FDIC OIG Unimplemented Recommendations
As of August 15, 2019

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
1	AUD-16-001	Audit of the FDIC's Information Security Program - 2015	4	Non-public report.	10/28/2015
2	AUD-17-001	Audit of the FDIC's Information Security Program - 2016	5	Non-public report.	11/2/2016
3	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	4	Non-public report.	10/25/2017
4	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	5	Non-public report.	10/25/2017
5	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	9	Non-public report.	10/25/2017
6	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	10	Non-public report.	10/25/2017
7	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	15	Non-public report.	10/25/2017
8	AUD-18-004	The FDIC's Governance of Information Technology Initiatives	3	Implement an enterprise architecture (EA) that is part of the FDIC's Information Technology (IT) Governance Framework and used to guide IT decision-making.	7/26/2018
9	AUD-18-004	The FDIC's Governance of Information Technology Initiatives	5	Incorporate the revised IT Governance Processes into applicable FDIC policies, procedures, and charters.	7/26/2018
10	AUD-18-004	The FDIC's Governance of Information Technology Initiatives	7	Identify and document the IT resources and expertise needed to execute the FDIC's IT Strategic Plan. ^	7/26/2018

^ The Corporation's Corrective Action Closure Package with OIG for review.

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
11	AUD-19-001	The FDIC's Information Security Program - 2018	2	Non-public report.	10/25/2018
12	AUD-19-001	The FDIC's Information Security Program - 2018	4	Non-public report.	10/25/2018
13	AUD-19-002	Controls Over System Interconnections with Outside Organizations	2	Execute Memorandum of Agreement (MOAs) and Interconnection Security Agreement (ISAs) with Organization 2 and Organization 10 in accordance with the relevant contracts.	12/4/2018
14	AUD-19-002	Controls Over System Interconnections with Outside Organizations	3	Revise the standard contract language used for future contracts involving system interconnections, in coordination with Division of Administration (DOA), to align with National Institute of Standards and Technology (NIST) guidance.	12/4/2018
15	AUD-19-002	Controls Over System Interconnections with Outside Organizations	7	Develop and implement policies and procedures to govern the secure transfer of data outside of the FDIC using technologies that are not considered system interconnections.	12/4/2018
16	AUD-19-003	Payments to Pragmatics, Inc.	1	Determine the portion of the $7,510 in unsupported labor charges that should be disallowed and recover that amount.	12/10/2018
17	AUD-19-003	Payments to Pragmatics, Inc.	2	Determine whether the remaining labor charges for the subject under Task Orders 4 and 5 are unsupported charges that should be disallowed.	12/10/2018
18	AUD-19-003	Payments to Pragmatics, Inc.	3	Determine the portion of the $39,979 in unallowable labor charges that should be disallowed and recover that amount.	12/10/2018
19	AUD-19-003	Payments to Pragmatics, Inc.	4	Determine whether additional labor charges should be disallowed for off-site work performed under Task Orders 4 and 5 that was not covered by the audit.	12/10/2018

^ The Corporation's Corrective Action Closure Package with OIG for review.

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
20	AUD-19-004	Security Configuration Management of the Windows Server Operating System	2	Establish and implement controls to ensure that Chief Information Officer (CIO) Organization policies and procedures are established before deploying new or modified IT processes or programs.	1/16/2019
21	AUD-19-004	Security Configuration Management of the Windows Server Operating System	3	Establish requirements to ensure the independence of security control assessors.	1/16/2019
22	AUD-19-004	Security Configuration Management of the Windows Server Operating System	4	Establish and implement procedures to ensure that contractor-submitted Continuous Controls Assessment (CCA) Reports are reviewed for consistency with applicable requirements in contractual agreements and that such reviews are documented. ^	1/16/2019
23	AUD-19-004	Security Configuration Management of the Windows Server Operating System	5	Require that CIO Organization management ensure the sufficiency of CCA Report reviews and provide feedback when review activities are deemed insufficient. ^	1/16/2019
24	AUD-19-005	Preventing and Detecting Cyber Threats	1	Require that all existing firewall rules be documented with an approval and mission/business need, including the duration of that need.	5/28/2019
25	AUD-19-005	Preventing and Detecting Cyber Threats	2	Establish and implement a firewall policy consistent with National Institute of Standards and Technology guidance.	5/28/2019
26	EVAL-17-007	Controls over Separating Personnel's Access to Sensitive Information	2	Incorporate a risk assessment of individual separating employees into the FDIC's preexist clearance process. ^	9/18/2017

^ The Corporation's Corrective Action Closure Package with OIG for review.

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
27	EVAL-18-004	Forward-Looking Supervision	1	Issue a comprehensive policy guidance document defining Forward-Looking Supervision, including its purpose, goals, roles, and responsibilities.	8/8/2018
28	EVAL-19-001	The FDIC's Physical Security Risk Management Process	1	Revise and update the FDIC Physical Security Program Circular and develop and implement procedures to define the roles, responsibilities, and requirements for physical security risk management activities and decision-making. These revisions should include: a. Ensuring that there is sufficient documentation and support for physical security risk management activities and decisions, including those decisions related to when the Interagency Security Committee (ISC) standards were determined to be not practical; b. Ensuring that each facility security level (FSL) determination is documented, accurate, and adequately supported; c. Ensuring that if an FSL is revised, the FDIC reviews the countermeasures and risk mitigation strategies for the facility; d. Updating and reviewing facility security plans on an annual basis; e. Ensuring that all facility security assessment (FSA) recommendations are identified, prioritized, and tracked; f. Identifying requirements for pre-lease physical security activities and deliverables; and g. Requiring that FDIC senior management be routinely advised of the status of the physical security program at FDIC Headquarters, Regional, Area, and Field Offices.	4/9/2019

^ The Corporation's Corrective Action Closure Package with OIG for review.

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
29	EVAL-19-001	The FDIC's Physical Security Risk Management Process	2	Establish and implement training requirements for personnel conducting facility security level (FSL) determinations and Facility security assessments (FSAs).	4/9/2019
30	EVAL-19-001	The FDIC's Physical Security Risk Management Process	3	Establish and implement controls to ensure that DOA maintains security assessment-related records in accordance with the FDIC Records and Information Management Policy Manual.	4/9/2019
31	EVAL-19-001	The FDIC's Physical Security Risk Management Process	4	Implement an automated facility security assessment (FSA) template, tool, or other mechanism to ensure that that the FSAs consider all threat, consequence, and vulnerability assessments of undesirable events and assess relevant countermeasures for each FDIC facility. This tool or mechanism should track and record: a. Recurring, structured testing and maintenance programs for the FDIC's electronic security systems; b. Controls for electronic building and access systems at FDIC facilities; c. Security countermeasures for child-care centers in FDIC facilities; d. Facility Security Plans for FDIC facilities; and e. Accurate facility security level (FSL) and FSA data.	4/9/2019
32	EVAL-19-001	The FDIC's Physical Security Risk Management Process	5	Track and record training programs for physical security awareness that is provided to FDIC employees and contractors annually.	4/9/2019
33	EVAL-19-001	The FDIC's Physical Security Risk Management Process	7	Document the justifications for the physical security activities that the FDIC has taken in response to recommendations, including decisions to accept risk or regarding expenditures for security countermeasures above the recommended standards for an assigned facility security level (FSL).	4/9/2019

^ The Corporation's Corrective Action Closure Package with OIG for review.

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
34	EVAL-19-001	The FDIC's Physical Security Risk Management Process	9	Identify goals and metrics for measuring the performance of the physical security program to ensure the timeliness, quality, and effectiveness of FDIC risk management process activities. ^	4/9/2019

^ The Corporation's Corrective Action Closure Package with OIG for review.