U.S. Securities and Exchange Commission

ITS Agile Offsite Facility (IAOF)
PRIVACY IMPACT ASSESSMENT (PIA)

February 1, 2023

Division of Enforcement

GENERAL INFORMATION - Project/System Information

The ITS Agile Offsite Facility (IAOF), directly supports the SEC Division of Enforcement (ENF) efforts to collect, receive, process, and store electronic submissions from Federal securities inspections, examinations, investigations, and litigation, across all SEC locations/regions.

The facility includes an IT network infrastructure (IAOF-Net) consisting of on-network and off-network systems designed specifically to collect, store, process, and transmit internal (SEC) and external (3rd party) digital evidence, operations data (e.g., case notes, chains of custody, emails), and metadata.

IAOF and IAOF-Net's support includes collecting, converting, analyzing, and producing electronic evidence in the document discovery process, documenting and presenting findings impartially, and objectively analyzing such findings using SEC-approved tools, procedures, and techniques developed by the ENF Information Technology (IT) Forensics program.
The work performed is as follows:

1. Onsite Computer Forensics
   - Process and analyze collected electronically stored information (ESI)
   - Create productions for delivery to SEC's Central Processing Unit (CPU), Chenega Scanning Facility
   - Image auditor laptops for CPU
   - Initiate and track chain of custody
   - Document processing activity
2. Offsite Data Collections (in field acquisitions)
   - Collect and preserve identified electronic storage devices (ESD) (e.g., computers, mobile devices, hard drives, thumb drive)
   - Track chain of custody
   - Document and report on collection activities
3. Data File Conversion (document/electronic file conversion)
   - iWork File Conversion
   - GraphPad File Conversion
   - iChat File Conversion
   - Audio/video file conversion
   - Accellion secure file transfer
4. Courier services
   - Transport media and/or evidence to and from the SEC CPU and the ITFL.
   - Track chain of custody

ESD containing ESI may be collected in the field, picked up via courier from the SEC CPU, or shipped directly to IAOF or SEC headquarters. Field collections are performed by SEC subcontractors deployed to various country, state, and/or local locations to collect and ship custodian data to IAOF or directly to SEC ENF.

Productions created from processed ESI and ESD delivered to IAOF or SEC are handled by an IAOF courier who performs pickup & transporting of materials to the SEC CPU and SEC twice weekly.

IAOF-Net is also used to communicate with SEC staff via approved email systems such as Microsoft Exchange and ZixMail.

1. Name of Project or System.
ITS Agile Offsite Facility Network

2. What is the purpose of the Project or System?
The ITS Agile Offsite Facility (IAOF) directly supports the SEC Division of Enforcement (ENF) Records Management efforts to collect, receive, process, and store electronic submissions from Federal securities inspections, examinations, investigations, and litigation, across all SEC locations/regions.

3. Requested Operational Date?
The system has been operational pursuant to the SEC Electronic Discovery Support of Litigation (EDSL) Services Contract Order No. 503102-21-F-0116 effective 12/01/2021. Based on the contract terms, ITS Agile (Contractor) has one (1) year from the effective date to comply with the SEC ATO system requirements, unless the SEC grants an extension. Actual date 12/01/2022.

4. System of Records Notice (SORN) number?
Information subject to the Privacy Act of 1974, as amended, collected in paper and electronic submissions from Federal securities inspections, examinations, investigations, and litigation are covered under SORN SEC-17 Enforcement Files 85 FR 85440 (January 27, 2021).

SECTION I - Data Purpose Specification

The legal authority for the collection of information is 15 U.S.C.77s, 77t, 78u, 77uuu, 80a-41, and 80b-9.17 CFR 202.5. The Division of Enforcement (ENF) staff has the primary responsibility to enforce Federal Securities Laws. The staff conducts investigations into possible violations of the Federal securities laws, and prosecute the Commission's civil suits in the Federal courts as well as its administrative proceedings. Information collected is considered evidentiary material and some documents are used in litigation. The Records Management Production Processing and Scanning Program (RMPPS) supports ENF's business process for handling and processing investigative and litigation material.

SECTION II – Data Minimization

Only authorized users will be granted access to the system; this access to information will be limited to a need to know basis. IAOF-Net collects, stores, process, and transmit internal (SEC) and external (3rd part) digital evidence, operations data and metadata.

These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with contract requirements as identified in SEC Electronic Discovery Support of Litigation (EDSL) Services Contract Order No. 503102-21-F-0116.

SECTION III – Data Sharing Practices

ITS Agile does not make the materials processed and stored available to any external entities. Access to materials and information is limited to a need-to-know basis when in the possession of ITS Agile. Administrative, physical, and technical controls are implemented to limit access to the information and prevent inadvertent or unauthorized disclosure to individuals without a need to know.

SECTION IV – Individual Participation

Individuals are not generally permitted to access or correct records about themselves in ENF materials[1].The materials are exempted from the Privacy Act insofar as it contains investigatory materials. However, subject to the exemption above, individuals may make a Privacy Act request for appropriate access, correction, and redress under the procedures described in 17 C.F.R. Subpart H-Regulations Pertaining to the Privacy of Individuals and Systems of Records Maintained by the Commission.

SECTION V – Data Quality and Integrity

Digital evidence is collected during onsite data collection operations using non-network connected forensic equipment by ITS Agile's offsite Mid-level Computer Forensic Specialists.

After quality control checks, external hard drives containing collected evidence and associated chains of custody and data collection paperwork are transferred from ITS Agile's offsite forensics staff to ITS Agile's onsite forensics staff at the ITFL. Due to COVID government site closures, all collected digital evidence that is being actively worked, is physically stored at IAOF.

SECTION VI – Security and Auditing

IAOF has implemented a series of ISO standard and digital forensic best practice quality assurance policies and procedures, in addition to the application of NIST SP 800-53 security and privacy controls that address appropriate information and information systems security safeguards that protect against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of SEC collected PII.

SECTION VII – Privacy Impact Analysis

[1] Under 5 U.S.C. 552a(k)(2), this system is exempted from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) and 17 CFR 200.303, 200.304, and 200.306, insofar as it contains investigatory materials compiled for law enforcement purposes. This exemption is contained in 17 CFR 200.312(a) (1).

Privacy Risk related to Uses of Information: There is a risk that unauthorized users may access the information in ITS Agile and use it for purposes that are inconsistent with the purposes for which it was collected or that authorized users may use the information for an unauthorized purpose.

Mitigation: This risk is mitigated through the use of role-based access controls in a secure web portal, which only permits authorized individuals from the vendor and SEC program management office to access information in the vendor's system, and through the vendor contract, which identifies the vendor's responsibility with respect to the records in its possession. In addition, SEC requires all vendor personnel who support the ITS Agile to sign a non-disclosure agreement. Vendor personnel also receive a Public Trust background investigation, computer security and privacy training, and agree to rules of behavior to indicate they understand and will adhere to appropriate data use.

Privacy Risk related to Notice: There is a risk that individuals may not be aware that their information will be sent to ITS Agile and then on to the SEC system.

Mitigation: This risk is mitigated through the publication of this PIA, which is adequate notice given the limited function and purpose of ITS Agile Offsite Facility. Individuals are provided appropriate notice at the point of collection of their information regarding the use of their information more generally and are also provided as appropriate with the opportunity to decline to provide information or otherwise consent to its use.

Privacy Risk related to Sharing: There is a risk that the information will be disclosed and used for a purpose that is not consistent with the purposes for which it was originally collected.

Mitigation: This risk is mitigated through various controls including initial intake/receipt, tracking and logging of all ENF productions for all SEC locations.

Privacy Risk related to Redress: There is a risk that individuals will not have the ability to access and amend records that ITS Agile holds.

Mitigation: This risk is mitigated because although there is no ability to access and amend records at ITS Agile, there are clear processes in place and notice provided to individuals at the point of collection regarding accessing and amending records provided to the SEC.