FDIC OIG Unimplemented Recommendations
As of February 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-17-004	Follow-up Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program	3	Take steps to ensure the reliability of contractor personnel data in Corporate Human Resource Information System - Human (CHRIS-HR). ^	6/8/2017
4	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	4	Non-public report.	10/25/2017
5	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	5	Non-public report.	10/25/2017
6	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	6	Non-public report. ^	10/25/2017
7	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	9	Non-public report.	10/25/2017
8	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	10	Non-public report.	10/25/2017
9	AUD-18-001	Audit of the FDIC's Information Security Program - 2017	15	Non-public report.	10/25/2017
10	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

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

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
11	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
12	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
13	AUD-19-001	The FDIC's Information Security Program - 2018	1	Non-public report. ^	10/25/2018
14	AUD-19-001	The FDIC's Information Security Program - 2018	2	Non-public report.	10/25/2018
15	AUD-19-001	The FDIC's Information Security Program - 2018	3	Non-public report.	10/25/2018
16	AUD-19-001	The FDIC's Information Security Program - 2018	4	Non-public report.	10/25/2018
17	AUD-19-002	Controls Over System Interconnections with Outside Organizations	1	Revise and update existing policies and procedures to address the Planning, Establishment, Maintenance, and Termination of system interconnections, including roles and responsibilities and documentation requirements.	12/4/2018
18	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
19	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

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

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
20	AUD-19-002	Controls Over System Interconnections with Outside Organizations	4	Ensure that Division and Office Interconnection Security Agreement (ISMs) review Memorandum of Agreement (MOAs) and ISAs annually to ensure they remain current.	12/4/2018
21	AUD-19-002	Controls Over System Interconnections with Outside Organizations	5	Implement procedures to regularly review, update, and reauthorize MOAs and ISAs, including contacting outside organizations when appropriate.	12/4/2018
22	AUD-19-002	Controls Over System Interconnections with Outside Organizations	6	Develop and implement procedures for providing written notification to technical staff within the FDIC and at outside organizations when a system interconnection is no longer needed.	12/4/2018
23	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
24	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
25	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
26	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
27	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
28	AUD-19-003	Payments to Pragmatics, Inc.	5	Document the disposition of the Pragmatics site visit in CEFile.	12/10/2018

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

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
29	AUD-19-003	Payments to Pragmatics, Inc.	6	Remind Oversight Managers of the requirement to document the disposition of required site visits in the FDIC's contract files.	12/10/2018
30	AUD-19-003	Payments to Pragmatics, Inc.	7	Ensure that all task orders under the Information Technology Application Services II (ITAS II) Basic Ordering Agreement (BOA) and Tasking Basic Ordering Agreement (TBOAs) identify a place of performance.	12/10/2018
31	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
32	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
33	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
34	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
35	AUD-19-004	Security Configuration Management of the Windows Server Operating System	7	Update the security plan for the Windows Server operating system to reflect current security controls.	1/16/2019
36	AUD-19-004	Security Configuration Management of the Windows Server Operating System	8	Define roles and responsibilities to ensure FDIC personnel update security plans as security controls change.	1/16/2019

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

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
37	EVAL-17-004	Technology Service Provider Contracts with FDIC-Supervised Institutions	1	Continue to communicate to financial institutions (FI) the importance of: • Fully considering and assessing the risks that Technology Service Providers (TSPs) could have on the financial institutions (FI's) ability to manage its own business continuity and incident response planning efforts; • Ensuring that contracts with TSPs include specific provisions that address FI-identified risks, protect FI interests, and provide details necessary to allow FIs to manage their own business continuity planning and incident response and reporting efforts through TSP operations; and • Clearly defining key contract terms that would be important in understanding FI and TSP rights and responsibilities in the event of a business disruption or computer security incident particularly for those contracts that FIs identify as critical or that have access to sensitive or personally identifiable information. ^	2/14/2017
38	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
39	EVAL-17-007	Controls over Separating Personnel's Access to Sensitive Information	3	Work with the FDIC's Chief Information Officer to establish appropriate policy for using data loss prevention to support the FDIC's pre-exit 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
40	EVAL-17-007	Controls over Separating Personnel's Access to Sensitive Information	10	Work with the FDIC's Chief Information Officer to develop an expanded and better defined use of the data loss prevention tool for separating contractors.	9/18/2017
41	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
42	EVAL-18-004	Forward-Looking Supervision	4	Conduct recurring retrospective reviews to validate that examiners thoroughly documented their written analyses of the financial institutions' practices regarding concentration risk management.	8/8/2018
43	OIG-18-001	The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches	9	Develop guidance and training to ensure that employees and contractors are fully aware of the responsibility to return all FDIC equipment and documents and the prohibition against removing any sensitive information from FDIC premises before they depart, and understand the consequences—including available legal remedies—of providing false or inaccurate statements to the FDIC related to that responsibility.	4/16/2018
44	OIG-18-001	The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches	10	Ensure that its policies, procedures, and practices result in statements and representations to Congress and the American public that are full and complete and reflect the latest information known to agency personnel.	4/16/2018
45	OIG-18-001	The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches	11	Update and correct prior statements and representations made to Congress regarding the incidents addressed in this Special Inquiry where previous information is no longer accurate, valid, or complete.	4/16/2018

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

#	OIG Report No.	Report Title	Rec No.	Recommendation	Issued Date
46	OIG-18-001	The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches	13	Ensure that Congressional communications policies, procedures, and guidelines establish a single office that has accountability and authority for providing timely responses compliant with Congressional requests and communicating with Congressional staff regarding those requests.	4/16/2018

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