FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for the
FDIC Office of the Chief Information Security Officer

Combined Operational Risk, Security, Investigations & Compliance Application (CORSICA)

Date Approved by Chief Privacy Officer (CPO)/Designee
1/31/2018

Section 1.0: Introduction

In accordance with federal regulations and mandates[1], the FDIC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).[2] The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the FDIC Privacy Program Staff at: privacy@fdic.gov, who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

Section 2.0: System/Project Description

2.1 In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.

The Combined Operational Risk, Security, Investigations and Compliance Application (CORSICA) is the FDIC's electronic governance, risk and compliance (eGRC) system based on the RSA Archer application. This web-based intranet solution consists of multiple modules that perform different types of business process management functions related to information security workload.

[1] Section 208 of the E-Government Act of 2002 requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum M-03-22 provides specific guidance on how Section 208 should be implemented within government agencies. The Privacy Act of 1974 imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, Section 522 of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

[2] For additional guidance about FDIC rulemaking PIAs, visit the Privacy Program website or contact the FDIC Privacy Program Staff at privacy@fdic.gov.

At present, the FDIC has deployed or is in the process of deploying the following modules:

- Federal Enterprise Management (deployed)
- Vendor Management (deployed)
- Security Operations Management (deployed)
- Case Management (deployed)
- Task Management (available/not in use)
- Schedule Management (available/not in use)
- Federal Enterprise Management (pending/future)
- Threat Management (pending/future)
- Business Continuity Management (pending/future)
- Assessment and Authorization (pending/future)
- Continuous Monitoring (pending/future)

The purpose of CORSICA is to create an environment for information security case management and process management. It will also replace existing manual processes. The tool will collect information about security incidents, forensic investigations, breaches[3] of personally identifiable information (PII), threat intelligence, and vendor security assessment processes and tracking. Future development will include vulnerability tracking through the Threat Management module, asset inventory through the Federal Enterprise Management module, continuous monitoring for detection and monitoring of compliance/risk issues through the Continuous Monitoring module, and automation of the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) process through the Assessment and Authorization module.

In terms of personally identifiable information (PII) contained in the system, this Privacy Impact Assessment (PIA) focuses on the Security Operations Management module which was deployed into production in 2015 to replace the Office of the Chief Information Security Officer's (OCISO) Remedy system. The Security Operations Management module automates and centralizes work activities and documentation related to FDIC Security Operations Center operations, incident response, and data breach management. The web-based intranet solution streamlines tracking and facilitates effective management of incident and breach investigations from initial report to closure by reducing paper-based and manual processes, consolidating response procedures, and providing enhanced reporting functionality. In addition, the solution provides a centralized repository for storing and reviewing data pertinent to responding to or recovering from an incident or breach and thus could contain any manner of PII involved in an incident. This data will be accessed by authorized personnel within OCISO, the Computer Security Incident Response Team (CSIRT) and divisions/offices for use in evaluating and mitigating the incidents, as well as determining and implementing appropriate corrective actions, such as providing notification and credit monitoring to affected individuals and entities.

In addition to the PII which may be collected in conjunction with incidents managed within the Security Operations Management module, the Vendor Management module contains PII, such as names and business contact information for vendor personnel. Therefore, this PIA also addresses this module. Refer to Section 3.0 of this PIA for additional information.

[3] A breach is an occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for an other than authorized purpose.

Section 3.0: Data in the System/Project

The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.

3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, etc.) will be collected, used or maintained in the system? Explain.

The system will contain the following types of PII relating to the categories of individuals specified below.

A. Incident Reporters and Investigators – The Security Operations Management module contains the names and work email addresses of FDIC employees and contractors assigned to investigate and remediate security incidents and data breaches. It will also contain identifying information, such as full names, system user names, network IDs, and contact information (typically work-related, however personal contact information, such as a personal cell phone number could be included) for incident reporters and their managers/supervisors, if applicable.

B. Subjects of Investigation / Parties that Caused the Incident – The Security Operations Management module contains the names of FDIC employees, contractors , or other individuals who violated or potentially violated FDIC privacy and security requirements and/or otherwise may have caused or been involved with FDIC security incidents and data breaches. In some cases, but not all, the party that caused the incident or subject of the investigation is also the incident reporter. In addition to their names, the system may contain work or personal contact information, employment information and/or other contextually sensitive details relating to the subject's potential motivation and/or involvement in FDIC security incidents and breaches. For example, the system may contain current employment information and details about the terms of an FDIC separation agreement for a former employee suspected of compromising FDIC data in order to provide a competitive edge to his new employer.

C. Affected Individuals and Entities – Authorized CORSICA users may upload copies of breached data and supporting documentation related to investigations of security incidents and breaches into the system. This data could potentially contain any manner of PII pertaining to potentially affected individuals and entities, including full name, home address, personal telephone number, social security number (SSN)/taxpayer identification number (TIN), place/date of birth, and financial information.

D. FDIC Vendors – The Vendor Management module will contain PII, such as names and business contact information for vendor personnel.

3.2 What is the purpose and intended use of the information you described above in Question 3.1?

The PII pertaining to incident reporters, investigators and subjects of investigations (detailed in Section 3.1, A-B) serves to document pertinent facts and parties involved in FDIC security incident investigations, as well as the basis for the risk level determinations and breach/non-breach classifications.

The PII pertaining to affected individuals/entities (detailed in Section 3.1, C) is required to determine and execute appropriate breach remediation activities, including the issuance of external notification and credit monitoring services to affected individuals and entities. SSNs/TINs are sometimes used for purposes of address verification in cases where FDIC does not have the current addresses of affected parties.

The PII pertaining to FDIC vendors (listed in Section 3.1, D) is necessary for tracking the status of vendor contracts, risk rating, and compliance status.

3.3 If Social Security Numbers (SSNs) are collected, used, or maintained in the system, please answer the following:

a) Explain the business purpose/need requiring the collection of SSNs: CORSICA is not designed to collect, use , or maintain SSNs, however, SSNs could be collected, used or maintained within CORSICA incidentally in conjunction with activities associated with the investigation and resolution of security incidents/breaches.

b) Aside from 12 U.S.C. § 1819, which provides the general authority for the Corporation to collect SSNs, are there any other Federal statutes/authorities that justify the collection and/or use of SSNs?

☐ Yes List any additional legal authorities:
☒ No Information collected and maintained within CORSICA is collected and maintained in conjunction with the support of FDIC's overarching examination and receivership authorities stipulated within 12 USC § 1819.

c) Is the SSN is masked or otherwise truncated within the system?

☐ Yes. Explain:
☒ No. Is it possible to mask or otherwise truncate the SSN within the system?
☐ Yes. Explain how it may be masked or truncated and why this has not been implemented:
☒ No. Explain why it may not be masked or truncated: CORSICA is not designed to collect, use , or maintain SSNs, however, SSNs could be collected, used or maintained within CORSICA in unmasked text fields or in otherwise unstructured formats incidentally in conjunction with activities associated with the investigation and resolution of security incidents/breaches..

d) Is access to SSNs (and other sensitive PII) restricted in any way to specific groups of users of the system?

☒ Yes. Explain: Access to information in CORSICA is managed and maintained based on user roles and the business requirements associated with those roles.
☐ No. Is it possible to restrict access to specific groups of users within the system?
☐ Yes. Explain how access may be restricted and why this has not been implemented:
☐ No. Explain why access cannot be restricted:

3.4 Who/what are the sources of the information in the system? How are they derived?

Automated Data Sources

The following information is pulled from, or derived from logs and alerts, produced by the systems listed below.

Data Source	Type of Data Provided by Source
Active Directory	Name, work email address, and telephone number of FDIC asset owners/users. System information for assets
Splunk	Event logs containing IP addresses, system names, FDIC User Ids, and access information
ServiceNow	Incident ticket information

Manual Data Sources

Authorized FDIC employees and contractors manually enter the information specified in Section 3.1 into the system. In addition, within the Security Operations Management module, authorized users may upload supporting documentation related to the incident (e.g., proof of user policy re-certification, pertinent correspondence, incident timelines, minutes from Breach Response Team meetings, etc.) and copies of breached data which may contain some or all of the PII specified in Section 3.1. Copies of breached data may be recreated or derived from FDIC systems/applications and hardcopy records.[4] In cases where breached data relates to a financial institution (FI) and cannot be recreated from FDIC systems or hardcopy records, FDIC may contact the FI to request a copy of the data and manually load it into the system for analysis and implementation of appropriate remediation activities, such as providing notification and credit monitoring to affected individuals.

Additionally, data captured by FDIC's Data Loss Prevention tool and Splunk Enterprise Security may be manually uploaded into the system for analysis and execution of appropriate remediation activities, such as providing notification and credit monitoring services to affected parties.

3.5 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

The Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) provides incident tracking numbers to the FDIC based on incidents reported to them. This allows the FDIC to match up its data with US-CERT's tracking number, ensuring reporting is coordinated and accurate.

FDIC often works in concert with state banking regulators who may provide data for incidents processed. State banking regulators are also occasionally reporters of incidents or subjects of investigation as they share workspace at some FDIC locations. CSIRT may also work with local law enforcement officials in pursing investigations of a criminal nature, and in concert with the FDIC Office of Inspector General. The purpose for providing the data and its use is for the investigation and documentation of information security incidents. By understanding the nature of the data, CSIRT can better understand what has occurred and the risk associated with the incident and what actions may need to be taken, such as offering credit monitoring services to individuals.

3.6 What other third-party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

CSIRT may collect data from private institutions that have a contractual relationship with FDIC to provide a service such as legal, information technology (IT), or financial support. The data obtained from these sources could potentially contain PII data of any type that may be related to the investigation of an incident or breach. The information would be gathered to further carry out cybersecurity investigations. This potentially includes: full name; date of birth; SSN, photographic identifiers; driver's license/state identification number; Employee Identification Number; mother's maiden name; home address; personal telephone numbers; medical information; financial information and/or numbers; certificates, legal documents, records or notes; investigation report or database; personal web URLs; personal email address; education records; military status and/or records; employment status and/or records; and foreign activities and/or interests. CSIRT will use names, user names, and system hostname to identify users within the system.

[4] For a listing of FDIC systems/applications and their associated Privacy Impact Assessments, visit https://www.fdic.gov/about/privacy/assessments.html.

The Vendor Management module is utilized to consolidate vendor data and profiles, the status of contracts, and determine risk levels. It also stores information as to which Division is responsible for the management of the vendor relationship.

3.7 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

☐ Yes Explain the issues and circumstances of being able to opt out (either for specific data elements or specific uses of the data):

☒ No Explain: Individuals cannot opt out by declining to provide personal information or by consenting only to a particular use of their information. CSIRT is required to gather all pertinent information regarding FDIC incidents. The information is required to document the investigation of actual and potential data breaches and as a basis for determinations related to risk and remediation activities.

Section 4.0: Data Access and Sharing

The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.

4.1 Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.

The primary users of the Security Operations Management module include authorized FDIC employees and contractors in the following areas who have a "need to know" the information contained in this system in order to carry out their duties:

- Individuals within the FDIC OCISO Security, Forensics, and SOC/CSIRT functions for purposes of initiating and conducting incident investigations and making decisions on changes in the enterprise that may improve the security posture of FDIC;
- Individuals within the FDIC OCISO Privacy functions and consultative officials for purposes of assisting Divisions with investigating potential and confirmed data breaches and making determinations regarding risk, mitigation, and FDIC actions required as a result of data breaches; and
- Division Information Security Managers and Incident Response Points of Contact for purposes of investigating, assessing risk, and mitigating incidents and breaches affecting their respective Divisions/Offices.

The primary users of the Vendor Management (VM) module include FDIC personnel in the following areas for the purposes described below:

- Business Process Owners – This includes oversight managers, technical monitors, or anyone intimately familiar with the business process that is being outsourced. These users will create and maintain records describing the type of data and its flow as it pertains to the business process.
- Information Security Managers (ISM) – ISMs assist the business process owners in completing the CORSICA/VM records. They also serve as the next signatory in the business workflow of the Security Profile questionnaire. They also have read/write access to the VM module to fulfill their ISM responsibilities.
- OCISO – OCISO staff are the final signatory of the Security Profiles and the Vendor Management business process. As with ISMs, they may need to make small edits and require read/write access as well as the ability to delete vendor records, which is subject to audit logging.

- Users with Read-Only Access – There are times when the data in CORSICA/VM needs to be read by certain users, including auditors and executives. These users will be unable to make modifications and will have read-only access.

In addition, authorized developers have access to the data in the non-production environment for the purpose of supporting the hardware, communication, database, etc. The Office of the Inspector General and Government Accountability Office may request access to data in the system through their FDIC government liaisons in order to perform their respective audit functions. This PIA will be updated on and as needed basis for the deployment of additional CORSICA modules.

4.2 How is access to the data determined and by whom? Explain the criteria, procedures, controls, and responsibilities for granting access.

Access to data in the Security Operations Management module is limited to authorized FDIC/OCISO employees and contractors within the Privacy Office, the Security Engineering and Protection Section (SPES) SOC/CSIRT unit, and the SPES Forensics unit, as well as division ISMs/Incident Response POCs and, upon request, other FDIC breach response officials.

Access to data in the Vendor Management module will be provided to business process owners, Information Security Managers, OCISO staff, and auditors/executives who require read-only access for authorized users.

All users who have access to the data must have the approval of their manager/supervisor and the program manager/data owner of the requested capability in order to be granted access. Additionally, CORSICA's functional security limits a user's access to specific data and restricts the user's ability to view and update data fields based on the specific functions assigned to his/her level of access. All access granted is determined on a "need to know" basis. Controls are documented in the official CORSICA system documentation. Access to CORSICA is managed in accord with FDIC access control policy, and user access to CORSICA is provisioned and tracked using the FDIC's Access Request and Certification System (ARCS).

4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.

☐ No

☒ Yes Explain. A server hosting middleware (Unified Connector Framework) software has push/pull endpoints to receive data from external SYSLOG servers which are then pushed into CORSICA via API calls. No development toward integration has yet been completed.

4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.

Other agencies and entities do not have direct access to the system. However, information in the system may be provided to external auditors with a business need upon request. In addition, for breaches involving financial institution (FI) customer data, FDIC may provide a list of breach-affected customer names to the FI for purposes of address verification and issuance of notification letters and offers of credit monitoring to the affected individuals.

4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.

The CORSICA program manager and data owners are responsible for the management and decision-making authority over this specific area of agency data. The program manager, data owners and DIT Information Security Manager serve as the sources of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing.

While the users referenced above share this data responsibly, it is every user's responsibility to abide by FDIC data protection rules that are outlined within the FDIC IT Security and Privacy Awareness Training which all employees are required to complete on an annual basis.

4.6 What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

Contractors are employed by FDIC's CIOO OCISO staff to provide development and maintenance support for CORSICA. Each contractor who has access to CORSICA data is required to complete the FDIC IT Security and Privacy Awareness Training on an annual basis, and sign an FDIC confidentiality agreement (Form FDIC 3700/46A).

Section 5.0: Data Integrity and Security

The following questions address how data security and integrity will be ensured for the system/project.

5.1 How is data in the system verified for accuracy, timeliness, and completeness?

PII is manually entered and uploaded into CORSICA during the incident investigation process. It is the responsibility of the authorized FDIC employee or contractor entering the data to accurately transcribe relevant information. To the extent inaccurate information is located, it will be edited for accuracy. CORSICA utilizes various field types for capturing information such as text, numeric, and date which allow only matching data types to be entered. Wherever possible, input masks are utilized in text fields which require specific formats for things such as SSNs (allowing only nine digits and includes dashes) and e-mail addresses (the @ and domain are required).

5.2 What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.

CORSICA utilizes access roles to assign "create," "read," "update," and "delete" access rights. CORSICA access roles are assigned to user groups. Users are then assigned to specific user groups based on business need. Records containing various field types are limited to specific user groups based on the evaluation of criteria within each record and are dynamic. Sections containing calculated fields or information not relevant to average users are contained in hidden administrative sections which require administrative privileges. User access to CORSICA requires management approval and is provisioned and tracked using the FDIC's Access Request and Certification System (ARCS).

Section 6.0: Data Maintenance and Retention

The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.

6.1 How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Data is retrieved using the report feature within CORSICA. Any field located within the application to which a user has access may be chosen for searching, filtering, and retrieving information. CORSICA was not designed to retrieve information by a personal identifier, and information is not typically retrieved using specific PII elements, such as name, but rather using other criteria, such as the name of an FDIC Division, a CSIRT incident number, a data breach number, or the status of an incident.

6.2 What kind of reports can be produced *on individuals*? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?

As noted in the previous section, any number of fields can be included in a CORSICA report. Therefore, a report could contain information specific to any record stored in the system to which the user has access. However, CORSICA is currently not designed to retrieve information by a personal identifier, nor is it utilized for this type of reporting. The ability to create and modify reports is controlled through access roles and is specific to each module within the system. Typical users generally do not have the ability to create, edit, or view reports. Developers have the ability to create reports which are then placed in dashboards. The access to dashboards is restricted by user group and report information is only visible to a user with valid access to the information.

6.3 What are the retention periods of data in this system? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

Full and differential database backups are performed weekly and copied to a storage area network. All backups older than two weeks are deleted automatically through structured query language (SQL) agent maintenance plans. There is currently no retention period for records maintained within CORSICA or procedures for the disposition of CORSICA data (other than backups), however, this issue will be addressed in the future, and FDIC Circular 1210.1, FDIC Records and Information Management (RIM) Policy Manual, will be used to guide the retention and data disposition process. Live data is stored within the instance database indefinitely.

6.4 In the Federal Register, under which Privacy Act System of Records Notice (SORN) does this system operate? Provide number and name.

Not Applicable. CORSICA does not operate as a system of records.

6.5 If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

Not Applicable.

Section 7.0: Business Processes and Technology

The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the Corporation made regarding business processes and technology.

7.1 Will the system aggregate or consolidate data in order to make privacy determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

CORSICA aggregates security incident information which may be associated with users, however the aggregated/consolidated data is not used to make privacy determinations or derive new data about individuals. The ability to create and view such reports is restricted to specific authorized individuals having a specific business need.

7.2 Is the system/project using new technologies, such as monitoring software, Smartcards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.

The system is not using new technologies to collect, maintain, or track information about individuals.

7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.

The system will not provide the capability to monitor individuals or users. CORSICA tracks changes to record information through the use of history log fields. By default, these fields track all fields indefinitely. Retention by days may be enabled and specific fields may be chosen for tracking. Currently, only users with read access to security incident records have the ability to view history log information. An out of the box audit role is available, but not implemented, which would also have this capability if implemented.

7.4 Explain the magnitude of harm to the Corporation if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the Corporation be affected?

Any exposure of privacy-related data could adversely affect the reputation of FDIC. Since the system may contain PII about members of the public, it is necessary to maintain safeguards to protect against the potential fraud or theft from either an FDIC employee or persons outside FDIC. Disclosure of this data could cause financial damage (e.g., identity theft) or other material harm to affected individuals and/or entities whose data is contained in the system. Therefore, FDIC takes all security precautions necessary to prevent unauthorized disclosure of data.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.

The completion of this PIA did not result in changes to business processes or technology.