4	6.4	0.0	0.0	77.0
1949	151.1	122.7	0.0	28.4	0.0833%	6.4	0.3	6.1	0.0	0.0	144.7
1948	145.6	119.3	0.0	26.3	0.0833%	7.0	0.7	6.3[6]	0.0	0.0	138.6
1947	157.5	114.4	0.0	43.1	0.0833%	9.9	0.1	9.8	0.0	0.0	147.6
1946	130.7	107.0	0.0	23.7	0.0833%	10.0	0.1	9.9	0.0	0.0	120.7
1945	121.0	93.7	0.0	27.3	0.0833%	9.4	0.1	9.3	0.0	0.0	111.6
1944	99.3	80.9	0.0	18.4	0.0833%	9.3	0.1	9.2	0.0	0.0	90.0
1943	86.6	70.0	0.0	16.6	0.0833%	9.8	0.2	9.6	0.0	0.0	76.8
1942	69.1	56.5	0.0	12.6	0.0833%	10.1	0.5	9.6	0.0	0.0	59.0
1941	62.0	51.4	0.0	10.6	0.0833%	10.1	0.6	9.5	0.0	0.0	51.9
1940	55.9	46.2	0.0	9.7	0.0833%	12.9	3.5	9.4	0.0	0.0	43.0
1939	51.2	40.7	0.0	10.5	0.0833%	16.4	7.2	9.2	0.0	0.0	34.8
1938	47.7	38.3	0.0	9.4	0.0833%	11.3	2.5	8.8	0.0	0.0	36.4
1937	48.2	38.8	0.0	9.4	0.0833%	12.2	3.7	8.5	0.0	0.0	36.0
1936	43.8	35.6	0.0	8.2	0.0833%	10.9	2.6	8.3	0.0	0.0	32.9
1935	20.8	11.5	0.0	9.3	0.0833%	11.3	2.8	8.5	0.0	0.0	9.5
1933-34	7.0	0.0	0.0	7.0	N/A	10.0	0.2	9.8	0.0	0.0	(3.0)

[1] The effective assessment rate is calculated from annual assessment income (net of assessment credits), excluding transfers to the Financing Corporation (FICO), Resolution Funding Corporation (REFCORP) and FSLIC Resolution Fund, divided by the average assessment base. Figures represent only BIF-insured institutions prior to 1990, and BIF- and SAIF-insured institutions from 1990 through 2005. After 1995, all thrift closings became the responsibility of the FDIC and amounts are reflected in the SAIF. Beginning in 2006, figures are for the DIF.

The annualized assessment rate for 2021 is based on full year assessment income divided by a four quarter average of 2021 quarterly assessment base amounts. The assessment base for fourth quarter 2021 was estimated using the third quarter 2021 assessment base and an assumed quarterly growth rate of one percent.

Historical Assessment Rates:

1934 – 1949 The statutory assessment rate was 0.0833 percent.

1950 – 1984 The effective assessment rates varied from the statutory rate of 0.0833 percent due to assessment credits provided in those years.

1985 – 1989 The statutory assessment rate was 0.0833 percent (no credits were given).

1990 The statutory rate increased to 0.12 percent.

1991 – 1992 The statutory rate increased to a minimum of 0.15 percent. The effective rates in 1991 and 1992 varied because the FDIC exercised new authority to increase assessments above the statutory minimum rate when needed.

1993 – 2006 Beginning in 1993, the effective rate was based on a risk-related premium system under which institutions paid assessments in the range of 0.23 percent to 0.31 percent. In May 1995, the BIF reached the mandatory recapitalization level of 1.25 percent. As a result, BIF assessment rates were reduced to a range of 0.04 percent to 0.31 percent of assessable deposits, effective June 1995, and assessments totaling $1.5 billion were refunded in September 1995. Assessment rates for the BIF were lowered again to a range of 0 to 0.27 percent of assessable deposits, effective the start of 1996. In 1996, the SAIF collected a one-time special assessment of $4.5 billion. Subsequently, assessment rates for the SAIF were lowered to the same range as the BIF, effective October 1996. This range of rates remained unchanged for both funds through 2006.

2007 – 2008 As part of the implementation of the Federal Deposit Insurance Reform Act of 2005, assessment rates were increased to a range of 0.05 percent to 0.43 percent of assessable deposits effective at the start of 2007, but many institutions received a one-time assessment credit ($4.7 billion in total) to offset the new assessments.

2009 – 2011 For the first quarter of 2009, assessment rates were increased to a range of 0.12 percent to 0.50 percent of assessable deposits. On June 30, 2009, a special assessment was imposed on all insured banks and thrifts, which amounted in aggregate to approximately $5.4 billion. For 8,106 institutions, with $9.3 trillion in assets, the special assessment was 5 basis points of each insured institution's assets minus tier one capital; 89 other institutions, with assets of $4.0 trillion, had their special assessment capped at 10 basis points of their second quarter assessment base. From the second quarter of 2009 through the first quarter of 2011, initial assessment rates ranged between 0.12 percent and 0.45 percent of assessable deposits. Initial rates were subject to further adjustments.

2011 – 2016 Beginning in the second quarter of 2011, the assessment base changed to average total consolidated assets less average tangible equity (with certain adjustments for banker's banks and custodial banks), as required by the Dodd-Frank Act. The FDIC implemented a new assessment rate schedule at the same time to conform to the larger assessment base. Initial assessment rates were lowered to a range of 0.05 percent to 0.35 percent of the new base. The annualized assessment rates averaged approximately 17.6 cents per $100 of assessable deposits for the first quarter of 2011 and 11.1 cents per $100 of the new base for the last three quarters of 2011 (which is shown in the table).

2016 Beginning July 1, 2016, initial assessment rates were lowered from a range of 5 basis points to 35 basis points to a range of 3 basis points to 30 basis points, and an additional surcharge was imposed on large banks (generally institutions with $10 billion or more in assets) of 4.5 basis points of their assessment base (after making adjustments).

2018 The 4.5 basis point surcharge imposed on large banks ended effective October 1, 2018. The annualized assessment rates averaged approximately 7.2 cents per $100 of the assessable base for the first three quarters of 2018 and 3.5 cents per $100 of the assessment base for the last quarter of 2018. The full year annualized assessment rate averaged 6.3 cents per $100 (which is shown in the table).

2019 Assessment income for 2019 included small bank credits of $703.6 million.

2020 Assessment income for 2020 included small bank credits of $60.7 million.

[2] These expenses, which are presented as operating expenses in the Statement of Income and Fund Balance, pertain to the FDIC in its corporate capacity only and do not include costs that are charged to the failed bank receiverships that are managed by the FDIC. The receivership expenses are presented as part of the "Receivables from Resolutions, net" line on the Balance Sheet. The narrative and graph presented on page 123 of this report shows the aggregate (corporate and receivership) expenditures of the FDIC.

[3] Includes $210 million for the cumulative effect of an accounting change for certain postretirement benefits (1992).

[4] Includes a $106 million net loss on government securities (1976).

[5] This amount represents interest and other insurance expenses from 1933 to 1972.

[6] Includes the aggregate amount of $81 million of interest paid on capital stock between 1933 and 1948.

Assets and Deposits of Failed or Assisted Insured Institutions and Losses to the Deposit Insurance Fund, 1934 - 2021
Dollars in Thousands

	Bank and Thrift Failures[1]			
Year[2]	Number of Banks/ Thrifts	Total Assets[3]	Total Deposits[3]	Losses to the Fund[4]
Total	**2,631**	**$947,307,165**	**$713,862,572**	**$105,132,739**
2021	0	0	0	0
2020	4	454,986	437,138	95,259
2019	4	208,767	$190,547	27,197
2018	0	0	0	0
2017	8	5,081,737	4,683,360	1,083,350
2016	5	277,182	268,516	42,474
2015	8	6,706,038	4,870,464	859,244
2014	18	2,913,503	2,691,485	378,362
2013	24	6,044,051	5,132,246	1,204,884
2012	51	11,617,348	11,009,630	2,385,085
2011	92	34,922,997	31,071,862	6,392,952
2010[5]	157	92,084,988	78,290,185	15,810,119
2009[5]	140	169,709,160	137,835,208	25,963,909
2008[5]	25	371,945,480	234,321,715	17,805,073
2007	3	2,614,928	2,424,187	157,440
2006	0	0	0	0
2005	0	0	0	0
2004	4	170,099	156,733	3,917
2003	3	947,317	901,978	62,647
2002	11	2,872,720	2,512,834	413,989
2001	4	1,821,760	1,661,214	292,465
2000	7	410,160	342,584	32,138
1999	8	1,592,189	1,320,573	586,027
1998	3	290,238	260,675	221,606
1997	1	27,923	27,511	5,026
1996	6	232,634	230,390	60,615
1995	6	802,124	776,387	84,472
1994	13	1,463,874	1,397,018	179,051
1993	41	3,828,939	3,509,341	632,646
1992	120	45,357,237	39,921,310	3,674,149
1991	124	64,556,512	52,972,034	6,001,595
1990	168	16,923,462	15,124,454	2,771,489
1989	206	28,930,572	24,152,468	6,195,286
1988	200	38,402,475	26,524,014	5,377,497
1987	184	6,928,889	6,599,180	1,862,492
1986	138	7,356,544	6,638,903	1,682,538
1985	116	3,090,897	2,889,801	648,179
1934 - 1984	729	16,719,435	12,716,627	2,139,567

Assets and Deposits of Failed or Assisted Insured Institutions and Losses to the Deposit Insurance Fund, 1934 - 2021 (continued)
Dollars in Thousands

Assistance Transactions				
Year[2]	Number of Banks/ Thrifts	Total Assets[3]	Total Deposits[3]	Losses to the Fund[4]
	154	**$3,317,099,253**	**$1,442,173,417**	**$5,430,481**
2010 - 2021	0	0	0	0
2009[6]	8	1,917,482,183	1,090,318,282	0
2008[6]	5	1,306,041,994	280,806,966	0
1993 - 2007	0	0	0	0
1992	2	33,831	33,117	250
1991	3	78,524	75,720	3,024
1990	1	14,206	14,628	2,338
1989	1	4,438	6,396	2,296
1988	80	15,493,939	11,793,702	1,540,642
1987	19	2,478,124	2,275,642	160,164
1986	7	712,558	585,248	93,179
1985	4	5,886,381	5,580,359	359,056
1984	2	40,470,332	29,088,247	1,116,275
1983	4	3,611,549	3,011,406	337,683
1982	10	10,509,286	9,118,382	1,042,784
1981	3	4,838,612	3,914,268	772,790
1980	1	7,953,042	5,001,755	0
1934 - 1979	4	1,490,254	549,299	0

[1] Institutions for which the FDIC is appointed receiver, including deposit payoff, insured deposit transfer, and deposit assumption cases.

[2] For 1990 through 2005, amounts represent the sum of BIF and SAIF failures (excluding those handled by the RTC); prior to 1990, figures are only for the BIF. After 1995, all thrift closings became the responsibility of the FDIC and amounts are reflected in the SAIF. For 2006 to 2021, figures are for the DIF.

[3] Assets and deposit data are based on the last Call Report or TFR filed before failure.

[4] Losses to the fund include final and estimated losses. Final losses represent actual losses for unreimbursed subrogated claims of inactivated receiverships. Estimated losses generally represent the difference between the amount paid by the DIF to cover obligations to insured depositors and the estimated recoveries from the liquidation of receivership assets.

[5] Includes amounts related to transaction account coverage under the Transaction Account Guarantee Program (TAG). The estimated losses as of December 31, 2021, for TAG accounts in 2010, 2009, and 2008 are $362 million, $1.1 billion, and $12 million, respectively.

[6] Includes institutions where assistance was provided under a systemic risk determination.

B. More About the FDIC

FDIC BOARD OF DIRECTORS

Jelena McWilliams

Jelena McWilliams was sworn in as the 21st Chairman of the FDIC on June 5, 2018. She serves a six-year term on the FDIC Board of Directors, and is designated as Chairman for a term of five years.

Ms. McWilliams was Executive Vice President, Chief Legal Officer, and Corporate Secretary for Fifth Third Bank in Cincinnati, Ohio. At Fifth Third Bank she served as a member of the executive management team and numerous bank committees including: Management Compliance, Enterprise Risk, Risk and Compliance, Operational Risk, Enterprise Marketing, and Regulatory Change.

Prior to joining Fifth Third Bank, Ms. McWilliams worked in the U.S. Senate for six years, most recently as Chief Counsel and Deputy Staff Director with the Senate Committee on Banking, Housing and Urban Affairs, and previously as Assistant Chief Counsel with the Senate Small Business and Entrepreneurship Committee.

From 2007 to 2010, Ms. McWilliams served as an attorney at the Federal Reserve Board of Governors, where she drafted consumer protection regulations, reviewed and analyzed comment letters on regulatory proposals, and responded to consumer complaints.

Before entering public service, she practiced corporate and securities law at Morrison & Foerster LLP in Palo Alto, California, and Hogan & Hartson LLP (now Hogan Lovells LLP) in Washington, D.C. In legal practice, Ms. McWilliams advised management and boards of directors on corporate governance, compliance, and reporting requirements under the Securities Act of 1933 and the Securities Exchange Act of 1934. She also represented publicly- and privately-held companies in mergers and acquisitions, securities offerings, strategic business ventures, venture capital investments, and general corporate matters.

Ms. McWilliams graduated with highest honors from the University of California at Berkeley with a B.S. in political science, and earned her law degree from U.C. Berkeley School of Law.

Martin J. Gruenberg

Martin J. Gruenberg has been the Acting Chairman of the FDIC Board of Directors since February 5, 2022. Since mid-2018, he has served as a member of the FDIC Board. Prior to that time, Mr. Gruenberg also served as Chairman of the FDIC, receiving Senate confirmation on November 15, 2012, for a five-year term. Mr. Gruenberg served as Vice Chairman and Member of the FDIC Board of Directors from August 2005, until his confirmation as Chairman. He served as Acting Chairman from July 2011 to November 2012, and also from November 2005 to June 2006.

Mr. Gruenberg joined the FDIC Board after broad congressional experience in the financial services and regulatory areas. He served as Senior Counsel to Senator Paul S. Sarbanes (D-MD) on the staff of the Senate Committee on Banking, Housing, and Urban Affairs from 1993 to 2005. He also served as Staff Director of the Banking Committee's Subcommittee on International Finance and Monetary Policy from 1987 to 1992.

Mr. Gruenberg served as Chairman of the Executive Council and President of the International Association of Deposit Insurers (IADI) from November 2007 to November 2012.

In addition, Mr. Gruenberg served as Chairman of the Federal Financial Institutions Examination Council from April 2017 to June 2018.

Since June 2019, Mr. Gruenberg has served as Chairman of the Board of Directors of the Neighborhood Reinvestment Corporation (NeighborWorks America), and he has been a member of the Board since April 2018.

Mr. Gruenberg holds a J.D. from Case Western Reserve Law School and an A.B. from Princeton University, Woodrow Wilson School of Public and International Affairs.

Michael J. Hsu

Michael J. Hsu became Acting Comptroller of the Currency on May 10, 2021, upon his designation as First Deputy Comptroller by Secretary of the Treasury Janet Yellen pursuant to her authority under 12 U.S.C. 4.

As Acting Comptroller of the Currency, Mr. Hsu is the administrator of the federal banking system and chief executive officer of the Office of the Comptroller of the Currency (OCC). The OCC ensures that the federal banking system operates in a safe and sound manner, provides fair access to financial services, treats customers fairly, and complies with applicable laws and regulations. It supervises nearly 1,200 national banks, federal savings associations, and federal branches and agencies of foreign banks that serve consumers, businesses, and communities across the United States and conducts approximately 70 percent of banking activity in the country. These banks range from community banks serving local neighborhood needs to the nation's largest most internationally active banks.

The Comptroller also serves as a Director of the Federal Deposit Insurance Corporation and a member of the Financial Stability Oversight Council and the Federal Financial Institutions Examination Council.

Prior to joining the OCC, Mr. Hsu served as an Associate Director in the Division of Supervision and Regulation at the Federal Reserve Board of Governors. In that role, he chaired the Large Institution Supervision Coordinating Committee Operating Committee, which has responsibility for supervising the global systemically important banking companies operating in the United States. He co-chaired the Federal Reserve's Systemic Risk Integration Forum, served as a member of the Basel Committee Risk and Vulnerabilities Group, and co-sponsored forums promoting interagency coordination with foreign and domestic financial regulatory agencies.

His career has included serving as a Financial Sector Expert at the International Monetary Fund, Financial Economist at the U.S. Department of the Treasury helping to establish the Troubled Asset Relief Program, and Financial Economist at the Securities and Exchange Commission overseeing the largest securities firms.

Mr. Hsu began his career in 2002 as a staff attorney in the Federal Reserve Board's Legal Division. He holds of a bachelor of arts from Brown University, a master of science in finance from George Washington University, and juris doctor degree from New York University School of Law.

Rohit Chopra

Rohit Chopra was confirmed as Director of the Consumer Financial Protection Bureau on October 12, 2021. The CFPB is a unit of the Federal Reserve System charged with protecting families and honest businesses from illegal practices by financial institutions, and ensuring that markets for consumer financial products and services are fair, transparent, and competitive.

In 2018, Mr. Chopra was unanimously confirmed by the U.S. Senate as a Commissioner on the Federal Trade Commission, where he served until assuming office as CFPB Director. During his tenure at the FTC, he successfully worked to strengthen sanctions against repeat offenders, to reverse the agency's reliance on no-money, no-fault settlements in fraud cases, and to halt abuses of small businesses. He also led efforts to revitalize dormant authorities, such as those to protect the Made in USA label and to promote competition.

Mr. Chopra previously served at the CFPB from 2010 to 2015. In 2011, the Secretary of the Treasury designated him as the agency's student loan ombudsman, where he led the Bureau's efforts on student lending issues. Prior to his government service, Mr. Chopra worked at McKinsey & Company, the global management consultancy, where he consulted in the financial services, health care, and consumer technology sectors.

Mr. Chopra holds a BA from Harvard University and an MBA from the Wharton School at the University of Pennsylvania.

Blake Paulson

Blake Paulson resigned from the FDIC Board of Directors as of May 10, 2021. Mr. Paulson had been an Acting FDIC Board member since January 14, 2021.

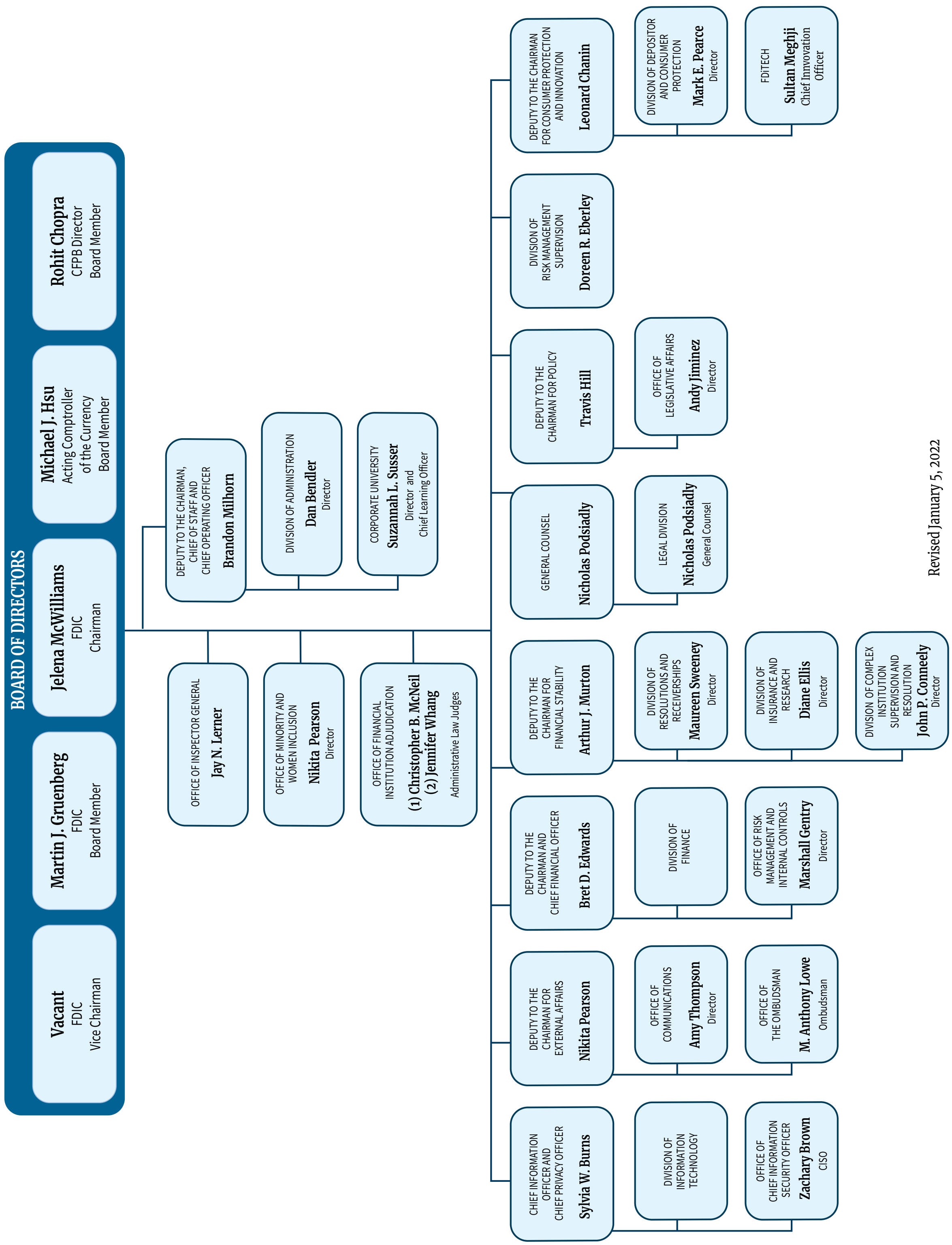
Dave Uejio

Dave Uejio resigned from the FDIC Board of Directors as of October 12, 2021. Mr. Uejio had been an Acting FDIC Board member since January 20, 2021.

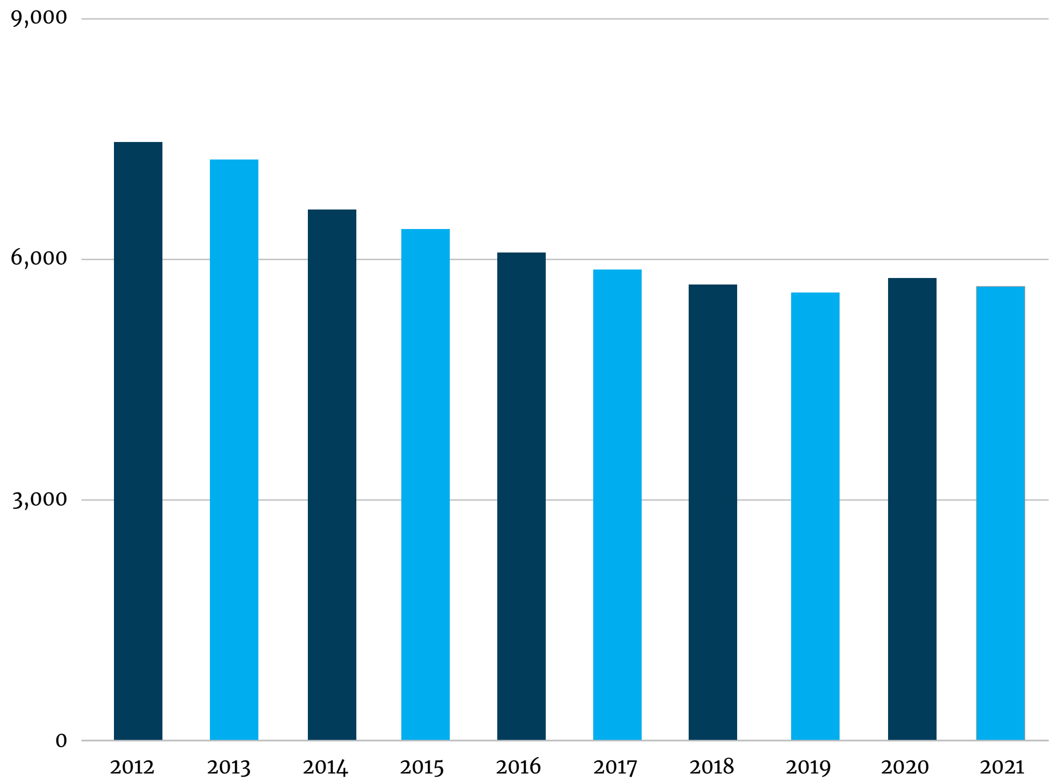
Subsequent Event:

Jelena McWilliams resigned from the FDIC Board of Directors effective February 4, 2022. Director Martin Gruenberg was named Acting FDIC Chairman effective February 5, 2022.

FDIC Organizational Chart



CORPORATE STAFFING TRENDS



7,476	7,254	6,631	6,385	6,096	5,880	5,693	5,593	5,776	5,670

FDIC Year–End Staffing

Note: 2012-2021 staffing totals reflect year-end full time equivalent staff.

Number of Employees by Division/Office (Year-End)[1]

	Total		Washington		Regional/Field	
Division or Office:	**2021**	**2020**	**2021**	**2020**	**2021**	**2020**
Division of Risk Management Supervision	2,484	2,559	159	152	2,325	2,407
Division of Depositor and Consumer Protection	787	818	115	116	672	702
Legal Division	440	438	295	293	145	145
Division of Administration	375	370	269	264	106	106
Division of Resolutions and Receiverships	317	343	90	96	228	248
Division of Information Technology	284	299	225	234	59	65
Division of Complex Institution Supervision and Resolution	280	258	130	125	150	133
Division of Insurance and Research	199	205	163	166	36	39
Division of Finance	134	154	131	150	3	4
Executive Support Offices[2]	103	67	92	58	11	9
Corporate University	65	63	57	56	8	7
Office of the Chief Information Security Officer	49	48	49	48	0	0
Executive Offices[3]	21	25	21	25	0	0
Office of Inspector General	132	130	84	79	48	51
TOTAL	**5,670**	**5,776**	**1,879**	**1,860**	**3,792**	**3,916**

[1] The FDIC reports staffing totals using a full-time equivalent methodology, which is based on an employee's scheduled work hours. Division/Office staffing has been rounded to the nearest whole FTE. Totals may not foot due to rounding.

[2] Includes the Offices of the Legislative Affairs, Communications, Ombudsman, FDITECH, Financial Adjudication, Minority and Women Inclusion, and Risk Management and Internal Controls.

[3] Includes the Offices of the Chairman, Vice Chairman, Director (Appointive), Chief Operating Officer, Chief Financial Officer, Chief Information Officer, Consumer Protection and Innovation, External Affairs, Policy, and Financial Stability.

Sources of Information

FDIC WEBSITE

www.fdic.gov

A wide range of banking, consumer, and financial information is available on the FDIC's website. This includes the FDIC's Electronic Deposit Insurance Estimator (EDIE), which estimates an individual's deposit insurance coverage; the Institution Directory, which contains financial profiles of FDIC-insured institutions; Community Reinvestment Act evaluations and ratings for institutions supervised by the FDIC; Call Reports, which are bank reports of condition and income; and *Money Smart*, a training program to help individuals outside the financial mainstream enhance their money management skills and create positive banking relationships. Readers also can access a variety of consumer pamphlets, FDIC press releases, speeches, and other updates on the agency's activities, as well as corporate databases and customized reports of FDIC and banking industry information.

FDIC CALL CENTER

Phone: 877-275-3342 (877-ASK-FDIC)
703-562-2222

Hearing Impaired: 800-925-4618
703-562-2289

The FDIC Call Center in Washington, DC, is the primary telephone point of contact for general questions from the banking community, the public, and FDIC employees. The Call Center directly, or with other FDIC subject-matter experts, responds to questions about deposit insurance and other consumer issues and concerns, as well as questions about FDIC programs and activities. The Call Center also refers callers to other federal and state agencies as needed. Hours of operation are 8:00 a.m. to 8:00 p.m., Eastern Time, Monday – Friday, and 9:00 a.m. to 5:00 p.m., Saturday – Sunday. Recorded information about deposit insurance and other topics is available 24 hours a day at the same telephone number.

As a customer service, the FDIC Call Center has many bilingual Spanish agents on staff and has access to a translation service, which is able to assist with over 40 different languages.

PUBLIC INFORMATION CENTER

3501 Fairfax Drive
Room E-1021
Arlington, VA 22226

Phone: 877-275-3342 (877-ASK-FDIC),
703-562-2200

Fax: 703-562-2296

FDIC Online Catalog: https://catalog.fdic.gov

E-mail: publicinfo@fdic.gov

Publications such as *FDIC Quarterly* and *Consumer News* and a variety of deposit insurance and consumer pamphlets are available at www.fdic.gov or may be ordered in hard copy through the FDIC online catalog. Other information, press releases, speeches and congressional testimony, directives to financial institutions, policy manuals, and FDIC documents are available on request through the Public Information Center. Hours of operation are 9:00 a.m. to 4:00 p.m., Eastern Time, Monday – Friday.

OFFICE OF THE OMBUDSMAN

3501 Fairfax Drive
Room E-2022
Arlington, VA 22226

Phone: 877-275-3342 (877-ASK-FDIC)

Fax: 703-562-6057

E-mail: ombudsman@fdic.gov

The Office of the Ombudsman (OO) is an independent, neutral, and confidential resource and liaison for the banking industry and the general public. The OO responds to inquiries about the FDIC in a fair, impartial, and timely manner. It researches questions and fields complaints from bankers and bank customers. OO representatives are present at all bank closings to provide accurate information to bank customers, the media, bank employees, and the general public. The OO also recommends ways to improve FDIC operations, regulations, and customer service.

Regional and Area Offices

ATLANTA REGIONAL OFFICE

Frank Hughes, Acting Regional Director
10 Tenth Street, NE
Suite 800
Atlanta, Georgia 30309
(678) 916-2200

States represented:

Alabama
Florida
Georgia
North Carolina
South Carolina
Virginia
West Virginia

CHICAGO REGIONAL OFFICE

Gregory Bottone, Regional Director
300 South Riverside Plaza
Suite 1700
Chicago, Illinois 60606
(312) 382-6000

States represented:

Illinois
Indiana
Kentucky
Michigan
Ohio
Wisconsin

DALLAS REGIONAL OFFICE

Kristie K. Elmquist, Regional Director
1601 Bryan Street
Dallas, Texas 75201
(214) 754-0098

States represented:

Arkansas
Colorado
Louisiana
Mississippi
New Mexico
Oklahoma
Tennessee
Texas

KANSAS CITY REGIONAL OFFICE

James D. LaPierre, Regional Director
1100 Walnut Street
Suite 2100
Kansas City, Missouri 64106
(816) 234-8000

States represented:

Iowa
Kansas
Minnesota
Missouri
Nebraska
North Dakota
South Dakota

NEW YORK REGIONAL OFFICE

Jessica Kaemingk, Acting Regional Director
350 Fifth Avenue
Suite 1200
New York, New York 10118
(917) 320-2500

States represented:

Delaware
District of Columbia
Maryland
New Jersey
New York
Pennsylvania

BOSTON AREA OFFICE

Jessica Kaemingk, Acting Regional Director
15 Braintree Hill Office Park
Suite 200
Braintree, Massachusetts 02184
(781) 794-5500

States and territories represented:

Connecticut
Maine
Massachsetts
New Hampshire
Puerto Rico
Rhode Island
Vermont
Virgin Islands

SAN FRANCISCO REGIONAL OFFICE

Kathy L. Moe, Regional Director
25 Jessie Street at Ecker Square
Suite 2300
San Francisco, California 94105
(415) 546-0160

States and territories represented:

Alaska
American Samoa
Arizona
California
Federated States of Micronesia
Guam
Hawaii
Idaho
Montana
Nevada
Oregon
Utah
Washington
Wyoming

Office of Inspector General

Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

February 2022

☆☆☆☆☆☆☆☆

Federal Deposit Insurance Corporation
Office of Inspector General

Office of Inspector General

Federal Deposit Insurance Corporation
Office of Inspector General

Date: February 17, 2022

Memorandum To: Board of Directors

From: Jay N. Lerner
Inspector General

Subject Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

The Office of Inspector General (OIG) presents its annual assessment of the Top Management and Performance Challenges facing the Federal Deposit Insurance Corporation (FDIC). This document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them.

This Challenges document is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. In several instances, we discuss topic areas where the OIG had previously conducted work to evaluate, audit, and review the FDIC's progress in these Challenge areas.

We identified nine Top Challenges facing the FDIC. This document incorporates and consolidates discussions of the risks identified in prior years and updates our assessments with respect to current conditions and circumstances. This year, we added a new Challenge regarding the FDIC's collection, analysis, and use of data, and we highlighted the importance of governance to ensure the effective execution of the FDIC's mission.

The Top Challenges facing the FDIC include:

1. The FDIC's Readiness for Crises;
2. Cybersecurity for Banks and Third-Party Service Providers;
3. Supporting Underserved Communities in Banking;
4. Organizational Governance at the FDIC;
5. Information Technology Security at the FDIC;
6. Security and Privacy at the FDIC;
7. The FDIC's Collection, Analysis, and Use of Data;
8. Contracting and Supply Chain Management at the FDIC; and
9. Human Resources at the FDIC.

We believe that this researched and deliberative analysis is beneficial and constructive for policy makers, including the FDIC Board and officials, as well as Congressional oversight bodies. We further hope that it is informative for the American people regarding the programs and operations at the FDIC and the Challenges it faces.

Executive Summary

The FDIC plays a unique and vital role in support of the U.S. financial system. The FDIC insures approximately $9.5 trillion in bank deposits at over 4,900 banks, supervises and examines more than 3,200 banks, oversees over $123 billion in the Deposit Insurance Fund (DIF) that protects bank depositor accounts, and resolves failed and failing banks.

This Top Management and Performance Challenges (TMPC) document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, in accordance with the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 10, 2021). This TMPC report is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

To compile this document, we considered comments from the FDIC, and while exercising our independent judgment, we incorporated suggestions where appropriate. We acknowledge several instances where the FDIC has taken steps to address the Challenge, particularly where the Agency has implemented concrete actions that demonstrate a direct relationship towards achieving a desired outcome. We also recognize that there may be other ongoing plans and intentions for future activities that might still be under development at the time of this writing.

We identified nine Top Challenges facing the FDIC:

The FDIC's Readiness for Crises. The FDIC must be prepared for all crises, because of its unique role in overseeing and administering the DIF, which insures the bank accounts of millions of depositors and consumers. The FDIC faces Challenges in fully developing its plans to respond to an unfolding crisis. Further, the FDIC should consider climate-related risks with respect to the report issued by the Financial Stability Oversight Council, and whether it will take actions in response to the report's recommendations in preparing its supervisory and examination processes. The FDIC should also be ready to respond to evolving risks associated with the current pandemic and other crises, including supervising and examining Government-guaranteed loans at banks and related fraud risks.

Cybersecurity for Banks and Third-Party Service Providers. Cybersecurity has been identified as the most significant threat to the banking sector and the critical infrastructure of the United States. The FDIC faces Challenges to ensure that examiners have the appropriate skillsets and knowledge to conduct information technology examinations that adequately identify and mitigate cybersecurity risks at banks and their third-party service providers (TSP). Further, the FDIC should establish a process to receive, analyze, and act on reports of significant cyber incidents at banks in order to adjust supervisory strategies, policies, and training for bank examiners; to warn other banks of such threats; and to prepare for potential bank failures. Mitigating cybersecurity risk is critical as a cyber incident at one bank or TSP has the potential to cause contagion within the financial sector. The FDIC also should assess the risks to banks presented by crypto assets, particularly with respect to the anonymous nature of these assets and the increased risk of money laundering and other wrongdoing.

Supporting Underserved Communities in Banking. The FDIC should ensure that its programs – including those that support Minority Depository Institutions and Community Development Financial Institutions -- are effectively designed to foster financial inclusion and reduce the number of unbanked and underbanked individuals. Further, the FDIC's examinations should continue to ensure that banks are in compliance with regulations that combat discriminatory lending practices against low-income borrowers and minority populations. The FDIC also should ensure that its examiners have the skills, capabilities, and procedures to assess the effect of banks' use of artificial intelligence in decision-making and minimize any undue bias related to the algorithms or historical data used.

Organizational Governance at the FDIC. Effective governance allows FDIC Board members and senior FDIC officials to manage the affairs of the Agency and its risks, formulate regulatory policy, and provide clear guidance to banks and FDIC Regional Offices. Through these processes, the FDIC can allocate resources, prioritize and improve the flow of risk information to decision-makers, and work towards achieving the FDIC's mission. The FDIC faces Challenges in providing clarity concerning the submission of motions presented to the Board of Directors for consideration and approval. Further, the FDIC should ensure that the Board, through its Audit Committee, can oversee and manage the risks identified and monitored through its Enterprise Risk Management Program. The FDIC also should clarify under what circumstances and which portions or provisions of Executive Branch policies or guidance are to be followed. In addition, the FDIC should ensure that weaknesses in FDIC programs are corrected and recommendations are addressed in a timely manner. FDIC rulemaking and guidance should also be aligned with other regulators to ensure that banks are not treated differently depending upon their primary regulator. FDIC internal guidance also should be clearly defined to ensure consistent application of FDIC program requirements. In addition, FDIC rulemaking should be a transparent process that analyzes the need for safety and soundness regulations and the compliance burden placed on banks.

Information Technology Security at the FDIC. The FDIC relies on its IT systems for day-to-day activities and especially during crises. The FDIC continues to face Challenges to ensure that it has strong information security processes to guard against persistent and increasing cyber threats against Federal agencies. Security control weaknesses of FDIC systems limit the effectiveness of FDIC controls, which places the confidentiality, integrity, and availability of FDIC systems and data at risk. The FDIC should address its outstanding corrective actions related to IT security controls, management of privileged Administrative Accounts, and oversight and monitoring of information systems. Further, the FDIC should ensure that it establishes effective security controls for its mobile devices and for the automated systems that monitor and control critical building services at facilities.

Security and Privacy at the FDIC. The FDIC employs a workforce of approximately 5,800 employees and 1,600 contract personnel at 92 FDIC facilities throughout the country, and it is custodian of 76 IT systems and voluminous hard-copy records. The FDIC should continue to manage risks associated with its personnel security and suitability processes to ensure that employees and contractors undergo appropriate and timely investigations and re-investigations commensurate with their positions. As well, the FDIC should maintain its risk-based physical security program and ensure that its policies promote an FDIC work environment that is free from discrimination, harassment, and retaliation. Further, the FDIC should have effective programs to safeguard all forms of sensitive and Personally Identifiable Information in its possession.

The FDIC's Collection, Analysis, and Use of Data. Data and information can enhance capabilities to mitigate threats against banks and the U.S. financial system. The FDIC faces Challenges in establishing effective processes to govern its sharing of threat information to guide the supervision of financial institutions. Effective sharing of threat information helps the FDIC to protect the DIF and the financial system by building situational awareness; supporting risk-informed decision-making; and influencing supervisory strategies, policies, and training.

The FDIC should establish a written governance structure and implement a Charter to establish a common understanding of its Threat Information Sharing program and define an overall strategy and requirements for it. Further, the FDIC should develop goals, objectives, and measures to guide the performance of its Intelligence Support Program, and it should establish adequate policies and procedures to define roles and responsibilities. The FDIC faces Challenges in the four component functions of Threat Information Sharing – acquisition, analysis, dissemination, and feedback. Further, the FDIC should improve the reliability of its internal data to ensure that the FDIC Board and senior officials can depend upon the data to assess program effectiveness throughout the organization.

Contracting and Supply Chain Management at the FDIC. The FDIC awarded over $2 billion in contracts for goods and services in 2021 in support of its mission. The FDIC faces Challenges to establish an effective contract management program that ensures the FDIC receives goods and services according to contract terms, price, and timeframes. Further, the FDIC should have processes in place to identify and ensure heightened monitoring of contracts for Critical Functions, so that the Agency maintains control of its mission functions and prevents over-reliance on contractors. The FDIC also should have programs in place to manage and mitigate security risks associated with the supply chains for contracted goods and services. Further, the FDIC should ensure notifications to contractors and sub-contractor personnel, so that they are advised about and aware of their whistleblower rights and protections, and that they know how to report allegations of misconduct, violations, and gross mismanagement.

Human Resources at the FDIC. The FDIC relies on the talents and skills of its employees to achieve its mission, and it faces Challenges in managing its human capital lifecycle. At the present time, nearly 25 percent of the FDIC workforce is eligible to retire, and this figure climbs to nearly 40 percent by 2026. These figures include personnel in key divisions supporting the FDIC mission – including the Division of Resolutions and Receiverships (over 59 percent by 2026); Division of Finance (over 55 percent by 2026); Legal Division (over 51 percent by 2026); and Division of Administration (about 49 percent by 2026). Further, the FDIC should continue to improve its program for the retention of employees, as well as the collection and analysis of relevant personnel data. In addition, the FDIC should continue to ensure diversity and inclusion among its workforce. Absent effective human capital management, the FDIC may lose valuable knowledge and leadership skill sets upon the departure of experienced examiners, managers, and executives. Meeting these Challenges is especially important as the FDIC shifts its operations to a hybrid work environment.

FDIC's Readiness for Crises

Key Areas of Concern

The primary areas of concern for this Challenge on Crisis Readiness are:

- Improving the Crisis Readiness framework at the FDIC and coordination with other financial regulators;
- Addressing climate-related risks to banks; and
- Supervising and examining banks for the risks associated with Government-guaranteed loans and fraud.

The OIG has identified Crisis Readiness as a Top Challenge for the FDIC since 2018.

The Financial Stability Oversight Council (FSOC), in its 2021 Annual Report (December 2021), stated that the "risks to U.S. financial stability today are elevated compared to before the pandemic." The FSOC Annual Report further indicated that "[s]ome episodes in financial markets [in 2021] generated unusually high volatility. . . Vulnerabilities include structural weakness in the financial system and its regulatory framework. Vulnerabilities in the financial system can amplify the impact of an initial shock, potentially leading to substantial disruptions in the provision of financial services." The FDIC should continue its efforts to be prepared for a wide range of crises that could affect bank operations, including cybersecurity threats, natural disasters, climate change, money laundering, and terrorism.

Improving the Crisis Readiness Framework at the FDIC and Coordination with Other Financial Regulators

The FDIC should fortify its operations and activities to address risks through the implementation of its Crisis Readiness plans. The FDIC should have agile supervisory processes to address risks stemming from crises, including climate-related risks.

In our OIG report, *The FDIC's Readiness for Crises* (April 2020), we found that the FDIC did not have documented Agency policy and procedures for a crisis readiness planning process; did not have an Agency-wide all-hazards readiness plan nor Agency-wide hazard-specific readiness plans; and did not train personnel on the plans' contents. The FDIC needed to fully establish seven elements of crisis readiness to be prepared to respond to any type of crisis that may impact the banking system: (1) policies and procedures; (2) plans; (3) training; (4) exercises; (5) lessons learned; (6) maintenance; and (7) assessment and reporting.

Based upon the findings in our report, the FDIC has taken several steps to institute crisis planning policies and procedures and has established a new Crisis Readiness & Response Section within the Division of Administration. While most of our recommendations have been implemented, the FDIC has yet to implement an important recommendation from our report issued in April 2020: to establish and implement Agency-wide hazard-specific readiness plans. Hazard-specific plans address special response procedures that may be unique to a particular hazard. The FDIC plans to implement this recommendation by March 2022.

In addition, the FDIC should coordinate with FSOC and its member agencies on Crisis Readiness planning. Both the Government Accountability Office (GAO) and the International Monetary Fund (IMF) have recommended that FSOC enhance its crisis preparedness role.[1] In particular, the IMF stated that FSOC "should devote greater attention to ensuring that the [Federal banking regulatory agencies] and the

Treasury have comprehensive and complementary organization-wide preparedness plans." FSOC's mandate includes responding to emerging financial stability threats and serving as a forum for coordination among its member agencies. As noted by the IMF, this design of FSOC allows for "collective crisis preparation to ensure decisive and coordinated responses from the entire FSOC community."

The Council of Inspectors General on Financial Oversight (CIGFO)[2] is preparing a guidance document for FSOC that is a compilation of information and activities that are integral to pre-crisis planning and crisis management. Once issued, the CIGFO Guidance may be used to assist FSOC in fulfilling its coordination role and help identify risks to the financial stability of the United States by considering: (i) the type of crisis planning materials that are available for collection and dissemination to and from member agencies; (ii) the threats posed to financial stability relating to potential gaps in crisis planning activities; and (iii) prioritizing crisis planning. In addition, the Guidance will provide useful information to member agencies about crisis readiness practices in order to improve preparedness procedures; identify potential gaps in readiness plans; and assist in managing future crises. The FDIC, as a member agency of FSOC, is in a position to support and advance this interagency effort.

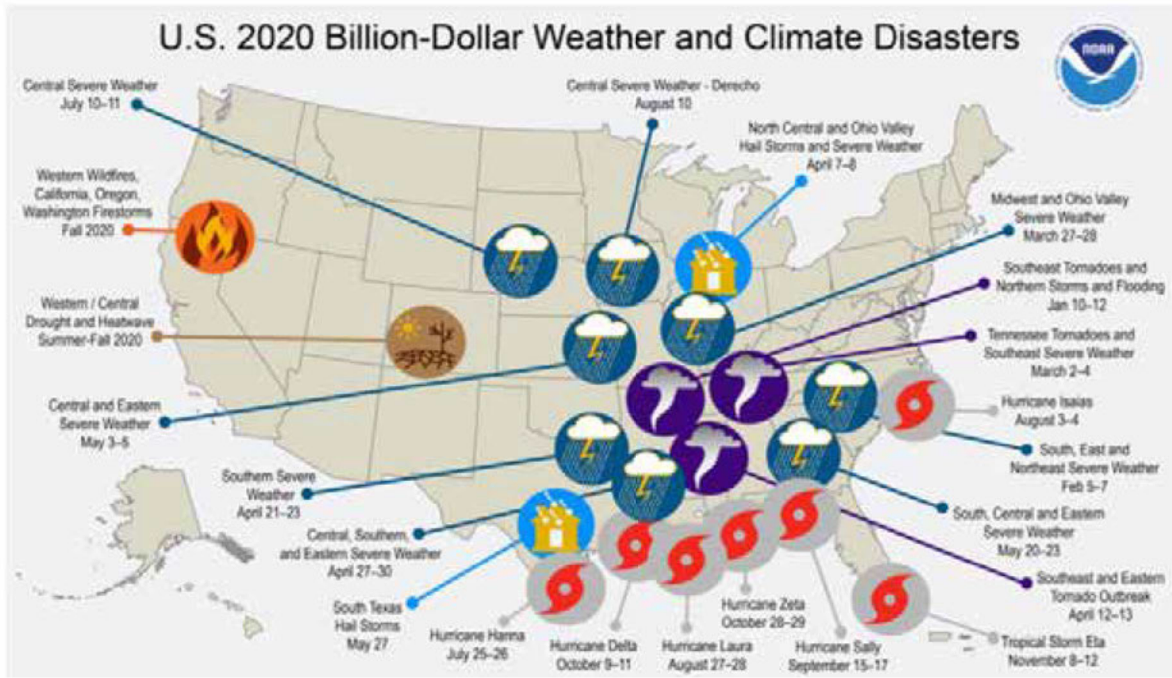
Addressing Climate-Related Risks to Banks

Banks may incur climate-related risks from exposure to losses from companies that rely on fossil fuels.[3] For example, banks may face losses on loans issued to entities that invest in oil, gas, power, utilities, and agriculture. According to CNBC, the "60 largest commercial and investment banks have collectively financed $3.8 trillion in fossil fuel company loans between 2016 and 2020."[4]

For the first time, both FSOC and the Federal Reserve Bank of New York have reported that climate change may affect the financial sector.[5] According to the Office of the Comptroller of the Currency (OCC), "[w]eaknesses in how banks identify, measure, monitor, and control the potential physical and transition risks associated with a changing climate could adversely affect a bank's safety and soundness, as well as the overall financial system."[6]

Further, bank portfolios include risk exposure to businesses and households that may suffer physical effects from climate-related risks.[7] According to estimates from the National Oceanic and Atmospheric Administration (NOAA), the cumulative cost for the 285 weather and climate disasters in the United States in 2020 exceeded $1.875 trillion, with 22 events resulting in at least $1 billion in damages (Figure 1).

Figure 1: U.S. 2020 Billion-Dollar Weather and Climate Disasters



Source: NOAA National Centers for Environmental Information, U.S. Billion-Dollar Weather and Climate Disasters (2021).

On May 20, 2021, the President signed Executive Order 14030, *Climate-Related Financial Risk,* to “advance consistent clear, intelligible, comparable, and accurate disclosure of climate-related financial risk.” This Executive Order required, among other things, an assessment of climate-related financial risk by Federal financial regulators.

On October 21, 2021, FSOC issued its *Report on Climate-Related Financial Risk* (FSOC Climate Report). The FSOC Climate Report characterized climate change as an “emerging threat to the financial stability of the United States” and made 30 recommendations to FSOC members related to four topic areas:

- **Building capacity and expanding efforts to address climate-related financial risks.** Agencies should invest in their capacity to define, identify, measure, monitor, assess, and report on the financial impact of climate change.
- **Filling climate-related data and methodology gaps.** Agencies should compile an inventory of existing climate-related risk data and develop plans to acquire additional needed data through collection, sharing, or procurement.
- **Enhancing public climate-related disclosures.** Agencies should assess current public disclosure requirements and adjust them to address climate-related risks.
- **Assessing and mitigating climate-related risks that could threaten the stability of the financial system.** Agencies should use scenario analysis such as modeling to assess climate-related financial risk and assess whether additional regulations or guidance are needed to clarify supervisory expectations.

The FSOC Climate Report noted that coordination among regulators, including international bodies, should be robust in order to expand capacity, improve data and measurement, enhance disclosures, assess the scale of potential vulnerabilities, and make appropriate adjustments in regulatory and supervisory tools. CIGFO is currently reviewing the actions of FSOC and its member agencies regarding the implementation of Executive Order 14030 and the recommendations in the FSOC Climate Report.

The FDIC Chair (hereinafter referring to the Chair who served from June 2018 to February 2022) abstained from casting her vote on the FSOC Climate Report, explaining that "FSOC has not had an adequate opportunity to conduct sufficient analysis, fully consider broader macro consequences, and thoroughly evaluate the impact of its recommendations."[8] The FDIC will need to determine whether it intends to implement the recommendations contained in the FSOC Climate Report. If the FDIC plans to implement the FSOC recommendations, the Agency will need to decide how it will undertake such actions. If the FDIC does not intend to implement such recommendations, it may be out of step with other Federal financial regulators with respect to bank examinations, crisis preparedness, and risk management.

In response to performance goals noted in the FDIC 2021 Annual Performance Plan, FDIC economists and policy staff have been working with other regulatory agencies and international bodies on climate-related financial risks, including participation on the Task Force for Climate-Related Financial Risks of the Basel Committee on Banking Supervision. The FDIC Division of Insurance and Research also has conducted research on climate-related risk to local banks and economies for six weather events in the United States. This research also assessed the impact on low- and moderate-income areas before and after each climate event.

In late 2021, the FDIC engaged with other banking regulators to draft a Request for Information and Comment (RFI/C) on climate-related financial risks. However, this RFI/C document was never issued or published, and as a result, no comments were received.

On December 16, 2021, the OCC issued a set of draft principles designed to support the identification and management of climate-related financial risks at institutions. These risks include Credit Risk, Liquidity Risk, Operational Risk, Legal/Compliance Risk, as well as other financial and non-financial risks. FDIC Regional Risk Committees have identified climate-related risks on a regional level, but as of December 2021, the FDIC had not identified climate-related risk on its Agency-wide Risk Inventory or Risk Profile as part of its Enterprise Risk Management program.

In order to address the FSOC recommendations, the FDIC would need a coordinated effort among its Divisions and Offices, other regulators, and international organizations.[9] In so doing, the FDIC would need to continue to gather climate-related risk data and establish processes to define, measure, monitor, assess, and report on these risks.

Further, according to the FSOC Climate Report, climate-related risk may disproportionately affect vulnerable populations and underserved communities. Additionally, the Environmental Protection Agency stated that "the most severe harms from climate change fall disproportionally upon underserved communities who are least able to prepare for, and recover from, heat waves, poor air quality, flooding and other impacts."[10] The FDIC will need to continue to consider how such risks affect its programs serving these communities.

Supervising and Examining Banks for the Risks Associated with Government-Guaranteed Loans and Fraud

In March 2020, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) created the Paycheck Protection Program

(PPP) in order to provide financial relief and Government-guaranteed loans to small businesses adversely affected by the pandemic. The PPP loans are provided through our Nation's banks and the program is administered by the Small Business Administration (SBA). According to the SBA, more than 11 million PPP loans were issued by more than 5,400 lenders—primarily community banks supervised by the FDIC. These PPP loans amounted to nearly $800 billion.[11] According to a study by the University of Texas, it is estimated that more than seven percent of loans made by banks had indications of fraud.[12]

As of March 2021, approximately 83 percent of FDIC-supervised institutions (2,689 banks) carried PPP loans on their balance sheets. These institutions held approximately 1.5 million PPP loans totaling about $145 billion. Based on our analysis of PPP loan data, 46 FDIC-regulated banks had PPP loan portfolios that accounted for more than 20 percent of the bank's total assets. In fact, six such banks held portfolios where PPP loans ranged from 50 to 75 percent of the bank's total assets.

As of March 2021, the U.S. Government has charged 474 defendants in 56 Federal districts with crimes related to pandemic fraud.[13] In particular, FDIC OIG investigations resulted in more than 110 indictments and criminal complaints, resulting in 65 arrests and 41 convictions. These cases involve defendants who aim to steal funds from a Government program that was intended to help those most in need during the pandemic. The PPP fraud schemes are complex and sophisticated, and they involve the use of synthetic identities, financial technology services (FinTech), bank insiders, and criminal organizations.

In June 2020, the FDIC stated its view that, "[g]iven the 100 percent SBA guarantee, there is, in effect, no credit risk associated with loans extended under the program, provided the lender complied with its obligations under the PPP."[14] However, because of the substantial volume of PPP loans at FDIC banks and the potential fraud associated with this program, there may be risk to banks that have not complied with the requirements of the PPP loan program. According to the program requirements, the Government may be released from its guarantee obligation if a bank fails to materially comply with program requirements, such as loan administration, underwriting, and servicing. If banks are not in compliance with program requirements, they may be required to absorb PPP loan losses. As a result, the loan guarantee is not absolute, and banks may bear credit risk for non-compliance with the PPP program.

The OCC has recognized banks' heightened compliance risks for PPP loans in its recent report *Semiannual Risk Perspectives* (Fall 2021), as well as in its prior OCC reports. In addition, PPP loans may pose reputational and compliance risks to financial institutions, and banks may have to set aside additional funding to address compliance and legal risks associated with potential loan revocation. We have ongoing work to review the FDIC's examination of the risks associated with PPP and other Government-guaranteed loans.

As a banking regulator that insures deposits and resolves failed banks, the FDIC must remain vigilant in preparing for future crises. The FDIC should continue to expeditiously develop and implement its Crisis Readiness framework and coordinate with other financial regulators. In so doing, the FDIC should assess and address the impact of climate-change risks in its crisis preparedness program activities and bank supervision. Further, the FDIC should closely examine the risks posed by guaranteed loan fraud.

Cybersecurity at Banks and Third-Party Service Providers

Key Areas of Concern

The primary areas of concern for this Challenge on Cybersecurity at Banks and Third-Party Service Providers (TSP) are:

- Ensuring that FDIC bank examinations adequately assess and address cybersecurity risks at financial institutions and their TSPs;
- Ensuring that banks report serious cyber security incidents to the FDIC in a timely manner, so that it can take appropriate action; and
- Supervising and managing risks associated with crypto assets.

The OIG has identified Cybersecurity in the banking sector as a Top Challenge for the FDIC since 2018, particularly with respect to TSPs and emerging technologies.

FSOC, in its *2021 Annual Report* (December 2021), noted that "[a] destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system by disrupting a key financial service or utility, causing loss of confidence among a broad set of customers or market participants, or compromising the integrity of critical data." The FSOC Annual Report continued that the financial sector "is vulnerable to ransomware and other malware attacks, denial of service attacks, data breaches, and other events. Such incidents have the potential to impact tens or even hundreds of millions of Americans and result in financial losses of billions of dollars due to disruption of operations, theft, and recovery costs."

In April 2021, the Chairman of the Federal Reserve Board (FRB) also identified cybersecurity risk at banks as the most significant risk to financial institutions today.[15] The FRB Chairman explained that "[t]here are cyber-attacks every day on all major institutions" and a successful attack on a large institution could cause a broad part of the financial system to come to a halt. According to *the OCC Semiannual Risk Perspective (Fall 2021)*, banks' expanded use of remote work for employees and increased use of TSPs increases the importance of cyber controls. Analysis by the Financial Crimes Enforcement Network (FinCEN) found that banks reported more than $590 million in suspicious activity related to ransomware in just the first 6 months of 2021. This figure was greater than the amount reported for the entire previous year ($416 million reported in 2020) – an increase of approximately 41 percent.

Banks may suffer cyber attacks directly at the institutions, or alternatively through interconnections with third parties that provide banks with services, such as accounting, transaction processing, loan servicing, and human resources.[16] *The 2021 FSOC Annual Report* stated that "financial institutions have increased their reliance on third-party service providers for teleworking tools and services. The interdependency of these networks and technologies supporting critical operations magnifies cyber risks, threatening the operational risk mitigation capabilities not just at individual institutions, but also of the financial sector as a whole."

In the *OCC Semiannual Risk Report* (Fall 2021), the OCC recognized that cyber actors continue to exploit "vulnerabilities in third-party hardware and software systems to conduct malicious cyber activities." Further, the Federal Reserve noted that "[c]yber shocks may spread through the financial system through complex and often unrecognized interdependencies across firms, including a layer of exposures to shared technologies and third-party service providers."[17] For example, in December

2021, the Cybersecurity & Infrastructure Security Agency issued an Emergency Directive regarding a vulnerability in remote software used by banks known as Apache Software Foundation's Log4j. For banks running this software, the vulnerability may allow hackers to download malware in order to steal customer login information, transfer funds, and open fraudulent accounts.[18] Also, in July 2021, cyber-hackers targeted the remote software of information technology (IT) firm Kaseya, which provides software as a service to banks. As a result, hackers were able to infiltrate Kaseya customers' networks and install ransomware. The ransomware locked the victim companies' data and released it only after a ransom of $70 million was paid in cryptocurrency.

Assessing and Addressing Cybersecurity Risks at Banks and Third-Party Service Providers

According to the Boston Consulting Group, "[f]inancial services firms are 300 times as likely as other companies to be targeted by a cyberattack."[19] A study by Constella Intelligence found that between 2018 and 2021, financial services companies suffered nearly 6,500 breaches that exposed 3.3 million records, including email communications, dates of birth, credit card information, addresses, telephone numbers, and account login credentials.[20] Further, bank employees' remote work increases cyber risks as employees access information remotely through multiple connections.[21] Employee wireless networks, router software, and cameras provide new means for cyber attacks.

Financial institutions of all sizes, including community banks, may be targets of cyber attacks. For example, in May 2021, two ransomware groups appear to have infiltrated the servers of three community banks, stealing data and demanding a ransom.[22] In the following month, a ransomware group attacked a New Jersey community bank. The bank stated that it was able to contain the attack, because it was made on a network that was separate from its operational systems.[23]

FDIC IT examinations must be capable of identifying and addressing weaknesses in cybersecurity risk management at supervised banks and their TSPs. The FDIC conducts IT risk examinations to assess whether bank management has appropriate controls in place to mitigate cybersecurity risks and to assess financial institutions' management of TSP risk. The FDIC also examines a subset of TSPs for the soundness of their risk management and cybersecurity practices. Since 2016, the FDIC has been using the Information Technology Risk Examination (InTREx) work program[24] to conduct bank IT examinations and assess financial institutions' oversight of TSPs. An initial InTREx procedure, the Information Technology Profile scoring matrix, is used by examiners to determine the scope of an IT examination consistent with the bank's IT complexity and risk profile, and to allocate resources to the examination. The scope of an IT examination may increase due to, among other things, the introduction of new business lines or technology, or the addition of a TSP.

The FDIC should ensure that its assessments accurately capture current and relevant risks and reflect the scope and complexity of banks' IT security and systems. The FDIC should also ensure that it has appropriate examination processes, resources, and staff. FDIC examiners should have up-to-date information on cyber controls and threats, and the requisite skills to identify risks and complete thorough examinations.

We are currently conducting an audit of the InTREx program. The objective of our work is to determine the effectiveness of the InTREx program in assessing and addressing IT and cyber risks at FDIC-supervised financial institutions.

Reporting Cybersecurity Incidents at Banks

Banks should report cyber incidents to Federal regulators in a timely manner so that the regulators may take appropriate supervisory actions to address and mitigate the risks associated with such incidents. It is important for regulators to receive this information, as a cyber incident at one bank could result in contagion from the affected bank to another bank, and prompt similar attacks at other banks. Armed with knowledge of cyber incidents, the FDIC can warn other supervised banks of these threats and execute preparations for potential bank failures if needed. Further, cyber incident reporting may allow the FDIC to shift examination and resolution resources to address these cyber risks. The FDIC also may use these incident reports to adjust its supervisory strategies, as well as its examinations, policies, and training to assist examiners in identifying and mitigating emerging risks.

On April 30, 2020, the OIG issued *a Management Advisory Memorandum* to the FDIC uncovering a gap in regulation. Federal regulations did not require banks to report destructive cyber incidents to Federal banking regulators, even though such incidents could jeopardize the safety and soundness of an institution. In response to our OIG Management Advisory Memorandum, Federal banking regulators proposed a regulation that would require financial institutions to promptly notify their primary Federal regulator in the event of a computer security incident.[25]

On November 18, 2021, Federal banking regulators promulgated a rule requiring that banks report computer security incidents "no later than 36 hours after the banking organization determines that a notification incident has occurred."[26] The FDIC should ensure that it has clear guidance, procedures, and processes in place to receive, evaluate, analyze, and investigate these reports from the banks.

Supervising and Managing Risks Posed by Crypto Assets

Crypto assets are a digital form of value that is issued or transferred using distributed ledger or blockchain technology.[27] The 2021 FSOC Annual Report recognized that "the rapid growth of digital assets, including stablecoins and lending and borrowing on digital asset trading platforms, is an important potential emerging vulnerability." The FSOC Report continued that digital assets "pose risks related to illicit financing, national security, cybersecurity, privacy, and international monetary and payment system integrity." It has been reported that the cryptocurrency market amounted to more than $2 trillion.[28]

According to the OCC Semiannual Risk Report (Fall 2021), banks are exploring "the development of crypto-custody services, crypto-asset derivative products, or the provisions of access to third-party crypto-related products." The Basel Committee on Banking Supervision stated that virtual currencies "raise financial stability concerns and increase risks faced by banks."[29] Crypto assets "have exhibited a high degree of volatility, and could present risks for banks as exposures increase, including liquidity risk, credit risk, market risk, operational risk (including fraud and cyber risks), money laundering / terrorist financing risk, and legal and reputation risks."[30]

The U.S. regulatory landscape for digital assets is unclear and fragmented. In May 2021, the Secretary of the Treasury stated that the United States does not yet have an "adequate framework" for tackling cryptocurrency regulation.[31]

The FDIC Chair noted that stablecoins (a fungible token pegged to or redeemable for fiat currency) could also lead to "money migrating out of insured banks with significant ramifications for credit creation, financial stability, and bank funding."[32] The Chairman of the FRB stated that "if [stablecoins] are going to be a significant part of the payments universe . . . we need an appropriate regulatory framework, which frankly we don't have."[33] The President's Working Group on Financial Markets' *Report on Stablecoins* noted that the prospect of a stablecoin not performing could cause mass redemption of multiple coins and fire sales of the reserve assets.[34] The market capitalization for stablecoins was estimated at approximately $115 billion as of July 2021.[35]

The FDIC should assess the risks involved with banks' entry into crypto assets and stablecoins, and determine what regulatory actions to take. The FDIC should also ensure that examiners have proper skillsets and training to understand and assess these risks. In addition, because the FDIC becomes responsible for the assets of a failed U.S. bank, the FDIC should determine how to resolve banks that hold digital assets. On May 21, 2021, the FDIC issued a request for information soliciting comments about current and potential digital asset activities. On November 23, 2021, bank regulators, including the FDIC, summarized their work on a crypto asset policy "sprint" on crypto-asset-related activities.[36] The FDIC's work in this area remains ongoing.

A cyber incident at a bank or its TSP has the potential for wide disruption throughout the banking sector. The FDIC should ensure that it has the procedures and personnel with the appropriate skills to conduct effective IT examinations to assess banks' cybersecurity risks. The FDIC should receive prompt notification of bank cyber incidents in order to take appropriate supervisory action. Further, the FDIC should evaluate the risks to banks posed by cryptocurrencies and stablecoins, and adjust FDIC guidance, policies, supervisory strategies, examination procedures, and training accordingly.

Supporting Underserved Communities in Banking

Key Areas of Concern

The primary areas of concern for this Challenge on Supporting Underserved Communities are:

- Fostering financial inclusion for the unbanked and underbanked; and
- Understanding bias risk associated with technology.

The OIG has identified Supporting Underserved Communities as a Top Challenge for the FDIC since 2020.

According to the World Bank, financial inclusion is a "key enabler to reducing poverty and boosting prosperity."[37] As noted by the FDIC Chair, "[w]hen talking about financial inclusion, the question before us is not merely whether a person has a checking account or a credit card but, more fundamentally, whether they are a part of the financial fabric of the United States."[38]

Fostering Financial Inclusion for the Unbanked and Underbanked

On January 20, 2021, the President issued Executive Order 13985, *Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, which aims to pursue a comprehensive approach to advancing equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality. The Executive Order requires that most Federal agencies "recognize and work to redress inequities in their policies and programs that serve as barriers to equal opportunity." Such policies and programs should include those geared towards financial inclusion.

In June 2021, the FDIC Chair emphasized, however, that despite the Agency's efforts, "millions of American households remain unbanked and millions of Americans do not have a credit score."[39] The Chair noted that "[t]he persistent gap in access to the banking system has shown that we must think outside the box to create a regulatory system that will help close this gap."

In a study published in October 2020, the FDIC found that 7.1 million U.S. households (5.4 percent) lacked a checking or savings account at an insured financial institution. Importantly, minority households were more likely to be among the unbanked. For example, 13.8 percent of Black households surveyed and 12.2 percent of Hispanic households surveyed were unbanked in 2019, as compared to only 2.5 percent of White households.

Further, as noted in the Crisis Readiness section of this Report, climate-related risk may disproportionately affect vulnerable populations and underserved communities. The Environmental Protection Agency stated that "the most severe harms from climate change fall disproportionally upon underserved communities who are least able to prepare for, and recover from, heat waves, poor air quality, flooding and other impacts."[40] The FDIC will need to consider how climate-related risks affect its programs serving these communities.

The FDIC should also ensure that its programs designed to foster financial inclusion and reduce the number of unbanked and underbanked individuals are effective. These programs include support of Minority Depository Institutions (MDI) and Community Development Financial Institutions (CDFI) that provide financial products and services to individuals and businesses in minority, low-income, and rural communities. The FDIC also promotes access to banking through community affairs programs in its Regional Offices.

Further, the FDIC conducts examinations to ensure that banks are in compliance with regulations such as the Community Reinvestment Act (CRA). The CRA and its regulations aim to “combat the legacy of discriminatory lending practices against low-income borrowers and minority populations.”[41]

In September 2021, the FDIC launched an initiative to address unbanked households. The Mission-Driven Bank Fund is a capital investment vehicle that will channel private-sector investments to support MDIs and CDFIs. The Fund is intended to help MDIs and CDFIs raise capital. Although the FDIC does not participate in the Fund’s management or individual investment decisions, the FDIC should assess the alignment of the Fund’s ongoing operations with FDIC objectives to ensure the advancement of equity in underserved communities. In addition, in November 2021, the FDIC established a new Office of Minority and Community Development Banking to support the Agency’s engagement with MDIs, CDFIs, and other mission-driven banks.[42] This effort remains under development.

Understanding Bias Risk Associated with Technology

According to the World Economic Forum survey of 151 global financial services companies, 85 percent are using artificial intelligence (AI) in their operations.[43] Banks’ use of AI includes, for example, lending decisions.[44] While AI has the potential to lower lending costs and improve the speed of credit decisions, such innovative technologies may have unintended consequences, such as the exclusion of individuals based on biased algorithms or flawed data.[45]

The Federal Reserve Bank of San Francisco noted that unchecked technological innovation can introduce a variety of risks and consumer harm.[46] Specifically, the Federal Reserve Bank of San Francisco cited a research study from the University of California at Berkley that indicated that machine learning can result in minority borrowers experiencing higher loan rates and more expensive financial products. Algorithms and complex machine learning models, such as AI, may rely on outdated or flawed data or mistakes in rule development.[47] For example, AI algorithms may perpetuate discriminatory lending practices and higher interest rates charged to African American and Latino borrowers, as reflected in historical loan data.[48]

On November 29, 2021, the Chairwoman of the Committee on Financial Services, U.S. House of Representatives, and Congressman Bill Foster transmitted a letter to financial regulators, including the FDIC, noting that the use of historical data as “inputs for AI and ML [machine learning] can reveal longstanding biases, potentially creating models that discriminate against protected classes, such as race or sex, or proxies of these variables.” The Committee highlighted several principles: Transparency and Explainability; Oversight and Enforceability; Safeguarding Consumer Privacy; and Promoting Fairness and Equity in AI Usage. The letter encouraged regulators to keep pace with the rapid developments to “ensure that AI regulation and rulemaking can meaningfully address appropriate governance, risk management, and controls over AI.”

The FDIC's consumer compliance examiners should have the proper skillsets to understand and assess the new technologies used by banks and detect potential biases. Further, examiners should have effective examination processes and procedures to monitor for technology biases.

The FDIC plays an important role in fostering economic inclusion and maintaining confidence in the U.S. banking system. It is well positioned to help support and empower minority communities' access to capital. The FDIC should continue its efforts to assess the effectiveness of its MDI and CDFI outreach programs and continue to promote financial and technological innovations to achieve economic inclusion while at the same time avoiding potential biases.

Organizational Governance at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge on Organizational Governance are:

- Clarifying protocols for submissions to the FDIC Board of Directors;
- Incorporating important risks into the FDIC's Enterprise Risk Management (ERM) program;
- Explaining whether the FDIC will follow certain Executive Branch policies and guidance;
- Addressing recurring recommendations;
- Ensuring clarity and consistency of FDIC policies and alignment with other regulators; and
- Enhancing FDIC rulemaking.

The OIG has identified Governance as a Top Challenge for the FDIC since 2018, particularly with respect to ERM and rulemaking.

FDIC Board members and senior FDIC officials are responsible for administering the affairs of the Agency, managing its risks, establishing regulatory policy, and providing clear guidance to banks and throughout the Agency. Organizational governance refers to a management framework that incorporates operational, financial, risk management, and reporting processes so that FDIC Board members and senior officials can effectively plan, govern, and meet strategic objectives.[49] A governance framework should ensure strategic guidance, effective monitoring of management, and accountability to stakeholders.[50]

FDIC Board members are appointed by the President and confirmed by the Senate, and include: the FDIC Chair, FDIC Vice Chair, Comptroller of the Currency, Director of the Bureau of Consumer Financial Protection (CFPB), and an independent Director. The FDIC Board has been operating with only four members since 2015, and the Vice Chair position has been vacant since April 2018. On December 31, 2021, the FDIC Chair announced that she would be resigning from her position, effective February 4, 2022 – thus, leaving three remaining members of the FDIC Board (an acting FDIC Chair, CFPB Director, and acting Comptroller of the Currency). In February 2022, the FDIC's Chief of Staff and Chief Operating Officer, Chief Innovation Officer, General Counsel, and Deputy Director for Policy also announced their departures from the FDIC. The Director of the Division of Insurance and Research will also retire in 2022.

Clarifying Protocols for Submissions to the FDIC Board of Directors

FDIC Board members play a critical role in shaping FDIC policies and processes. FDIC Board members are responsible for considering and approving motions brought before the Board, such as the issuance or modification of regulations and guidance. However, the process for bringing such measures to the Board has been in dispute.

On November 26, 2021, the CFPB Director, as a member of the FDIC Board, requested that the Board take action to publish a Request for Information and Comment (RFI/C) regarding bank merger transactions; this action was also recommended by two other Board members. On the same day, the FDIC General Counsel wrote that this action was not valid, because the FDIC bylaws do not confer authority to an individual Board member to circulate an item for a vote, and such authority rests with the Executive Secretary under the supervision of the General Counsel and at the direction of the Chair.

On December 6, 2021, the three Directors submitted written votes to approve the RFI/C, and the FDIC General Counsel reiterated his position that the CFPB Director (as a member of the FDIC Board) did not have authority to circulate an item for a vote, and that the subsequent Directors' responses did not constitute valid votes. The CFPB Director expressed his view that the FDIC Board had approved the RFI/C.

On December 9, 2021, the CFPB released the RFI/C on its website, and the FDIC issued a statement that the document was not approved for publication because there was no valid vote by the FDIC Board according to longstanding FDIC internal policies and procedures.[51] At a Board meeting on December 14, 2021, the CFPB Director (as a member of the FDIC Board) moved that the written vote on the RFI/C be included in the minutes of the Board meeting, and the Chair ruled that the motion was not in order.

The dispute about the authorities of the FDIC Chair and individual Board members to bring items before the FDIC Board for a vote creates uncertainty about the organizational governance and structure of the FDIC. The FDIC should clarify and resolve the requirements for consideration of actions by the FDIC Board of Directors.

Incorporating Risks into the FDIC's Enterprise Risk Management Program

The FDIC faces an array of risks that should be identified, assessed, and considered by the FDIC Board and senior FDIC officials. Enterprise Risk Management (ERM) is an essential component of governance that provides an entity-wide view of the full spectrum of internal and external risks facing an organization. Effective ERM provides information to Board members and senior FDIC officials, so that they can allocate resources appropriately, effectively prioritize and proactively manage risk, improve the flow of risk information, and work towards achieving the FDIC's mission. ERM assists Federal agencies in the identification, assessment, and mitigation of external and internal risks. On May 25, 2021, the FDIC Board delegated ERM responsibilities to its Audit Committee, which now oversees the ERM program and is responsible for ensuring that relevant risks are identified and addressed. It is not clear or transparent the processes by which the FDIC Audit Committee will consider the range of risks facing the enterprise, and debate and deliberate over the proposed risk ratings. The Audit Committee oversees and has responsibility for the agency's ERM activities.

In our OIG evaluation, *The FDIC's Implementation of Enterprise Risk Management* (July 2020), we determined that ERM was not fully implemented at the FDIC, and, therefore, proper execution of program activities, roles, and responsibilities had yet to take place. Without a mature governance structure over ERM, the FDIC could not be sure that ERM would be fully integrated into the Agency and its culture, and the FDIC would develop a comprehensive portfolio view of risk at the Agency. The FDIC addressed the eight recommendations from our OIG report. In 2021, the FDIC conducted a survey of Agency personnel about the ERM program; the response rate was 22 percent. The FDIC survey noted that less than half of survey participants were familiar with the FDIC's ERM program, including the FDIC's Risk Appetite Statement and how to use it.

Further, since the issuance of our report, we have found that the FDIC's ERM process has not identified certain existing risks and not fully assessed the potential impact of other risks, for example:

- **Personnel Security and Suitability.** In our report, *The FDIC's Personnel Security and Suitability Program* (January 2021), we found that the FDIC's ERM program did not fully reflect the extent of risks associated with untimely, incomplete, or inadequate background investigations.

- **Critical Functions in Contracts.** In our report, *Critical Functions in FDIC Contracts* (March 2021), we found that the FDIC's ERM Risk Inventory did not recognize procured Critical Functions as a separate and distinct risk, or as an analytical factor in determining inherent or residual risk associated with cybersecurity and privacy support services. A Critical Function is an activity that is necessary for an agency to effectively perform and control its mission and operations.

- **Climate-Related Financial Risk**. The ERM program has not considered or addressed the risks associated with climate change, as identified in the FSOC Climate Report (referenced in the Crisis Readiness Challenge).

- **Supply Chain Risk.** The FDIC has not established an Agency-wide consideration of supply chain risk. As a result, the FDIC's ERM does not capture certain supply chain risks that FDIC Divisions and Offices face, nor does it capture supply chain risks associated with non-IT products and services.

We also note that the FDIC's Enterprise Risk Management program has not considered the risks associated with the requirements for Board of Directors' consideration and approval of motions (discussed above), nor the risks related to the Agency's review of bank mergers noted in the RFI/C submitted and approved by the three FDIC Directors.[52] These risk factors are not part of the FDIC's Risk Inventory nor its Risk Profile.

Explaining Whether the FDIC Will Follow Certain Executive Branch Guidance

The Executive Branch regularly issues policies and guidance for Federal agencies, in the form of Executive Orders, Presidential Directives, OMB Circulars and Memoranda, and National Institute of Standards and Technology (NIST) guidance. Such policies and guidance often address risks in operational areas such as information technology, security, privacy, contracting, and risk management. The policies and guidance provide best practices that Executive Branch agencies must implement to mitigate operational risks. In many cases, independent agencies such as the FDIC are not required to follow such requirements; however, the FDIC has, in a number of cases, chosen to voluntarily comply with all, or portions of, certain policies and guidance.

It is not clear under what circumstances and which specific portions or provisions of the policies or guidance are to be followed. Ambiguity in the FDIC's determinations and lack of clarity may result in inconsistencies with other agencies (including other bank regulators) and may cause uncertainty and confusion among FDIC employees in the application of such policies and guidance. In addition, such determinations may not seem clear or transparent to the American public.

For example, in our OIG report, *Whistleblower Rights and Protections for FDIC Contractors* (January 2022), we found that the FDIC Division of Administration's (DOA) Acquisition Services Branch voluntarily adopted some of the Federal whistleblower provisions and requirements for insertion into its contracts. However, the FDIC's Legal Division, under its separately delegated contracting authority, did not operate consistently with the FDIC's DOA. The FDIC Legal Division had neither adopted any whistleblower rights notification provisions for contractors nor included any whistleblower clauses in its contracts. Further, we found that FDIC procedures and processes were not aligned with laws, regulations, and policies designed to ensure notice to contractor and subcontractor employees about their whistleblower rights and protections.

The FDIC should clearly articulate and explain its determinations regarding whether or not to follow Executive Branch policies and guidance, and it should be transparent under what circumstances and which specific portions or provisions of the policies or guidance are to be followed. Consistent analysis and application, and centralized documentation of these decisions would enhance the confidence and transparency of FDIC operations, programs, and functions.

Further, in our recent OIG reports, we found that when the FDIC chooses not to implement certain Executive Branch policies, its programs incur risks that these policies were intended and designed to address or mitigate. For example:

- **Contracting:** The OMB issued Policy Letter 11-01 to provide Federal agencies with guidance on managing contracts for the performance of Critical Functions.[53] The FDIC's Legal Division concluded that the Policy Letter did not apply to the FDIC, but it may be used for guidance. In our OIG evaluation, *Critical Functions in FDIC Contracts* (March 2021), we found that the FDIC did not have policies and procedures for identifying Critical Functions in its contracts, as recommended by the OMB Policy Letter. Without these best practices in place, the FDIC cannot be assured that it will provide sufficient management oversight of contractors performing Critical Functions.

- **Enterprise Risk Management (ERM):** In 2016, in an effort to modernize existing agency risk management efforts across the Federal Government, the OMB updated its Circular A-123.[54] The FDIC took the position that it was not required to follow OMB Circular A-123. As noted earlier, in our OIG evaluation, *The FDIC's Implementation of Enterprise Risk Management* (July 2020), we found that the FDIC did not fully implement its ERM program in accordance with OMB criteria. Specifically, the FDIC did not establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to ERM. Further, the FDIC did not clearly define the roles, responsibilities, and processes of the committees and groups involved in ERM.

- **Supply Chain Risk:** In our OIG report on *The FDIC's Information Security Program—2021* (October 2021), the FDIC stated that the NIST publications for supply chain risk management were not binding on the FDIC, but that the FDIC chose to follow the guidance. NIST guidance includes a Risk Management Framework for supply chains, and the framework is purposefully designed to be technology neutral so that the methodology can be applied to any type of information system without modification.[55] However, the FDIC's Supply Chain Risk Management (SCRM) Directive limits the applicability of the NIST framework solely to IT systems, products, and services. As a result, non-IT purchases are not assessed against the NIST framework for supply chain risks.

- **Rulemaking Cost Benefit Analysis:** In our report, *Cost Benefit Analysis Process for Rulemaking* (2021), we found that the FDIC did not follow identified best practices from Executive Orders, GAO, and other Federal agencies to establish and document a process for determining when to perform cost benefit analyses and how the analyses should be conducted.

Addressing Recurring Recommendations

The FDIC Board and senior officials should also ensure that program weaknesses are promptly resolved and remediated. The FDIC has encountered several examples in which the OIG has made repeated recommendations to the FDIC in order to improve its programs and operations. Unaddressed program improvement recommendations increase the likelihood that the underlying vulnerabilities or deficiencies will continue or recur. To mitigate these risks, these recommendations should be addressed by the FDIC in a timely manner.

We have identified repeated breakdowns in controls, for example:

- **Incomplete contract files.** We made recommendations to address incomplete contract files in two reports issued between 2018 and 2019. In our OIG reviews *Payments to Pragmatics* (December 2018) and *Contract Oversight Management* (October 2019), we found that FDIC personnel did not retain appropriate contract documentation in the FDIC's contract repository known as "CE File." Without this documentation, the FDIC faces challenges in monitoring and enforcing contracts in the event of contractor noncompliance. Further, the FDIC may incur additional costs to recover or replace lost documentation, as such processes may require labor-intensive manual searches through hard-copy documentation.

- **Confidentiality Agreements for Contractors.** We identified missing or inadequate Confidentiality Agreements in three reports between 2017 and 2022. In our OIG reviews *Controls over Separating Personnel's Access to Sensitive Information* (September 2017), *Security of Critical Building Services at FDIC-owned Buildings* (March 2021), and *Whistleblower Rights and Protections for FDIC Contractors* (January 2022), we found that the FDIC either did not obtain Confidentiality Agreements from its contractors and contract personnel as required by the contracts, or did not use the current up-to-date Confidentiality Agreement form. Without the required Confidentiality Agreements, the FDIC has reduced assurance that contractors and subcontractors will protect sensitive FDIC information.

- **Cybersecurity.** In each of our past four annual reviews of FDIC information security (2018 through 2021), we reported weaknesses related to the FDIC's management of Administrative Accounts.[56] Weaknesses in the FDIC's processes for managing Administrative Accounts increase the risk of unauthorized activity, such as individuals accessing, modifying, deleting, or exfiltrating sensitive information. We also found that the FDIC continues to have overdue and unaddressed information security control deficiencies. Without consistently addressing control deficiencies in a timely manner, FDIC data is vulnerable to security exploits from unmitigated threats.

- **Personnel Security and Suitability Program.** In our OIG evaluation, *The FDIC's Personnel Security and Suitability Program* (PSSP)(January 2021), we found several deficiencies that were similar to those identified in previous reports -- including our OIG *evaluation* of the FDIC's PSSP conducted 6 years earlier in 2014.[57] Specifically, a number of issues had not been corrected, including:
  - Completing preliminary background investigations within allowed timeframes;
  - Keeping records of background investigation documentation;
  - Ensuring that background investigation levels match an individual's position risk; and
  - Ensuring the reliability of background investigation data in FDIC systems.

The FDIC should ensure that the Agency addresses programmatic weaknesses in a timely manner. Absent correction, these weaknesses continue to inhibit program performance and expose FDIC information, systems, and personnel to vulnerabilities.

Ensuring Clarity and Consistency of FDIC Policies and Alignment with Other Regulators

FDIC internal guidance to its personnel should be clearly defined and aligned, as appropriate, with other financial regulators. Without clear guidance, the FDIC cannot ensure that its personnel will consistently apply FDIC policies in a coherent, Agency-wide manner. Further, similarly-situated banks may be treated differently as FDIC guidance may be applied inconsistently or in conflict with guidance from other regulators.

In our OIG evaluation, *Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders* (BSA/AML) (December 2021), we found that the FDIC and the Federal Reserve Board used different guidance to assess whether to terminate BSA/AML Consent Orders. As a result, for one of our sampled Consent Orders, the FDIC and the Federal Reserve Board assessed similar facts about the bank and its holding company, but came to different conclusions regarding the timing for terminating their respective BSA/AML Consent Orders. The Federal Reserve Board maintained its Consent Order longer than the FDIC, while the FDIC terminated its Order and included uncorrected provisions in an informal enforcement action. The FDIC should align its termination criteria with other financial regulators, so that FDIC-supervised banks are treated similarly to other regulated banks.

We also found that FDIC guidance did not address how Regional Office personnel should apply key policy terms to determine whether to terminate a Consent Order. For 4 of 10 sampled Consent Order Terminations, FDIC guidance did not address how to apply the terms "substantial compliance" and "partially met." As a result, the FDIC could not be certain that these four Consent Orders were terminated using a consistent interpretation of these terms. The term, "partially met," provides extremely wide latitude to terminate a Consent Order when any portion of it is met. The FDIC should ensure consistent treatment of FDIC-supervised banks regardless of the bank's geographical location.

Further, Consent Order termination decisions were not centrally monitored. Monitoring decisions across Regional Offices would serve as an important internal control to identify the potential for inconsistent application of Consent Order termination guidance across Regional Offices. We made 10 recommendations to enhance the FDIC's guidance regarding termination of its Consent Orders, and related processes, monitoring, and documentation.

Enhancing FDIC Rulemaking

FDIC rulemaking should be a transparent process that analyzes the need for safety and soundness regulation and the compliance burden placed on banks. A foundational component of rulemaking is the FDIC's access to reliable information to measure a regulation's costs and benefits. Quantifying both the costs and benefits of significant financial regulations can be challenging, and it often may be imprecise and unreliable.[58] For example, performing such analysis can be difficult, because it involves theory, modeling, statistical analysis, and other tools to predict future outcomes based on certain assumptions.[59]

In our OIG review, *Cost Benefit Analysis Process for Rulemaking* (February 2020), we found that the FDIC had not established and documented a process to determine when and how to perform cost benefit analyses in its rulemaking process. In addition, the FDIC was not transparent in publishing (i) the reason(s) why a cost benefit analysis was or was not performed; (ii) the reason(s) for the depth of analysis performed; (iii) the analytical scope and methodology used; and (iv) the analysis performed. Without transparent cost benefit analyses, stakeholders such as financial institutions, the public, and Congress may not understand the FDIC's analyses and conclusions.

Also, we found that the FDIC did not perform cost benefit analyses after issuance of a final rule. Without performing cost benefit analyses of existing rules or establishing a formal process to proactively review each final rule, the FDIC may not identify duplicative, outdated, or overly burdensome rules in a timely manner. In addition, the FDIC may not ensure that its rules are effective and achieve their intended objectives/outcomes.

We made five recommendations in this report; however, none of them have been implemented since the report was issued in February 2020. The FDIC had originally designated an Expected Completion Date for four of these recommendations as June 30, 2021; however, the Agency has extended the time period for implementation of its corrective actions. FDIC staff indicated that the reason for the extension was to allow for the completion of the FDIC's review process for a draft directive and accompanying staff guidance on regulatory analysis.

Effective governance by the FDIC Board and executives ensures that the FDIC is prepared to meet its mission. The FDIC should clarify the protocols for submitting motions to the Board for consideration. Further, the FDIC's ERM program should assist the FDIC Board and Agency officials by identifying and assessing external and internal threats and risks in order to adjust relevant policies and controls. When such policies and controls are found to be weak, the FDIC should continue to take steps to correct these deficiencies in a timely manner and ensure that corrective actions remain effective. The FDIC should be clear about whether and to what extent it adopts Executive Branch policies. In addition, the FDIC should have clear internal policies and procedures to ensure consistent implementation of FDIC programs by its personnel. FDIC policies should be aligned with other regulators, as appropriate, to ensure consistent treatment of banks. The FDIC should also ensure that the process for rulemaking is transparent and that rules are based on sound cost benefit analysis.

IT Security at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge on IT Security are:

- Improving the FDIC's overall information security;
- Managing the security of mobile devices; and
- Improving security controls over the FDIC's critical building services.

The OIG has identified IT Security as a Top Challenge for the FDIC since 2018.

On December 6, 2021, the Office of Management and Budget (OMB) stated that "[t]he United States Government continues to face increasingly sophisticated efforts to compromise Federal IT systems, challenging current defenses and creating an urgent need to evolve to a new security paradigm."[60] In Fiscal Year 2020, OMB reported that Federal agencies had suffered 30,819 cybersecurity incidents, an 8 percent increase over the incidents in 2019.[61]

On November 4, 2021, the Cybersecurity & Infrastructure Security Agency (CISA) issued a Directive stating that the United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the American people's security and privacy.[62] The CISA Directive stated that the Federal Government must improve its efforts to protect against these campaigns as these vulnerabilities pose a significant risk to agencies and the Federal enterprise.

FDIC IT systems support day-to-day operations of the Agency and are critical to the Agency's mission. As of August 2021, the FDIC had 76 IT systems containing significant amounts of information about FDIC employees, supervised banks, and depositors. For example, the FDIC's Failed Bank Data System holds nearly 2,500 terabytes of sensitive information from over 500 bank failures. A cyber incident at the FDIC could severely limit its capabilities to meet mission requirements, particularly during a crisis. In addition, cyber incidents could compromise sensitive business information and Personally Identifiable Information.[63]

Improving the FDIC's Information Security

In our OIG audit, *The FDIC's Information Security Program–2021* (October 2021), we found that while the FDIC had established and strengthened some security controls from the prior year, there remained several security control weaknesses that limited the effectiveness of the FDIC's information security program and practices. These deficiencies placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. The highest risk security weaknesses noted in our report included:

- **High Number of Overdue and Unaddressed High- and Moderate-Risk Plans of Action and Milestones (POA&M).** POA&Ms are used to track the progress of corrective actions pertaining to security vulnerabilities. We found that as of July 2021, 176 high- and moderate-risk POA&Ms remained unremediated. Without consistently and timely addressing control deficiencies, the FDIC will continue to face an increasing backlog of POA&Ms, leaving its data more vulnerable to security exploits from unmitigated threats and reducing its overall security posture.

- **Ad-Hoc Supply Chain Risk Management Processes at the FDIC.** The FDIC has not defined processes and procedures that support the underlying components of its SCRM directive. Without these SCRM processes and procedures, the FDIC cannot be assured that it will accurately identify and monitor its supply chain risks.

- **Administrative Account Management Needs Improvement.** During 2021, we identified 11 additional open POA&Ms related to privileged user access. Weaknesses in the FDIC's processes for managing Administrative Accounts increased the risk of unauthorized activity, such as individuals accessing, modifying, deleting, or exfiltrating sensitive information.

- **Inadequate Oversight and Monitoring of FDIC Information Systems.** Federal agencies must ensure that entities operating information systems on behalf of the Federal Government meet the same security and privacy requirements as Federal agencies. Historically, several systems, components, and services that should have been assessed by the FDIC according to these requirements were instead subject to a now-rescinded assessment methodology. As a result, the FDIC did not subject these systems to a proper risk assessment, authorization to operate, or ongoing monitoring.

We made six recommendations to improve the IT security systems at the FDIC, in addition to five recommendations that remain from prior Financial Information Security Act (FISMA) reports (including one recommendation from our OIG report issued on November 2, 2016).

Managing the Security of Mobile Devices

The FDIC has issued approximately 4,700 smartphones and tablets to its employees and contractor personnel. While these mobile devices may enhance communications, they also introduce the risk of cyber threats, such as "malware" that can allow an actor to exploit vulnerabilities on the devices; eavesdrop wireless communications over public networks; and collect and monitor data on mobile applications installed by users, such as the user's location, contacts, and browsing history.

In our OIG report, *Security and Management of Mobile Devices* (August 2021), we found that the FDIC had not established or implemented effective controls and practices to secure and manage its mobile devices in three of nine areas assessed. FDIC policies, procedures, and guidance were outdated and did not reflect current business practices pertaining to mobile devices, and they did not address key elements promulgated by NIST. The FDIC policy on mobile devices was more than 18 years old—issued prior to the introduction of smartphones and tablets—and focused on obsolete technologies such as pagers.

The FDIC policies did not address its Bring Your Own Device program, nor the risks associated with personal use of FDIC-furnished mobile devices, such as non-work related applications, and texting, messaging, and video. We also found that FDIC employees and contractor personnel had downloaded non-work related applications, including dating services, shopping, sports entertainment, and movie streaming services. We made nine recommendations to strengthen the FDIC's management of mobile devices. As of the date of this Top Challenges Report, the FDIC aims to implement these recommendations by May 2022.

Improving Security Controls over Critical Building Services

The FDIC uses building automation systems to monitor and control critical services at its facilities, such as the supply of electrical power, HVAC (heating, ventilation, and air conditioning), and water services. In our OIG audit, *Security of Critical Building Services at FDIC-owned Facilities* (March 2021), we found that the FDIC security controls over three information systems were not effective to monitor, manage, and help ensure the uninterrupted delivery of critical building services. We identified weak account management practices, the use of unsupported vendor software, and a lack of security oversight and monitoring. Such ineffective controls and practices increased the risk of unauthorized access to these three systems, which could have led to a disruption of the systems, corruption of the systems' data, or other malicious activity. We made 10 recommendations to improve the security controls over three critical building systems at the FDIC and 4 recommendations remain outstanding.

In addition, we have ongoing work to review the adequacy and effectiveness of FDIC security controls over its wireless networks and its Windows Active Directory.

The FDIC is dependent upon IT systems for day-to-day activities—especially during a banking crisis. The FDIC should ensure that its IT security can withstand increasing risks to Federal systems. Strong IT security is paramount to ensure that the FDIC can fulfill its mission and protect the sensitive information of bank customers and employees, and FDIC personnel.

Security and Privacy at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge on Security and Privacy are:

- Improving the effectiveness of the FDIC's Personnel Security and Suitability processes;
- Implementing management of Physical Security based upon risk assessments;
- Sustaining a work environment free from discrimination, harassment, and retaliation; and
- Securing sensitive and Personally Identifiable Information.

The OIG has identified Security and Privacy as a Top Challenge for the FDIC since 2019.

The FDIC is responsible for the security and safety of approximately 5,800 employees and 1,600 contract personnel who work at 92 FDIC facilities throughout the country. The FDIC is also the custodian of 76 IT systems and a large volume of hard-copy records on premises and in archival storage.

Improving the Effectiveness of the FDIC's Personnel Security and Suitability Processes

An important step in mitigating risk to the FDIC is ensuring that employees and contractors undergo appropriate security and suitability screening. In March 2021, the GAO stated that "[a] high-quality personnel security clearance process minimizes the risks of unauthorized disclosures of classified information and helps ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed."[64]

The FDIC should be assured that its employees and contractors are properly screened and investigated before being granted access to systems and entrusted with sensitive, confidential, or, in some cases, classified information. In our OIG evaluation, *The FDIC's Personnel Security and Suitability Program* (PSSP) (January 2021), we concluded that the FDIC's PSSP program was not fully effective in ensuring the timely completion of preliminary suitability screenings, background investigations commensurate with position risk designations, and re-investigations. We found that four contractor employees with unfavorable background investigation adjudications continued to work at the FDIC for periods ranging from nearly 8 months to 5 years (until we notified the FDIC about these cases). Further, the FDIC did not remove seven contractor personnel with unfavorable adjudications in a timely manner, did not follow its Insider Threat protocols, and conducted limited risk assessments for contractors with unfavorable adjudications.

The FDIC also did not initiate numerous required periodic reinvestigations in a timely manner. In addition, data on contractor position risks were unreliable, employee background investigations were often not commensurate with position risk, FDIC personnel security files were frequently missing some preliminary background investigation data, and the FDIC was not meeting its goals for completing preliminary background investigations within a specified timeframe. The FDIC took urgent action to address our recommendations in this report. The FDIC should sustain controls over its personnel security programs as it hires employees and contractors.

Implementing Physical Security Based on Risks

The FDIC should ensure that its facilities have appropriate physical security controls in place to safeguard personnel. According to the Congressional Research Service, Federal facilities and employees, contractors, and visitors to such facilities "face a variety of threats, including illegal weapon and explosive possession, robbery, riots, civil disturbances, homicide, and arson."[65]

The FDIC maintains 92 leased or owned facilities across the country and is in the process of assessing facility needs as it transitions to a hybrid workplace. In our OIG evaluation, *The FDIC's Physical Security Risk Management Process* (April 2019), we concluded that the FDIC had not established an effective physical security risk management process to ensure that it met required standards and guidelines. We found that the FDIC frequently did not document its decisions regarding facility security risks and countermeasures, and such decisions were not guided by defined policies or procedures. Without documentation of these decisions, FDIC executives and oversight bodies were not able to fully consider and review the rationale for these determinations.

We also found that the FDIC did not conduct key activities in a timely or thorough manner for determining facility risk level, assessing security protections in the form of countermeasures, mitigating and accepting risk, and measuring program effectiveness. For example, for one of its medium-risk facilities, the FDIC began, but did not complete, an assessment more than 2½ years after the FDIC occupied the leased space. Collectively, these weaknesses limited the FDIC's assurance that it met Federal standards for physical security over its facilities. We made nine recommendations to address the weaknesses in the FDIC's physical security risk management process, and the FDIC has implemented them. The FDIC should continue to monitor its physical security program controls as threats change and as the FDIC reviews and modifies its space needs for buildings and facilities.

Sustaining a Work Environment Free from Discrimination, Harassment, and Retaliation

The FDIC Chair has stated that, "[t]he FDIC does not tolerate discrimination, harassment (including sexual harassment), or retaliation, and every allegation of these unlawful behaviors is taken seriously. FDIC managers and supervisors must address harassment allegations immediately and appropriately."[66] Sexual harassment negatively impacts workplace culture. It can undermine employee morale and can cause employee engagement and productivity to decline. According to a survey conducted by Deloitte (March 2019), 52 percent of women experienced some form of harassment within the last 5 years. Further, a report from Project Include (March 2021) found that 26 percent of respondents experienced an increase in gender-based harassment during the pandemic. On December 21, 2021, the Ranking Member of the Senate Committee on Banking, Housing and Urban Affairs noted that "federal employees at multiple agencies covered by the jurisdiction [of the Senate Banking Committee] have alleged experiencing harassment, discrimination, or other forms of abuse by agency officials in recent months."[67]

In our OIG evaluation, *Preventing and Addressing Sexual Harassment* (July 2020), we found that the FDIC had not developed a sexual harassment prevention program that fully aligned with the five core principles promoted by the Equal Employment Opportunity Commission. As part of our work, in April 2019, we conducted a survey of FDIC employees that indicated approximately 8 percent of FDIC respondents (191 of 2,376) had experienced sexual harassment at the FDIC during the period January 2015 to April 2019. This figure was similar to the results of a survey previously conducted by the Merit Systems Protection Board (MSPB) based on an earlier timeframe; the Government-wide average in this MSPB survey was 14 percent. Although 191 FDIC respondents reportedly experienced sexual harassment, the FDIC received only 12 reported sexual harassment allegations during the relevant timeframe.

Our survey further indicated that 38 percent of FDIC respondents who stated they had experienced sexual harassment said that they did not report the incident(s) for "fear of retaliation," and nearly 40 percent of FDIC respondents did not know, or were unsure, how to report allegations of sexual harassment. We recommended that the FDIC enhance its policies, procedures, and training to facilitate the reporting of sexual harassment allegations and address reported allegations in a prompt and effective manner. The FDIC has addressed the recommendations in this report. The FDIC should continue to ensure that it maintains an effective program to combat sexual harassment.

Securing Sensitive and Personally Identifiable Information

The FDIC should have effective processes to manage, monitor, and safeguard its information and ensure the safety and privacy of the records it keeps. FDIC information includes, for example, sensitive information about banks and Personally Identifiable Information (PII) and Social Security Numbers of employees, contractors, bank management, and bank deposit holders.

Recently, the GAO reviewed the handling of PII by five Federal financial regulators, including the FDIC.[68] With regard to the FDIC, the GAO found that the FDIC "did not establish agency-wide metrics to monitor privacy controls." Without such controls, PII held by the FDIC may be at increased risk of compromise.

In our OIG audit, *The FDIC's Privacy Program* (December 2019), we found that the FDIC had not established an effective privacy program to manage and monitor PII. The FDIC's controls and practices for its Privacy Program did not comply with four relevant privacy laws and/or OMB policy and guidance. Specifically, the FDIC did not:

- Fully integrate privacy considerations into its risk management framework designed to categorize information systems, establish system privacy plans, and select and continuously monitor system privacy controls;
- Adequately define the responsibilities of the Deputy Chief Privacy Officer or implement Records and Information Management Unit responsibilities for supporting the Privacy Program;
- Effectively manage or secure PII stored in network shared drives and in hard copy, or dispose of PII within established timeframes; and
- Ensure that Privacy Impact Assessments were always completed, monitored, and retired in a timely manner.

These deficiencies increased the risk of PII loss, theft, and unauthorized access or disclosure, which could lead to identity theft or other forms of consumer fraud against individuals. We made 14 recommendations designed to enhance the effectiveness of the FDIC's Privacy Program and practices.

As of the date of this Top Challenges Report, actions to remediate three recommendations remain unimplemented since the issuance of our report in December 2019, including those related to:

- Developing and approving privacy plans for all information systems;
- Updating policies and procedures for the current organizational structure of the Privacy Program; and
- Developing and implementing controls to ensure that PII is stored in networks and hard copy in accordance with laws, regulations, policies, and guidelines.

Further, in our OIG audit, *The FDIC's Information Security Program – 2019* (October 2019), we found that the FDIC had not adequately controlled access to sensitive information and PII stored in hard copy. For example, we identified instances in which sensitive information stored on internal network shared drives was not restricted to authorized users. We also conducted walk-throughs of selected FDIC facilities and found significant quantities of sensitive hard-copy information stored in unlocked filing cabinets and boxes in building hallways. We recommended that employees and contractor personnel properly safeguard sensitive electronic and hardcopy information.

The security and safety of FDIC personnel, facilities, and information is critical to its mission and operations. The FDIC can continue to enhance protection in these areas through improvements to its programs to assess personnel suitability, safeguard facilities, mitigate workplace sexual harassment, and ensure the security and privacy of information held in custody by the FDIC.

The FDIC's Collection, Analysis, and Use of Data

Key Areas of Concern

The primary areas of concern for this Challenge on Collection, Analysis, and Use of Data are:

- Establishing processes to share threat information;
- Ensuring reliable data for FDIC decision-making; and
- Managing the financial and economic impact of the pandemic.

The OIG has identified Sharing of Threat Information as a Top Challenge for the FDIC since 2018.

The U.S. Government collects and gathers significant volumes of data and information on threats facing the financial and banking sectors. This threat data and information from across the Federal Government may assist the FDIC in its mission to examine and inform banks, implement supervisory strategies, make policy determinations, allocate resources, and ensure U.S. financial stability.

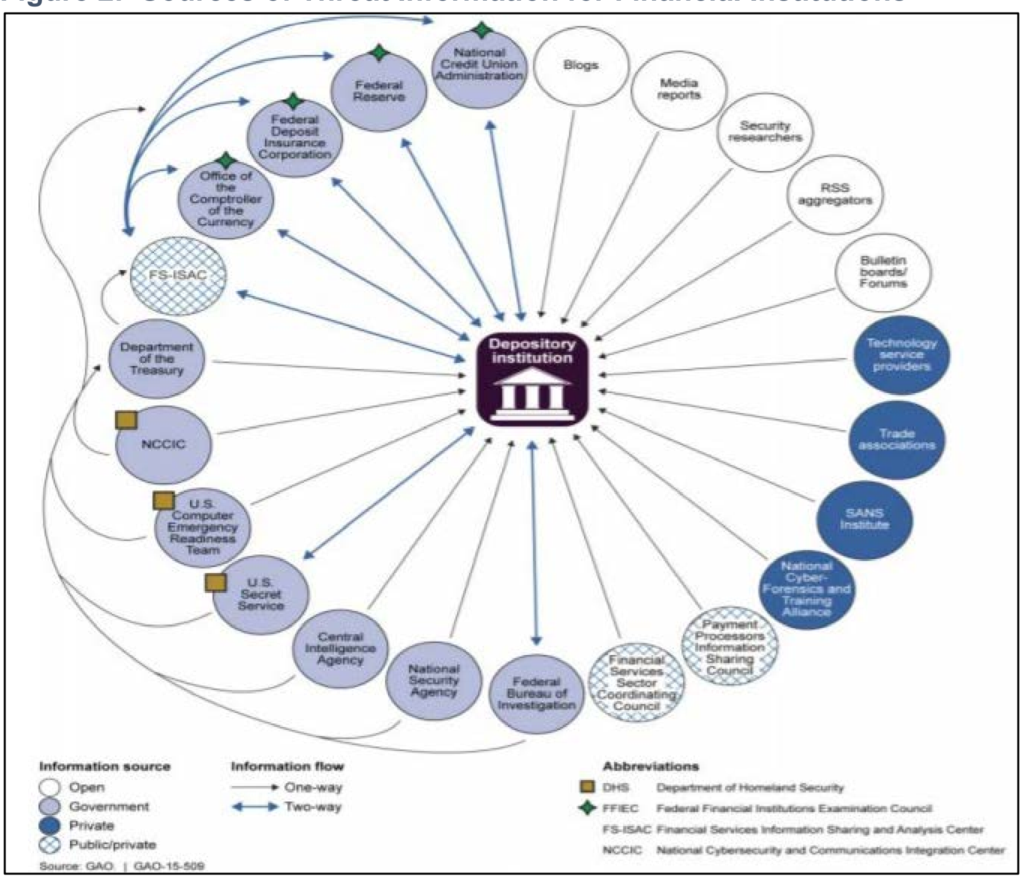
The [FSOC 2021 Annual Report] recognized the critical importance of sharing threat information with the Financial Services Sector and among Federal Government agencies. The OCC also encouraged monitoring of information provided by law enforcement and international organizations regarding "how criminals adapt scams and money-laundering techniques to exploit new vulnerabilities created by the pandemic."[69]

In addition, data can help Federal agencies, such as the FDIC, understand and improve program performance.[70] Through data-driven decision-making, regulators can use data to inform their decision-making processes and validate a course of action.[71] Data can also be used as an input for modeling and to identify trends. Such modeling can allow Government agencies to prevent problems rather than react to them.[72] For the FDIC, such models may allow the FDIC to forecast financial risks to the banking sector and adjust supervisory strategies, staffing, and budgeting accordingly.

Establishing Processes to Share Threat Information

As shown in Figure 2, the GAO recognized that numerous Federal Government agencies hold information relevant to banks

Figure 2: Sources of Threat Information for Financial Institutions



and the banking sector. In Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), the Administration encouraged reducing barriers to sharing threat information, specifically among Federal agencies and service providers.

The FDIC, along with its Government partners, collects and queries threat information contained within U.S. Government databases and repositories. The FDIC should acquire, analyze, and disseminate threat information to inform senior FDIC officials and decision-makers, FDIC examiners and Regional personnel, its supervisory program officials, and banks.[73]

In our OIG audit, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (January 2022), we found that the FDIC did not establish effective processes to govern its sharing of threat information. Specifically, the FDIC did not establish appropriate governance through a written governance structure and complete, approve, and implement a governance Charter to establish a common understanding of the role for its Threat Information Sharing program or define an overall strategy and requirements for it.

Further, the FDIC did not develop goals, objectives, or measures to guide the performance of its Intelligence Support Program. The FDIC also did not establish adequate policies and procedures to define roles and responsibilities for key stakeholders involved in the threat information-sharing program and activities or fully consider program risks in its ERM process.

We also identified gaps in each of the four component functions of Threat Information Sharing:

- **Acquisition.** The FDIC did not develop written procedures for determining its threat information requirements. As a result, the FDIC has limited assurance that it will acquire all relevant threat information to support its business operations and programs.

- **Analysis.** The FDIC did not establish procedures to guide its analysis of threat information. Absent such procedures, the FDIC relied solely on the discretionary judgment of certain individuals to determine the extent to which threat information should be analyzed to support FDIC business needs and the supervision of financial institutions.

- **Dissemination.** The FDIC did not develop procedures for disseminating threat information. Absent such procedures, decisions regarding what to disseminate, to whom, and when, are left solely to the discretion of individuals, which could lead to inconsistent or untimely communications. The FDIC had not established an infrastructure that would allow for secure handling of sensitive information, including transmission, storage, and disposition of such information.

- **Feedback.** The FDIC did not establish a procedure to obtain feedback from recipients of threat information to assess its utility and effectiveness. Such structured feedback could provide valuable information regarding the extent to which such threat information is timely and actionable, and FDIC personnel use threat information.

We also found numerous gaps in the FDIC's management of threat information sharing, including: Not having backup personnel for its Senior Intelligence Officer (SIO) or plans for an absence or departure; Not establishing minimum training requirements for the SIO position; Not obtaining required security clearance for certain senior FDIC officials; and Not properly categorizing unclassified threat information.

We made 25 recommendations to the FDIC to improve its processes for sharing threat information. We have additional work planned to assess the FDIC's sharing of threat information with its supervised banks and the banking sector.

Ensuring Reliable Data for FDIC Decision-Making

Data is a key input into the FDIC's decision-making processes. The FDIC Board and senior FDIC officials utilize various data sets to assess program performance, whether FDIC programs are meeting established goals, or whether goals or data collection should be modified. Incorrect, incomplete, and otherwise faulty data can lead to ineffective decision-making especially when data is the basis for policy determinations. Therefore, it is critical that the FDIC support and maintain the integrity of its data systems.

We found deficiencies in data reliability, collection, and analysis in a number of recent OIG reviews, for example:

- **Errors in Examination Completion and Mailing Dates.** In our OIG evaluation, *Reliability of Data in the FDIC Virtual Supervisory Information on the Net System* (ViSION System) (November 2021), we found that the FDIC's risk assessment used for the ViSION system data had not been reassessed or updated in over a decade, since 2009. Also, we found that of the four key data elements we tested in the FDIC's ViSION system, two were reliable and two were not reliable.[74] The unreliable data included recorded dates for the completion of bank examinations and mailing of bank examination reports. Errors in either date increase the risk of inaccurate reporting of examination performance metrics to FDIC management and the public. We made six recommendations to the FDIC to improve ViSION data reliability.

- **Exclusion of Data for Government Reporting.** In our OIG audit, *FDIC's Compliance under the Digital Accountability and Transparency Act of 2014* (November 2021), we found that the FDIC's submission of financial and award data excluded information for the Federal Savings and Loan Insurance Corporation Resolution Fund (FRF) and the Resolution Trust Corporation (RTC). As a result, obligation and outlay amounts for the FRF and RTC were not available for display on the Government website, USASpending.gov. We made three recommendations to clarify FDIC data reporting.

- **Unreliable Background Investigation Data.** We found FDIC data on employee and contractor background investigations was often not reliable. In our OIG evaluation, *The FDIC's Personnel Security and Suitability Program* (January 2021), we found that contractor position risk levels recorded in FDIC systems were unreliable. As a result, the FDIC could not determine whether these contractors received background investigations commensurate with their positions. We also found that FDIC systems were missing data for employee and contractor preliminary background investigation completion dates.

- **Incorrect BSA Reporting to the Board and other Agencies.** In our OIG evaluation, *Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders* (December 2021), we found that the FDIC did not consistently track Consent Order termination data in its system of record. As a result, the FDIC provided nine incorrect reports to the FDIC Board of Directors concerning enforcement actions; and did not report three BSA/AML Consent Order terminations in a quarterly report to the Financial Crimes Enforcement Network (FinCEN) in the Department of the Treasury.

- **Analysis of Collected Data:** In our OIG memorandum, *The FDIC's Management of Employee Talent* (September 2021), we found that the FDIC did not have a process for collecting and analyzing the various types of data that can be used to assess employee retention across the Agency as part of its talent management strategy. Specifically, the FDIC did not have a systematic process to holistically capture and analyze data, and to ensure that the information flowed to the Divisions and Offices. Such a process would help the FDIC develop a coherent strategy for managing retention activities throughout the Agency, provide an Agency-wide view of the progression and movements of the FDIC workforce, and provide helpful insights on employees' decisions to stay or separate.

Timely and reliable information assists the FDIC in mitigating risks and supports data-driven and transparent decision-making. In addition, threat information from across the Federal Government may assist in examining and informing banks, implementing supervisory approaches, making policy determinations, allocating resources, and ensuring the stability of the financial system. In addition, reliable and accurate program data allows the FDIC Board and senior management to measure and assess the effectiveness of FDIC programs and to support decision-making.

Contracting and Supply Chain Management at the FDIC

Key Areas of Concern

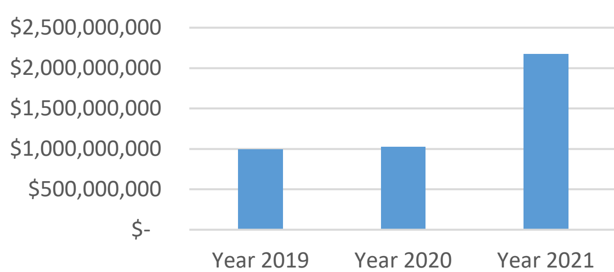
The primary areas of concern for this Challenge on Contracting and Supply Chain Management are:

- Improving the FDIC's contract management process;
- Managing risks associated with the FDIC's supply chain; and
- Ensuring whistleblower rights and protection notices for contractor personnel.

The OIG has identified Contracting as a Top Challenge for the FDIC since 2018.

According to the FDIC's November 2021 Awards Summary Report, the FDIC issued 483 contract actions for total award amounts of over $2 billion. As shown in Figure 3, FDIC contract award amounts doubled in 2021 when compared to 2020 ($1.025 billion) and 2019 ($994 million).

Figure 3: FDIC Contracts Total Award Amounts



Source: FDIC Awards Summary Report (November 2021)

The FDIC should have strong oversight of its contracts. Contract oversight includes activities such as monitoring and validating invoices prior to payment, approving contract deliverables for goods and services, monitoring contractor activities against contractual timelines, and ensuring contractors comply with required security and confidentiality requirements.

Improving the FDIC's Contract Management Process

In the most recent audit of the FDIC's financial statements in 2021, the GAO identified 10 deficiencies "related to contract-payment review processes that collectively represent a significant deficiency in FDIC's internal control over financial reporting." In addition, the GAO noted five deficiencies in the 2020 financial statement report. The GAO concluded that the "FDIC cannot reasonably assure internal controls over contract payments are operating effectively, which increases the risks of improper payments and financial statement misstatements."[75]

We have also conducted a number of reviews that found weaknesses in FDIC contract oversight management. In our OIG evaluation, *Contract Oversight Management* (October 2019), we concluded that the FDIC needed to strengthen its contract oversight management, particularly in terms of its information system and contract documentation. We determined that the FDIC's contracting management information system had limited data and reporting capabilities for Agency-wide oversight of its contract portfolio. We found that the FDIC was overseeing acquisitions on a contract-by-contract basis rather than on a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency.

As a result, FDIC Board Members and other senior management officials were not provided with a portfolio-wide view or the ability to analyze historical contracting trends across the portfolio, identify anomalies, and perform ad hoc analyses to identify risk or plan for future acquisitions. Therefore, we recommended that the FDIC provide enhanced contract portfolio reports to FDIC executives, senior management, and the Board of Directors. This recommendation remains unimplemented since the issuance of our report in October 2019. The FDIC had originally designated an Expected Completion Date for this recommendation as December 31, 2020.

Further, in our OIG evaluation, *Critical Functions in FDIC Contracts* (March 2021), we reviewed two existing FDIC contracts with Blue Canopy Group, LLC, which performed services in support of the FDIC's information security and privacy program. FDIC contracts with Blue Canopy amounted to approximately 38.3 percent ($16.2 million) of the FDIC's annual operating expenses for Information Security ($42.3 million) in 2019. We had previously found that "the FDIC hired [Blue Canopy] to assess certain security controls . . . for which the FDIC had also assigned the firm duties related to design and/or execution . . . . [T]his arrangement limited the firm's independence and *impaired the firm's ability to conduct impartial security control assessments*."[76] [Emphasis added.]

We found that the FDIC did not have policies and procedures to identify Critical Functions at the Agency, nor did it implement any heightened contract monitoring activities for Critical Functions. Therefore, the FDIC did not identify services provided by Blue Canopy as Critical Functions. As a result, the FDIC cannot be assured that it will provide sufficient management oversight of contractors performing Critical Functions or supervision to ensure that the Agency does not lose control of its mission or operations. We made 13 recommendations to strengthen the FDIC's identification and monitoring of contracts involving Critical Functions. As of the date of this Top Challenges Report, 12 recommendations remain unimplemented. Further, 5 of these 12 recommendations are unresolved, meaning FDIC management did not propose acceptable corrective actions for these recommendations.

Establishing an Effective Supply Chain Risk Management Program

According to NIST, there are inherent risks associated with an agency's supply chain for contracted goods and services.[77] According to the GAO, supply chain risks include, for example:

- **Installation of hardware or software containing malicious logic** causing significant damage by allowing attackers to take control of entire systems and read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations' systems; or destroy systems.

- **Installation of counterfeit hardware or software** threatening the integrity, trustworthiness, and reliability of information systems because they fail more often and more quickly, and provide an opportunity to insert a back door to give an intruder remote access.

- **Failure or disruption in the production or distribution of critical products**, including manmade and natural disruptions of the supply of IT products critical to Federal agencies.

- **Reliance on a malicious or unqualified service provider** that can use its access to systems and data to gain access to information, commit fraud, disrupt operations, or launch attacks against other computers or networks.

- **Installation of hardware or software that contains unintentional vulnerabilities** such that defects in code or misconfigurations can be exploited to gain access to information systems and data and disrupt service.[78]

Organizations may have reduced visibility, understanding, and control of these risks when their vendors rely on second- and third-tier suppliers and service providers. The European Union Agency for Cybersecurity reported that hackers often focus on an entity's vendor systems for supply chain attacks and predicted that supply chain cyberattacks would quadruple in 2021.[79]

In our report, *The FDIC's Information Security Program–2021* (October 2021), the FDIC's SCRM operated at a Level 1 (Ad Hoc). We found that the FDIC's SCRM Program is still in its initial phase, and procedures that support the underlying components have not yet been defined in accordance with FISMA requirements. Specifically, the FDIC did not have procedures that defined:

- How to implement its SCRM policy or strategy and associated baseline SCRM controls;
- Obtaining assurance over external service providers' compliance with the FDIC's cybersecurity requirements, including:
    - How to identify and prioritize externally provided systems, components, and services;
    - The organizational requirements for cybersecurity and SCRM for externally provided systems, system components, and services;
    - The tools or methods used to validate that SCRM requirements are being met;
    - The risk-based processes for evaluating SCRM risks associated with suppliers;
    - How awareness is maintained over risks stemming from upstream suppliers through monitoring activities; and
    - The integration of its acquisition process and the use of contractual stipulations detailing appropriate SCRM measures for external providers.
- Management of counterfeit components, including:
    - How to detect and prevent counterfeit components;
    - How to maintain configuration control over components being repaired or serviced; and
    - The process for reporting counterfeit components.

Because the FDIC is a financial regulator and holds sensitive and nonpublic information, it is a potential target of adversaries seeking to interfere with its regulatory activities or obtain information for their own advantage. Ad hoc SCRM processes limit the FDIC's ability to identify vulnerabilities throughout its supply chain consistently, and to manage and monitor associated risks effectively.

Ensuring Whistleblower Rights and Protection Notices for Contractor Personnel

FDIC contracts should contain a provision notifying contractors that they must provide their employees with information regarding the rights and protections for whistleblowers.[80]

In our OIG evaluation, *Whistleblower Rights and Protections for FDIC Contractors* (January 2022), we found that the FDIC had not aligned its procedures and processes with laws, regulations, and policies designed to ensure notice to contractor and subcontractor employees about their whistleblower rights and protections. The FDIC also did not always comply with the whistleblower rights notification requirements it established. Specifically, the FDIC did not incorporate the Whistleblower Rights Notification Clause into three of the nine contracts that we tested. Further, the FDIC's Legal Division did not adopt any whistleblower rights notification provisions for contractors or include any whistleblower clauses in its contracts. The FDIC also did not verify that contractors and subcontractors notified employees of their whistleblower rights and protections.

Without clear guidance and direction on where and to whom to report a violation of any law, rule, or regulation; gross mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to public health and safety, FDIC contractors may not take the initiative to report such allegations. The FDIC should make it clear in its contracts that contractors must notify their employees that such whistleblower allegations may be reported to the FDIC OIG Hotline. We made nine recommendations to improve the FDIC's compliance with legal requirements, including required contract clauses regarding contractor obligations to notify employees of whistleblower disclosure rights and protections.

Contracting is an important function at the FDIC. The FDIC should prioritize improving its oversight to ensure proper contract monitoring, especially for Critical Functions. The FDIC should also mitigate supply chain risk by establishing a robust SCRM strategy that allows the Agency to assess, evaluate, monitor, and mitigate supply chain risk. The FDIC must also ensure that it has processes in place to advise contractors and subcontractors of their whistleblower rights and protections.

Human Resources at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge on Human Resources are:
- Optimizing talent management throughout the Agency;
- Managing a wave of potential employee retirements at the FDIC; and
- Ensuring diversity and inclusion within the FDIC workforce.

The OIG has identified Human Resources as a Top Challenge at the FDIC since 2019, particularly with respect to potential retirements among FDIC personnel.

In March 2021, the GAO continued to recognize strategic human capital management as a Government-wide area of high risk.[81] The GAO identified the need for Federal agencies to measure and address existing mission-critical skill gaps. A lack of strategic workforce planning may have lasting effects on the capacity of an agency's workforce and its ability to fulfill its mission.

Workforce planning is especially important as the FDIC shifts towards a hybrid work model that includes the potential for a significant increase in employees working remotely. On January 4, 2022, the FDIC reached agreement with the National Treasury Employees Union on new policies to support a hybrid work environment and expanded telework opportunities. New and enhanced skillsets may be required for this transition. According to the Society of Human Resource Management, employee traits such as adaptability, resiliency, self-motivation, communication and collaboration have become critical for successful remote work.[82]

Optimizing Talent Management Throughout the FDIC

As part of an agency's talent management, the Office of Personnel Management (OPM) recommends retention strategies as a way to create an environment where employees understand and are committed to the mission of the organization and empowered to make a difference.[83] The term, "talent management," encompasses attracting and retaining talent for improving organizational performance, while also considering attrition.[84] Talent management also seeks to address competency gaps, by implementing and maintaining programs to attract, develop, promote, and retain talent, particularly for mission-critical positions and occupations.

In our OIG memorandum, *The FDIC's Management of Employee Talent* (September 2021), we identified concerns with the FDIC's management of its employee retention. Specifically, we found that the FDIC:

- **Did not have clear goals to manage employee retention.** The FDIC had strategic plans in place in March 2021 related to its management of employee retention. However, two of the three FDIC talent retention goals were not objective, quantifiable, and measurable. As a result, the FDIC could not assess its progress towards these goals.

- **Did not have a systematic process for collecting and analyzing employee retention data.** The FDIC did not have a systematic process to holistically capture and analyze data, and to ensure that the information flowed to the Divisions and Offices. Such a process would help the FDIC develop a coherent strategy for managing retention activities throughout the Agency, provide an Agency-wide view of the progression and movements of the FDIC workforce, and provide helpful insights on employees' decisions to stay or separate.

- **Did not establish metrics or indicators to measure the effectiveness of its retention activities or actions.** Instead, the FDIC tracked its "inputs" – that is, the implementation status of the activities or actions designed to meet its employee retention goals. Thus, the FDIC could not determine whether or not its retention activities were working effectively.

We made three recommendations to improve the FDIC's management of talent at the Agency.

Managing a Wave of Potential Retirements at the FDIC

The FDIC faces a wave of potential retirements among its workforce in the coming years. As shown in the Table more than 25 percent (1,536 individuals) of the FDIC workforce is currently eligible to retire. This figure climbs to nearly 40 percent (2,356 individuals) within 5 years by 2026. The FDIC's retirement-eligibility rates are higher than the 15-percent eligibility rate last reported for the entire Federal Government.[85]

The FDIC faces significant risks regarding retirement eligibility in key Divisions involved in crises readiness efforts. As noted in the Table, more than a third of the employees in four key FDIC Divisions are currently eligible to retire – that is, the Division of Resolutions and Receiverships, Division of Finance, Division of Administration, and Legal Division. Absent seasoned professionals from these Divisions with knowledge of lessons learned from past crises, the FDIC may not be sufficiently agile in executing resolution and receivership activities in future crises. Also, all FDIC Divisions have more than 18 percent of their workforce who are currently eligible to retire.

Table: FDIC Employee Retirement Eligibility

Division		2022	2023	2024	2025	2026
DOF		45.2	47.4	52.6	55.6	55.6
DRR		42.7	48.6	53.3	57	59.5
LEGAL		41.7	43.8	46.7	48.9	51.6
DOA		34.1	39.1	42.5	45.93	49
RMS		21.6	25.1	29	32.5	35
DIT		21.5	25.5	28.5	31.2	34.9
CISR		18.8	24.7	28	32.8	36
DIR		18.6	20.5	24.7	27.4	28.8
DCP		18.3	21.1	24.4	27.7	31.1
Overall for FDIC		25.3	29	32.6	35.9	38.8

Source: OIG analysis of FDIC-provided retirement eligibility as of July 2021.

In addition, more than 36 percent of the Executives and Managers at the FDIC are eligible to retire currently. These rates climb for FDIC Executives and Managers to nearly 60 percent by 2026. Such retirements may result in gaps in leadership positions. Leadership gaps can cause delayed decision-making, reduced program oversight, and failure to achieve Agency goals.

Ensuring Diversity and Inclusion Within the FDIC Workforce

On June 25, 2021, the President issued Executive Order 14305 on "Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce." This Executive Order charged Federal agencies with assessing the current state of diversity, equity, inclusion, and accessibility within their workforces and developing strategic plans to eliminate barriers faced by underserved employees.[86] The FDIC Chair has stated that "[p]romoting diversity at all levels of the FDIC's workforce continues to be a key challenge for the agency, especially the ability to attract, retain, and advance minorities and women in our bank examiner workforce."[87]

In June 2021, the FDIC reported that 68.5 percent of all FDIC employees were White, 16.9 percent were Black/African American, 4.5 percent were Hispanic, 7.5 percent were Asian/Pacific Islander, 0.6 percent were American Indian/Alaska Native, and 2 percent were two or more races.[88] By comparison, at the end of 2020, 61.5 percent of the Federal workforce was White, 18.4 percent were Black, 9.4 percent were Hispanic, 6.9 percent were Asian/Pacific Islanders, 1.6 percent were Native American/Alaskan Native, and 1.9 percent were more than one race.[89] The FDIC's 2021-23 Diversity, Equity, and Inclusion Strategic Plan includes prioritized actions to continue to promote FDIC workforce diversity.

The FDIC is driven by its human resources. The FDIC must continue to focus on managing its human capital lifecycle—hiring, talent management, and retirements—under its new hybrid operating structure, including promoting diversity and inclusion throughout the FDIC workforce. Without diverse, dedicated, and trained staff, it risks falling short of achieving its goals.

---

[1] IMF, *United States Financial System Stability Assessment* (August 2020); U.S. Government Accountability Office, *Financial Stability: Agencies Have Not Found Leveraged Lending to Significantly Threaten Stability but Remain Cautious Amid Pandemic* (GAO-21-167) (December 2020).
[2] The Dodd-Frank Wall Street Reform and Consumer Protection Act created CIGFO to provide oversight of the Financial Stability Oversight Council. CIGFO is chaired by the Inspector General of the Department of the Treasury and includes nine additional Inspectors General, including the Inspector General of the FDIC.
[3] Federal Reserve Bank of New York Staff Report, *Climate Stress Testing* (September 2021); Financial Stability Oversight Council, *Report on Climate-Related Financial Risk* (October 21, 2021).
[4] CNBC, These are the world's largest banks that are increasing and decreasing their fossil fuel financing (April 22, 2021).
[5] Federal Reserve Bank of New York Staff Report, *Climate Stress Testing* (September 2021); Financial Stability Oversight Council, *Report on Climate-Related Financial Risk* (October 21, 2021); FSOC, *2021 Annual Report*.
[6] OCC Bulletin 2021-62, *Principles for Climate-Related Financial Risk Management for Large Banks* (December 16, 2021).
[7] Federal Reserve Bank of New York Staff Report, *Climate Stress Testing* (September 2021); Financial Stability Oversight Council, *Report on Climate-Related Financial Risk* (October 21, 2021).
[8] Statement by FDIC Chairman at the Financial Stability Oversight Council Meeting (October 21, 2021).
[9] Federal Reserve Press Release, Federal Reserve Board announces it has formally joined the Network of Central Banks and Supervisors for Greening the Financial System, or NGFS, as a member (December 15, 2020); American Banker, *Will FDIC, OCC follow Fed into global climate group?* (May 18, 2021).
[10] Environmental Protection Agency Press Release, *EPA Report Shows Disproportionate Impacts of Climate Change*

on Socially Vulnerable Populations in the United States (September 2, 2021).
[11] SBA, Paycheck Protection Program Report, Approvals through May 31, 2021.
[12] McCombs School of Business, University of Texas at Austin, *Did FinTech Lenders Facilitate PPP Fraud?* (December 6, 2021).
[13] Department of Justice, *Justice Department Takes Action Against COVID-19 Fraud* (March 25, 2021).
[14] FDIC Regional Directors Memorandum 2020-022, *Examination Considerations Related to the Paycheck Protection Program* (June 22, 2020).
[15] CBS News, *Jerome Powell Full 60 Minutes Interview transcript* (April 2021).
[16] OCC, *Semiannual Risk Perspective* (Fall 2021); Board of Governors of the Federal Reserve System, *Financial Stability Report* (November 2021).
[17] Board of Governors of the Federal Reserve System, *Financial Stability Report* (November 2021).
[18] American Banker, *Log4j Security Vulnerability Is a Double Threat to Banks* (December 23, 2021).
[19] Boston Consulting Group, *Global Wealth 2019: Reigniting Radical Growth* (June 2019).
[20] Constella Intelligence, *Financial Services Sector Exposure Report: 2018-2021 Findings and Trends*.
[21] American Banker, *Bankers Must Confront Security Risk of Remote Work* (December 22, 2021).
[22] American Banker, *'It's Very Scary': Small Banks Quietly Hit By Ransomware Attacks* (May 24, 2021).
[23] American Banker, *Ransomware Group Attacks A New Jersey Bank—Then Shuts Down* (June 16, 2021).
[24] The InTREx work program includes examination procedures used to determine the Uniform Rating System for Information Technology. The procedures also assess compliance with Appendix B to Part 364 of the *FDIC Rules and Regulations* entitled *Interagency Guidelines Establishing Information Security Standards* and cybersecurity preparedness.
[25] Notice of Proposed Rulemaking, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers*, 86 Fed. Reg. 2299 (January 12, 2021).
[26] *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 223 (November 23, 2021).
[27] These digital assets are not insured by the FDIC. According to the National Institute of Standards and Technology (NIST), distributed ledgers, such as blockchains, are tamper-resistant digital records of transactions that, once established, cannot be changed. NIST Internal Report 8202, *Blockchain Technology Overview* (October 2018).
[28] Bloomberg, *Crypto Market Retakes $2 Trillion Market Cap Amid Bitcoin Gains* (August 15, 2021).
[29] Basel Committee on Banking Supervision, *Discussion Paper: Designing a Prudential Treatment for Crypto-assets* (May 2021).
[30] Basel Committee on Banking Supervision, *Discussion Paper: Designing a Prudential Treatment for Crypto-assets* (May 2021).
[31] Bloomberg, *Yellen Says U.S. Lacks Adequate Regulatory Framework for Crypto* (May 4, 2021).
[32] Remarks of FDIC Chairman at Money 20/20 Conference (October 27, 2021).
[33] Time, *Fed Chairman Says U.S. Might Need More Crypto Regulations, Here's What That Means for Investors* (August 12, 2021).
[34] President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins* (November 2021).
[35] American Banker, *PNC Chief Executive Warns of Threat from Stablecoins* (October 15, 2021).
[36] Financial Institution Letter 75-2021, *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps* (November 23, 2021).
[37] The World Bank, *Financial Inclusion.*
[38] FDIC Chairman, Remarks at *Fintech: A Bridge to Economic Inclusion Conference* (June 29, 2021).
[39] FDIC Chairman, Remarks at *Fintech: A Bridge to Economic Inclusion Conference* (June 29, 2021).
[40] Environmental Protection Agency Press Release, *EPA Report Shows Disproportionate Impacts of Climate Change on Socially Vulnerable Populations in the United States* (September 2, 2021).
[41] Cleveland Federal Reserve, *The CRA Is Important for Underserved Communities, and Your Input Can Help Modernize It* (November 16, 2020).
[42] Message from FDIC Chair, *New Office and Continued Focus on Minority Depository Institutions and Other Mission-Driven Banks* (November 2, 2021).
[43] World Economic Forum, *Transforming Paradigms A Global AI in Financial Services Survey* (January 2020).
[44] American Banker, *Banks Warming to AI-based Lending* (October 21, 2019).
[45] Brookings Institution, *Reducing Bias in AI-based Financial Services* (July 10, 2020).
[46] Federal Reserve Bank of San Francisco, *Community Development Innovation Review, Regulation to Build a More Inclusive Financial System and Drive Financial Health* (August 19, 2021).
[47] Brookings Institution, *Reducing Bias in AI-based Financial Services* (July 10, 2020).
[48] Forbes, *The AI-Bias Problem And How FIntechs Should Be fighting It: A Deep Dive With Sam Farao* (September 29, 2021), *citing*, University of California at Berkley, *Consumer-Lending Discrimination in the FinTech Era* (November 2019).
[49] Deloitte, *Developing an effective governance operating model – A guide for financial services boards and management teams*.
[50] Organization for Economic Co-operation and Development (OECD), *G20/OECD Principles of Corporate Governance* (2015).

[51] See FDIC Statement on CFPB Statement; the Joint Statement of the CFPB Director and FDIC Director (stating that in light of extensive consolidation in the banking industry over the last 30 years, "the effectiveness of the regulatory framework in meeting the requirements of the Bank Merger Act is critical to the future safety and soundness, financial stability, community accountability, and competitiveness of the banking system."), and Statement of Acting Comptroller of the Currency.

[52] On December 17, 2021, the Department of Justice, Antitrust Division, issued a request for public comments on its guidelines regarding bank mergers.

[53] OMB Office of Federal Procurement Policy, Policy Letter 11–01, *Performance of Inherently Governmental and Critical Functions* (September 2011).

[54] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016).

[55] NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A Systems Lifecycle Approach for Security and Privacy* (December 2018).

[56] *The FDIC's Information Security Program – 2021*; *The FDIC's Information Security Program – 2020*; *The FDIC's Information Security Program – 2019*; *The FDIC's Information Security Program – 2018*.

[57] Prior to March 2017, the FDIC closed recommendations without OIG review of the corrective actions. As of March 2017, the OIG now reviews all corrective actions to determine whether the FDIC's actions satisfy the recommendation and therefore can be considered closed.

[58] Yale Law Journal Forum, *Cost-Benefit Analysis of Financial Regulation: A Reply* (January 22, 2015).

[59] Congressional Research Service, *Cost-Benefit Analysis and Financial Regulator Rulemaking* (April 12, 2017).

[60] OMB, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021).

[61] OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress* (Fiscal Year 2020). For example, in November 2021, a hacker gained access to an FBI email system and sent more than 100,000 emails. FBI Press Release, *FBI Statement on Incident Involving Fake Emails* (November 13, 2021).

[62] CISA Binding Operational Directive Advisory 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (November 3, 2021).

[63] For example, in April 2021, threat actors gained access to five Federal agencies through remote connection software service provider, Ivanti. The FDIC used an Ivanti product known as Pulse Secure and took action to remediate the vulnerability. In December 2020, Federal networks were compromised by a software update from IT management services company SolarWinds. FDIC uses a SolarWinds product and FDIC officials represented that they disconnected its use. Also in December 2020, nation state actors exploited a vulnerability in VMware products that allowed attackers to forge security credentials and gain access to protected date. The FDIC uses a VMware product and FDIC officials represented that they took action to apply the patch and reduce the risk of exploitation.

[64] GAO, *High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-risk Areas*, (GAO-21-119SP) (March 2021).

[65] Congressional Research Service, *Federal Building and Facility Security: Frequently Asked Questions* (January 27, 2021).

[66] FDIC, *Equal Employment Opportunity Policy Statement* (October 29, 2020).

[67] United States Senate Committee on Banking, Housing, and Urban Affairs Minority Press Release, *Toomey Encourages Federal Employees to Report Allegations of Misconduct* (December 20,2021).

[68] GAO, *Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information* (GAO-22-104551) (January 2022).

[69] OCC, *Semiannual Risk Report* (Fall 2021).

[70] GAO, *Issue Summary: Using Data and Evidence to Improve Federal Programs*.

[71] Harvard Business School, *The Advantages of Data-Driven Decision Making* (August 26, 2019).

[72] Deloitte, *Anticipatory Government, Preempting Problems Through Predictive Analytics* (June 24, 2019).

[73] The Department of Homeland Security (DHS) defines the term, "threat," as "a natural or human-created occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property." See DHS Risk Lexicon Terms and Definitions, 2017 Edition – Revision 2 (October 2017).

[74] The ViSION system is an FDIC mission-essential system that supports the FDIC's supervision and insurance responsibilities and provides users with access to financial, examination, and supervisory information on financial institutions.

[75] GAO, *Management Report: Improvements Needed in FDIC's Internal Control over Contract-Payment Review Processes* (GAO-21-420R) (May 13, 2021).

[76] FDIC OIG, *Security Configuration Management of the Windows Server Operating System* (January 2019).

[77] NIST, Special Publication 800-161 - *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015). Supply chain refers to "organizations, people, activities, information and resources, possibly international in scope, that provide products or services to consumers."

[78] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, (GAO-18-667T) (July 12, 2018).

[79] Europe Union Agency for Cybersecurity, Press Release, *Understanding the Increase in Supply Chain Security Attacks* (July 29, 2021).

[80] Pub. L. 114-261, *An Act to Enhance Whistleblower Protection For Contractor and Grantee Employees* (December 14, 2016).

[81] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP) (March 2021).
[82] The Society for Human Resource Management, *4 Essential Soft Skills for Successful Remote Work* (November 5, 2020).
[83] OPM, *Guidance on Establishing an Annual Leadership Talent Management and Succession Planning Process* (November 2017).
[84] The McKinsey Quarterly, *The War for Talent* (1998 Number 3).
[85] FedWeek, *Retirement Wave? Eligibility Numbers Holding Steady* (January 7, 2020).
[86] Executive Order 14305, *Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce* (June 25, 2021). The FDIC Legal Division asserted that the Executive Order is not binding on the FDIC, but that the FDIC may voluntarily implement the Executive Order's requirements.
[87] Statement of FDIC Chair, *On Oversight of Regulators: Does Our Financial System Work for Everyone?* (August 3, 2021).
[88] FDIC OMWI, *Total FDIC Workforce Demographics as of June 30, 2021.*
[89] White House, *Strengthening the Federal Workforce* (May 2021).

D. Acronyms

AEI	Alliances for Economic Inclusion
AFS	Available-For-Sale
AHDP	Affordable Housing Disposition Program
AI	Artificial Intelligence
AIG	American International Group, Inc.
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
ANPR	Advance Notice of Proposed Rulemaking
ASBA	Association of Supervisors of Banks of the Americas
ASC	Accounting Standards Codification
BCBS	Basel Committee on Banking Supervision
BoA	Bank of America, N.A.
BSA	Bank Secrecy Act
Call Report	Consolidated Reports of Condition and Income
CAMELS	**C**apital adequacy; **A**sset quality; **M**anagement capability; **E**arnings quality; **L**iquidity adequacy; **S**ensitivity to market risk
CARES Act	Coronavirus Aid Relief and Economic Security Act
CBAC	Community Bank Advisory Committee
CCP	Central Counterparties
CDFI	Community Development Financial Institution
CECL	Current Expected Credit Losses
CEO	Chief Executive Officer
CFO Act	Chief Financial Officers' Act
CFPB	Consumer Financial Protection Bureau
CFR	Center for Financial Research
CFT	Countering the Financing of Terrorism
CFTC	Commodity Futures Trading Commission
CIO	Chief Information Officer

CIOO	Chief Information Officer Organization
CISR	Division of Complex Institution Supervision and Resolution
CMG	Crisis Management Group
CMP	Civil Money Penalty
ComE-IN	Advisory Committee on Economic Inclusion
COVID-19	Coronavirus Disease 2019
CRA	Community Reinvestment Act
CRC	Consumer Response Center
CSBS	Conference of State Bank Supervisors
CSRS	Civil Service Retirement System
DCP	Division of Depositor and Consumer Protection
DFA	Dodd-Frank Act
DIF	Deposit Insurance Fund
DIR	Division of Insurance and Research
DIT	Division of Information Technology
DOA	Division of Administration
DRR	Division of Resolutions and Receiverships
EC	European Commission
EDIE	Electronic Deposit Insurance Estimator
EGRRCPA	Economic Growth, Regulatory Relief, and Consumer Protection Act
EU	European Union
ERM	Enterprise Risk Management
FAQs	Frequently Asked Questions
FASB	Financial Accounting Standards Board
FBO	Foreign Bank Organization
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FEHB	Federal Employees Health Benefits
FERS	Federal Employees Retirement System
FFB	Federal Financing Bank

FFIEC	Federal Financial Institutions Examination Council
FFMIA	Federal Financial Management Improvement Act
FID	Financial Institution Diversity
FinCEN	Financial Crimes Enforcement Network
FinTech	Financial Technology
FIRREA	Financial Institutions Reform, Recovery and Enforcement Act
FISMA	Federal Information Security Modernization Act of 2014
FMFIA	Federal Managers' Financial Integrity Act
FRB	Board of Governors of the Federal Reserve System
FRF	FSLIC Resolution Fund
FRWG	Financial Regulatory Working Group
FSB	Financial Stability Board
FSLIC	Federal Savings and Loan Insurance Corporation
FSOC	Financial Stability Oversight Council
FTE	Full-Time Employee
GAAP	Generally Accepted Accounting Principles
GAO	U.S. Government Accountability Office
GDP	Gross Domestic Product
GPRA	Government Performance and Results Act
G-SIBs	Global Systemically Important Banks
G-SIFI	Global SIFIs
HMDA	Home Mortgage Disclosure Act
IADI	International Association of Deposit Insurers
IDI	Insured Depository Institution
IMF	International Monetary Fund
IRS	Internal Revenue Service
IT	Information Technology
LCFI	Large Complex Financial Institution
LIBOR	London Inter-bank Offered Rate
LIDI	Large Insured Depository Institution

LMI	Low- Moderate-Income
LURAs	Land Use Restriction Agreements
MDI	Minority Depository Institutions
ML	Machine Learning
MOL	Maximum Obligation Limitation
MOU	Memoranda of Understanding
MRBA	Matters Requiring Board Attention
MWOB	Minority- and Women-Owned Business
MWOLF	Minority-and Women-Owned Law Firms
NAMWOLF	National Association of Minority-and Women-Owned Law Firms
NCDA	National Center for Consumer and Depositor Assistance
NCUA	National Credit Union Administration
NPR	Notice of Proposed Rulemaking
NSFR	Net Stable Funding Ratio
OCC	Office of the Comptroller of the Currency
OIG	Office of the Inspector General
OLF	Orderly Liquidation Fund
OMB	U.S. Office of Management and Budget
OMWI	Office of Minority and Women Inclusion
OO	Office of the Ombudsman
OPM	Office of Personnel Management
ORMIC	Office of Risk Management and Internal Controls
OTS	Office of Thrift Supervision
PPP	Paycheck Protection Program
Q&A	Question and Answer
QFC	Qualified Financial Contract
REFCORP	Resolution Funding Corporation
RFI	Request For Information
RMS	Division of Risk Management Supervision
RTO	Return to Office

SBA	Small Business Administration
SEC	Securities and Exchange Commission
SIFI	Systemically Important Financial Institution
SLA	Shared-Loss Agreement
SMS	Systemic Monitoring System
SNC	Shared National Credit Program
SRAC	Systemic Resolution Advisory Committee
SRR	SIFI Risk Report
SSGNs	Securitizations and Structured Sale of Guaranteed Note
TLAC	Total Loss-Absorbing Capacity
TSP	Federal Thrift Savings Plan
TSP (IT-related)	Technology Service Providers
UDAA	Unclaimed Deposits Amendments Act of 1933
UK	United Kingdom
Treasury	U.S. Treasury
VIEs	Variable Interest Entities
VITA	Volunteer Income Tax Assistance
WRH	Wisconsin Rural Housing