PRIVACY IMPACT ASSESSMENT—MARCH 2021

Automated Background Investigation System (ABIS) v.1

Does the CFPB use the information to benefit or make a determination about an individual?	Yes
What is the purpose?	Supports the prescreening and adjudicating of background investigations and security clearances.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Generally applicable: Appropriate opportunities for notice, consent, access, and redress.

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Act"), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau ("CFPB" or "Bureau"). The Bureau administers, enforces, and implements federal consumer financial protection laws. In support of these responsibilities, the Bureau's Administrative Operations Division provides personnel security and credentialing services for Bureau employees and contractors, including pre-employment processing, credentialing, security adjudications, background investigations, and security clearance processing activities. Information is collected to support these services to determine whether an individual is suitable for Bureau employment or on behalf of the Bureau as an employee, contractor, intern, Bureau advisory board member, expert witness, or detailee. The collection of this information is authorized by Executive Orders 9397, as amended by 13478, 10450, 10577, 10865, 12968, and 13470; Civil Service Act of 1883, Section 2; Public Laws 82-298 and 92-261; Title 5, U.S.C. Sections 1303, 1304, 3301, 7301, and 9101; Title 22, U.S.C. Section 2519; Title 42 U.S.C. Sections 1874 (b)(3), 2165, 2201, and 2455; Title 50 U.S.C. Section 435b(e); Title 5 CFR Sections 731, 732 and 736; Homeland Security Presidential Directive 12 (HSPD 12); and, OMB Circular No. A-130.

The Bureau is required to complete background investigations for suitability and security clearance determinations to ensure individuals supporting the Bureau are deemed reliable, trustworthy, and suitable for the role they will fulfill. The Bureau's Office of Security utilizes the Automated Background Investigation System (ABIS), a commercial off the shelf (COTS) web-based system, to support the collection of data that is used by the Bureau to initiate background investigations.

ABIS is used to initiate, track, process, close Bureau-initiated background investigations and security clearances, and curate case documentation. ABIS also provides automated integration with Office of Personnel Management's (OPM's) e-Delivery via Connect:Direct which enables the Bureau to electronically receive results of closed background investigations and results of fingerprint verifications that are maintained by OPM. ABIS reduces processing time for background investigations, standardizes adjudication procedures, reduces manual processing and associated errors with the collection and processing of paperwork. ABIS also provides a centralized system of records the Bureau uses to conduct background investigations and maintain associated documentation, such as email communication with the candidate, copies of forms submitted by the individual, etc. ABIS also has components, such as the ABIS External Interface Controller (EIC), that the Bureau may use for secure electronic submission of

information. Other than the functionality that EIC provides to electronically collect information directly from an individual, ABIS is not externally accessible by individuals for any other purpose.

The Bureau conducts background investigations for individuals who are candidates for Bureau employment, internships, contract support, advisory board member participation, expert witnesses, and detailees. To complete a background investigation the Bureau collects personally identifiable information (PII) to include information related to selective service registration, military service information, professional history, personal history, credit history and related background information. The PII data elements typically collected includes Social Security Number (SSN); date of birth; legal first name; legal middle name; legal last name; suffix; birthplace (country, city and state as applicable); citizenship status; email address; home street address, city, state and zip code; phone number; and an individual's signature.

The Bureau has different mechanisms to collect information, to include manual collection through Optional Form (OF) 306, *Declaration for Federal Employment,* electronically ABIS components and modules, CFPB name check forms (referred to as Federal Bureau of Investigation (FBI) Name Check Request – Expert Witness and FBI Name Check Request – Advisory Board forms), and through requests for information from other federal agencies. The processes by which the Bureau collects information and enters it into ABIS may vary depending on the role of the individual (e.g., employee or intern, contractor, advisory board member, expert witness, or detailee). Each method for collection is described in more detail in Section 1 below.

Once the Bureau collects the information, it is shared with Defense Counterintelligence and Security Agency (DCSA) (via OPM) who conducts the background investigation for all candidate types on behalf of the Bureau. Authorized Bureau staff (herein referred to as Personnel Security Staff) have access to the OPM NP2 portal. The NP2 is the secure portal which allows authorized Personnel Security Staff to access a gateway to DCSA's automated systems (Electronic Questionnaires for Investigations Processing (e-QIP), Personnel Investigations Processing System (PIPS), and Clearance Verification System (CVS)) for the purpose of checking whether a candidate has a recently completed investigation. If the subject has an investigation that is recent and at the appropriate level which has been favorably adjudicated, Bureau Personnel Security Staff will accept the investigation on reciprocity. If a recent and completed background investigation has not occurred, Personnel Security Staff will initiate a background investigation (details regarding this process are described in the sections below). The Bureau's Office of Security employs the use of adjudicative support services offered by OPM for adjudication of

contractor employees. The adjudication determinations are sent by OPM through the NP2 portal on a daily spreadsheet and the spreadsheet is uploaded into the ABIS system. All other cases, such as Federal employees, interns, advisory board member and expert witness adjudications are completed by the Bureau's Office of Security within the ABIS System. Like the purpose of sharing information with NP2, authorized Personnel Security Staff also uses General Service Administration's (GSA's) USAccess System for fingerprint enrollment to conduct FBI fingerprint checks. The Bureau leverages GSA to collect fingerprint from candidates and then transmits it to DCSA to conduct the check against FBI database, however, the Bureau does not maintain fingerprints in ABIS. The results of fingerprint checks are transmitted electronically through the secure connection provided through OPM e-Delivery and Connect: Direct, from DCSA to ABIS. Both e-Delivery and Connect:Direct provide a secure, authenticated electronic one-way connection for OPM to submit results of investigations directly into ABIS.

The scope of this PIA is to identify and mitigate privacy risks associated with ABIS and its components and modules. The collection, maintenance, and use of the information within ABIS are covered by OPM System of Records Notice (SORN) OPM/GOVT-1, General Personnel Records, and OPM SORN OPM Central-9, Personnel Investigations Records. The Bureau is authorized to use information covered under this SORN in accordance with Title 5 of the U.S. Code, section 1104, which allows OPM to delegate personnel management activities to other Federal agencies. Upon determination of an individual's suitability for a role within the Bureau, the individual's record is kept in accordance with the established records retention schedule identified below. The OPM NP2 is out of scope for the purposes of this PIA, but NP2 is discussed in the OPM NP2 PIA found at https://www.opm.gov/information-management/privacy-policy/privacy-policy/p2.pdf. The GSA USAccess system is also out of scope for this PIA, but USAccess is discussed in the USAccess PIA found at https://www.ncua.gov/files/publications/privacy/usaccess.pdf.

The ABIS and its components are developed using the agile methodology. As such, system change requests and security assessment and authorization (SA&A) documentation address privacy relative to systems development, including, as warranted and appropriate: statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment.

The Paperwork Reduction Act (PRA) applies to specific forms used to collect information:

- Information collected on OPM Form 306, Declaration for Federal Employment, is approved by OMB information collection number (ICR) 3206-0182.

- Information collected on the CFPB FBI Name Check Request – Advisory Board form is approved by OMB ICR 3170-0037 Application for the Bureau's Advisory Committees.

The CFPB FBI Name Check Request – Expert Witness form is exempt from PRA requirements as, in general, criminal investigations do not require OMB approval.

Privacy Risk Analysis

The collected information includes PII and details about an individual's professional background, personal background, credit history, and criminal history. If exposed, this information significantly raises privacy risks such as identity theft, and can cause public embarrassment, loss of reputation, or loss of current employment. Further, the manual submission of completed forms increases the risk of exposure during transmission, and errors associated with inputting the data manually in to ABIS. These risks are present at each stage of the data lifecycle, from collection of the data, use of the data to include disclosure of the data, and retention of the data. This PIA examines these risks and measures that the Bureau implements to mitigate these risks. The Bureau's Privacy Program has considered system privacy controls that mitigate primary risks associated with ABIS related to the following privacy principles:

Data Quality and Integrity

There are four primary methods for collecting information from individuals; through manual collection via Form 306, the CSPP and the CFPB FBI and Expert Witness Name Check forms, through electronic collection via the ABIS-EIC, and through a manual Bureau intra-agency request. The manual processes require individuals to complete PDF forms and submit the documents via email to the Bureau. This information must be inputted into the ABIS system by a Bureau employee, introducing the risk of input errors. These errors could lead to an incomplete or delayed background investigation as the accuracy of information provided to OPM is essential to clearly identify the individual subject to the background investigation process. The Bureau has taken measures to reduce this risk by:

- Introducing the ABIS-EIC component for collecting contractor candidate information. The component provides an electronic collection of information that contractor candidates can access through a web-based interface secured by a multi-factor authentication (MFA) process. The Bureau is evaluating expansion of this submission method for all individuals.

- For manual collection through forms and through intra-agency requests, copies of all forms and emails are uploaded into ABIS as part of the candidate record. In the event of an error inputting information into ABIS, the Bureau may consult with the candidate to verify that their information is accurate.

Security

Given the content and sensitivity of information held within ABIS, the data may be a target for unauthorized access and/or risk insider threats. Information within ABIS is therefore subject to the appropriate technical, physical, and administrative controls implemented through the Bureau's National Institute of Standards and Technology (NIST) based risk management process which identifies risk, analyzes the risk, prioritizes the risk, and develops plan to remediate the risk. It is through these processes that controls such as encryption for data maintained within the system are implemented to reduce overall risk to the data within the system. NIST control families, including Identification and Authentication (IA), Risk Assessment (RA), and Systems and Communications Protection (SC) controls, will be implemented to restrict access to the information to only authorized staff.

Individual Participation

ABIS collects a comprehensive amount of data that includes PII elements, professional history, personal history, credit information, education history, etc. The information is used to determine the suitability of an individual for a role within the Bureau, and this may result in an adverse conclusion, such as a previously undisclosed criminal record or credit history concern. Such adverse conclusions could result in a denial of employment or a position at the Bureau. This may be the result of an incorrect piece of information or the incorrect identification or alias of an individual as part of the background information. The Bureau is required to notify individuals to find out what information about him or her is in a record and how it is used, and for an individual to correct or amend their records. In the event of an adverse conclusion, the Bureau will notify the individual of the investigation outcome, and the specific adverse event, along with a process for the individual to respond to the conclusions by providing a method to correct information or to provide an explanation of the conclusion for further consideration. Furthermore, individuals may request from the Bureau the records that contain their information within the context of the routine uses published in the applicable SORNs, and as authorized under applicable laws.

Limits on Uses and Sharing of Information

Given the amount of information and the sensitivity of the PII there are risks that the information may be used for unauthorized purposes. The Bureau mitigates these risks by implementing access controls within ABIS to ensure only authorized Office of Security staff have access to the information. Further only Bureau Personnel Security Staff (per discussion in the sections below) can share the information with DCSA via OPM and GSA, and this sharing is limited to DCSA and GSA for the purpose of conducting background investigation and fingerprint check processes. The sharing is consistent with routine uses identified within the SORNs referenced above and Interagency Agreement (IAA) – Agreement Between Federal Agencies (FMS 6-10 7600A/B) forms that are renewal annually between the Bureau, OPM, and GSA.

The Bureau considered other privacy principles and determined that they do not pose a notable risk. For example, data minimization is not a risk as the information collected is the minimum amount required by OPM in order to accurately identify an individual and complete a background investigation. The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate.

Privacy Risk Management

1. Describe what information the CFPB collects, how the information is collected, and the sources from which the information is collected.

Information is collected directly from individuals who perform several roles in support Bureau operations, including Federal employees, contractors, expert witnesses, Director's advisory board members, interns, and detailees. Information is collected from individuals through four methods:

- Employees and Interns: Candidates for Federal employment or an internship complete Optional Form (OF) 306, Declaration for Federal Employment, as part of the employee hiring package provided by the Bureau's Administrative Resource Center (ARC). This form is completed by the candidate and then mailed or emailed to the ARC. The form is then provided to Office of Security, and the information is manually entered into the ABIS system by authorized Security Personnel Staff. The information collected includes SSN, place of birth, full name, citizenship status, copy of passport (if necessary); date of

birth, maiden name and nicknames used, phone numbers, selective service registration, military service history, background information, declaration of relatives who are employed by the Bureau, and signature. Specific to intern candidates, school transcripts are also collected and uploaded into ABIS for review by Personnel Security Staff.

- Contractors: Contractor candidates will utilize the ABIS-EIC, which allows an individual to submit their data in an electronic format directly into the ABIS system without the use of a physical form. Upon the award of a contract, the Bureau Contracting Office Representative (COR) will reach out to the contract awardee which will provide the contractor's name, phone number, email address, and role the contractor will perform on the project. This information is entered into ABIS by the COR. Personnel Security Staff then employ a third-party MFA process to securely provide the contractor candidate a PIN number and a secure weblink for accessing the EIC so the candidate can verify their identity and submit their PII electronically. This MFA process only uses a contractor's email address or phone number to either email, text, or leave a voicemail with the PIN. Once the individual is authenticated into the EIC, the information collected includes SSN, date of birth, copy of passport (if necessary); full name, birthplace to include city and state, citizenship, email address, home street address, and home city and state with zip code. Once the contractor candidate submits their information, the EIC component electronically uploads the information into ABIS. The EIC component does not retain the information and does not further communicate with the contractor candidate after the information is uploaded into ABIS. All records within the EIC component are automatically deleted once transmission of the data into ABIS is complete. The MFA process provides some capability for the Bureau to verify and authenticate that the form is being completed by the correct candidate.
- Advisory Board Members: Director advisory board member candidates must complete the FBI Name Check Request – Advisory Board form as part of the Bureau's board member onboarding package provided by the Director's External Affairs Office. The information collected through the form also includes name of Advisory Board for which the individual is applying, full name, SSN, date of birth, place of birth, citizenship status, country of citizenship, present employer, data of employment start, employer phone, and other relevant identifying information. The information provided is inputted into ABIS, and then authorized Personnel Security Staff access DCSA via the OPM NP2 to initiate the FBI Name Check process. DCSA then submits name check requests to the FBI in

order to determine an individual's suitability and eligibility in seeking employment with the federal government. The results of the FBI Name Check process are submitted to DCSA, and then provided to the Bureau via OPM e-Delivery directly into ABIS. Personnel Security Staff also access the GSA USAcess to initiate a fingerprinting check process. Once the individual's information is entered into USAccess, the individual receives an email from the Bureau HSPD12 Admin with instructions to select a place to enroll fingerprints. Once an individual completes the fingerprint enrollment process, the Personnel Security Staff release the fingerprints in the GSA USAccess system to DCSA. DCSA submits the fingerprints to the FBI. The FBI results are then transmitted to DCSA who them releases the results to the Bureau via Connect:Direct. Once complete Personnel Security Staff review the information to determine the suitably of the individual.

- Expert Witnesses: Similar to Advisory Board Members, Expert Witness candidates must complete the Federal Bureau of Investigation (FBI) Name Check Request – Expert Witness form as part of the Bureau's onboarding package provided by sponsoring office. The information collected through the form also includes email address, full name, SSN, date of birth, place of birth, citizenship status, country of citizenship, present employer, data of employment start, employer phone, and residential address. The information provided is inputted into ABIS, and then authorized Personnel Security Staff access DCSA via the OPM NP2 to initiate the FBI Name Check process. DCSA then submits name check requests to the FBI in order to determine an individual's suitability and eligibility in seeking employment with the federal government. The results of the FBI Name Check process are submitted to DCSA, and then provided to the Bureau via OPM Connect:Direct directly into ABIS. If the FBI name check results are not received within 10 business days, the sponsor is offered the option of processing a fingerprint check to get an approval sooner. If yes to fingerprint process, the Once the individual's information is entered into USAccess, the individual receives an email from the Bureau HSPD12Admin with instructions to select a place to enroll fingerprints. Once an individual completes the fingerprint enrollment process, the Personnel Security Staff release the fingerprints in the GSA USAccess system to DCSA. DCSA submits the fingerprints to the FBI. The FBI results are then transmitted to DCSA who then releases the results to the Bureau via Connect: Direct directly into ABIS. Once complete, Personnel Security Staff review the information to determine the interim suitably of the

individual. Personnel Security Staff also access the GSA USAcess to initiate a fingerprinting check process. One the individual's information is entered into USAccess, the individual receives an email from the Bureau HSPD12 Admin with instructions to select a place to be fingerprinted. Once an individual completes the fingerprinting process, the results are submitted to the Bureau via USAccess. Once complete Personnel Security Staff review the information to determine the interim suitably of the individual.

- Detailees: Bureau detailee candidates provide information upon request by ARC via their current federal agency employer. ARC sends an email to the Bureau Office of Security point of contact of the federal agency where the candidate is currently employed and requests the name, SSN, date of birth, current employment status, investigation type and completion date, and adjudication date of the most recent background investigation. All information submitted to the Bureau Office of Security and the information is manually entered into the ABIS system, and copies of all forms or email received by the Office of Security about the candidate are uploaded and added to the individual's record in ABIS.

The information collected from each of these sources is inputted into ABIS as a record. Copies of the forms and emails that contain the information are also uploaded into ABIS and attached to the individual's record. Once the information is uploaded into ABIS, Personnel Security Staff access the OPM NP2 portal to first check the CVS to see if a candidate currently has a recent complete background investigation. If a recent, complete background investigation does not exist, the Personnel Security Staff will initiate the appropriate background investigation process. If the candidate has a completed and suitable background investigation, the Personnel Security Staff manually records the date and type of the completed investigation into ABIS to adjudicate the candidate's suitability on reciprocity. The Personnel Security Staff also takes a screenshot of the CVS/PIPS record which is also uploaded into ABIS and added to the candidate's record. If the individual does not have a complete and active investigation, the Personnel Security Staff accesses e-QIP via the OPM NP2 e-QIP system to initiate a background investigation as describe above.

Upon successful completion of the background investigation, the Bureau is notified via the NP2 system. The NP2 sends an email to the Personnel Security Staff and electronically transfers the results of the investigation via Connect:Direct directly into the candidate's record in ABIS. OPM also provides fingerprints results via Connect:Direct directly into ABIS. The Bureau's Personnel

Security staff review the results and then decide on the suitability of the individual based upon the results of the background investigation, suitability factors and security requirements related to the position. Personnel Security Staff enters the adjudication determination into ABIS and ABIS sends an automated email to the employee notifying them of the final adjudication determination. The adjudication determination is uploaded into the OPM messaging system for processing.

In certain cases, the background investigation results may reveal possible suitability concerns such as financial issues or a criminal record. Upon review of the issue, the Personnel Security Staff may decide to communicate via email directly with the subject to request resulting documentation of the issues that were reveal in the background investigation. All correspondence with the subject is uploaded into the subject's ABIS record.

The information collected through each method described above is the minimum amount necessary to adjudicate or complete background investigations. Each PII element is required to accurately identify the individual in order to perform the appropriate background investigation, and to accurately characterize the individual's background and suitability. The purpose of ABIS is to secure information on a subject background investigation and manage the investigation process, which requires sharing of PII with DCSA via OPM and GSA. No information is collected via a third party and no PII is available through public use of third-party websites or applications associated with ABIS or its components.

2. Describe CFPB's objective for the information.

ABIS provides the Bureau with a centralized system for the collection of information from individuals who are candidates for Bureau employment, internships, contract support, advisory Board Member participation, and detailees. The sole use of this information is for Bureau Personnel Security Staff acting as adjudicators to determine an individual's suitability, employment fitness, and/or for eligibility and access determinations, and to ensure that any person employed or supporting the Bureau is reliable, trustworthy, of good conduct and character, and loyal to the United States. To make these determinations the Bureau must collect the minimum amount of data required by DCSA to determine if a favorable, complete background investigation has recently been conducted, or to initiate a background investigation for a candidate.

The Bureau collects the minimum amount of information required by the OPM to determine if a recent and favorable investigation has been completed for use in determining suitably with the

candidate, in accordance with 5 C.F.R. parts 2, 5, 731, 732, 736, and 1400 that establishes the requirements for agencies to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions. Depending upon the scope of the particular background investigation for the Bureau candidate, OPM is authorized to collect information under Executive Orders 9397, 10450, 10577, 10865, 12333, 12968, 13467 as amended, 13488, and 13549; 5 U.S.C. §§ 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. §§ 272b, 290a, 2519; 31 U.S.C. §§ 1537; 42 U.S.C. §§1874(b)(3), 2165, 2201, and 20132; 50 U.S.C. § 3341; Public Law 108-136; and Homeland Security Presidential Directive (HSPD) 12.

In accordance with these laws, regulations, and guidance listed the Bureau must collect enough PII to accurately identify the individual, including details about their personal and professional background and history. For example, SSN is collected to keep records about the individual accurate with ABIS, as individuals may share the same name and birth date, making it otherwise difficult to clearly identify one individual from another to complete a background investigation.

Outside of the stated purpose above, PII is not used for any other purpose.

3. Describe how CFPB shares any of the information with third parties with whom the CFPB shares the information for compatible purposes, e.g. federal or state agencies, the general public, etc.

The Bureau collects information from the sources mentioned above and inputs the information into ABIS (apart from EIC, where information is electronically collected and uploaded into ABIS). Once the information is in ABIS, Personnel Security Staff log into NP2 portal and manually enters information from the ABIS record into the appropriate system. If the candidate has a completed and suitable background investigation active within CVS/PIPS, the Personnel Security Staff records the date and type of the completed investigation into ABIS and accepts on reciprocity the suitability determination, and takes a screenshot of the PIPS system record which is also uploaded into ABIS and added to the subject's record. If the subject does not have a recently completed and favorable investigation, then Personnel Security Staff initiates a request within the e-QIP system. Personnel Security Staff also initiates a fingerprint check process via USAccess. When the background investigation and fingerprint check is complete, OPM will submit the results via NP2 into ABIS using OPM's Connect:Direct and e-Delivery, which are electronic delivery methods of closed and complete OPM investigation files in a secure manner, eliminating the need to mail hard copies of investigative files to the Bureau.

The purpose of collection and sharing of this information by the Bureau is covered by and consistent with the routine uses published in OPM SORN GOVT-1, General Personnel Records, and OPM SORN OPM Central-9, Personnel Investigations Records, for the purposes of collecting relevant PII to identify the individual, inform the source of the nature and purpose of a background investigation, and to identify the type of information requested.

4. Describe what opportunities, if any, individuals to whom the information pertains have to (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

The publication of this PIA, OPM SORN GOVT-1, General Personnel Records, and OPM SORN OPM Central-9, Personnel Investigations Records, provide notice to the public on the intended purpose and use of PII that is submitted as part of background investigations.

In addition, notice and consent are discussed specific to certain collections of information from candidates:

- Individuals applying for Bureau employment or an internship complete OF 306, Declaration for Federal Employment, as part of the hiring package provided to the candidate by the Bureau. The Instructions and Privacy Act Statement sections of the form provides notice to individual that answers must be truthful and complete. Information, including SSN, is collected to keep records accurate and help identify individuals in agency records. The submission of this information is voluntary, however, if accurate and complete information is not provided the application for background investigation cannot be completed.
- Contractor candidates complete an electronic form via the ABIS-EIC component. The electronic form provides a Privacy Act Statement that the information submitted via the form will aid in the completion of a background investigation. Submission of the information is voluntary, however, failure to submit this information does not allow the subject to begin the background investigation.
- Board Member candidates complete the CFPB FBI Name Check Request – Board Member form. The form provides a Privacy Act Statement stating that providing information, including an SSN, is voluntary, however failure to provide the information may affect the completion of the background request. By signing and submitted the form, the candidate

provides consent to disclosure to other federal agencies to aid in the background investigation.

- Expert Witness candidates complete the FBI Name Check Request – Expert Witness check form. The form provides a Privacy Act Statement stating that by providing information, including an SSN, is voluntary, however failure to provide the information may affect the completion of the background request. By signing and submitted the form, the candidate provides consent to disclosure to other federal agencies to aid in the background investigation.
- Detailee candidate information is provided to the Bureau by the candidate's current federal agency employer. The notice and consent to submission of candidate information is handled by the federal employer prior to the submission of candidate information to the Bureau. The Bureau does not provide further notice or consent for the collection of this information.

The Bureau gives individuals the ability to request access and amendment to their personal information in accordance with the Privacy Act and the Bureau's Privacy Act regulations, at 12 C.F.R. 1070.50 et seq. As it pertains to OPM investigative processes, in accordance with OPM SORN OPM Central-9 individuals may contact the Federal Investigative Offices of OPM. Please review the SORN for further information on procedures and certain exemptions specific to these processes.

5. Explain the standards and relevant controls that govern the CFPB's—or any third-party contractor(s) acting on behalf of the CFPB—collection, use, disclosure, retention, or disposal of information.

A full security review of ABIS has been conducted by the Bureau based on all applicable federal laws, directives, and standards. The Bureau has developed and followed a Security Implementation Plan (SIP) identifying the necessary security and privacy controls that govern the collection, use, and maintenance of PII within the system. Additionally, ABIS will receive an Authority to Operate (ATO) in accordance with Bureau policies and NIST guidance.

The Bureau issues authorized personnel access to the system following the Bureau's User Access Request process. Some users may also include authorized Bureau contractors. Employees and contractors must complete system training, including confidentiality and privacy briefings, prior to being granted access to ABIS. Users will be granted roles based on their need to perform

development and maintenance, and access to PII within these roles will be strictly review, approved, and monitored by the system owner. The Bureau uses the following technical and administrative controls to secure the data and create accountability for the Bureau's appropriate collection, use, disclosure, and retention of the information:

- Implementation and assessment of applicable NIST 800-53 control(s) to ensure privacy controls are in place to protect PII.
- Reviews of system audit logs to validate authorized access and identify potential unauthorized access to PII.
- Annual Bureau Personnel Privacy Training is required for all employees and contractors, to include those that support ABIS.
- A Bureau Privacy Breach Response and Recovery Plan is in place in the event a breach of information is identified.
- Compliance with Bureau privacy policy and procedures is monitored consistent with the Bureau's Privacy Continuous Monitoring Plan.
- Data Quality and Integrity Checks are performed in accordance with the Bureau's Data Access Policy.
- Role-based Access Controls: Access to the system is strictly governed by the system owner and requires program approval prior to access being granted to the system. Any access granted to authorized individuals is reviewed periodically to determine if access is still required, and if not, disabled and removed.
- Background checks of contractors and federal employees are completed prior to granting access to the ABIS system.

Specific to role-based access, the following users will have access to information collected and maintained by ABIS:

- Bureau Office of Security Users (full time employees and contractors) have access to ABIS to review records within the system and manage the background investigation process. Specific to sharing the information with OPM, Personnel Security Staff have access to ABIS records to check on the status of background investigations or initiate background investigations.
- Developers (full time employees and contractors) have access to the system to develop enhancements to the system, such as the development of the ABIS-EIC component. Developers do not have access to records or PII within the system and cannot make

changes to the system that affect records or PII within the system. Upon finalization of an ABIS development project, Developers provide the project to the Release Management Team and Developer access to the system is disabled.

- Business Analysts (full time employees and contractors) work with development teams to configure data flow and conduct user acceptance testing (UAT). Business Analysts generally do not have access to records or PII within ABIS and cannot make changes to the system that affects records or PII within the system. However, Business Analysts may request access to records or PII within ABIS when testing development projects within ABIS. To gain access Business analysts must be granted access to records and PII within ABIS by the system owner, stating the specific purpose for the access. Once the purpose is completed, this access is no longer required, access is removed.
- Release Management Team (full time employees and contractors) has access to records and PII within ABIS when required for moving an approved development project into production within ABIS. Access is granted by the system owner based upon the requirements for the release of the development project to production, and once this purpose is complete access is removed.
- System Administrators (full time employees and contractors) have full access to the system, including records and PII. System administrators are considered privileged users and as such will have access to all data in the system, including PII, for the purposes of controlling, monitoring, and other administrative functions. These system administrators have elevated access within the system, which have been approved by the system owner, as well as the Information Security owner.

The Bureau maintains ABIS records in accordance with the National Archives and Records Administration (NARA) approved General Records Schedule (GRS) 5.6 Security Records, Items 180 and 181. For records of people not issued clearances (including case files of applicants not hired) the records are to be destroyed after one year after consideration of the candidate ends, but longer retention is authorized if required for business needs. For records of people issued clearances, the records should be destroyed 5 years after the employee or contractor relationship ends, but longer retention is authorized if required for business use.

There are no disclosure avoidance techniques or standards established in disclosing information to OPM to aid in the background investigation process. OPM prescribes a specific process and minimum data requirements by federal law and regulations that prevent the Bureau from employing techniques such as masking partial digits of an SSN.

As a result of conducting this PIA, the Bureau is investigating the expansion of employing additional ABIS components, such as ABIS-EIC, which improves the security and privacy of candidate PII by streamlining the information submission process, thereby reducing the reliance on manual submission of forms.

6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf of the CFPB, e.g., government contractors discussed in Question 5.)

The Bureau shares collected background information with OPM to aid in the background investigation process. Personnel Security Staff are granted access to the OPM NP2 portal by OPM for the purposes of reviewing active or recently completed background investigations, or to initiate a background investigation. Access to the NP2 portal is strictly managed by both OPM and the CFPB Personnel Security Office. Any disclosure of information to OPM is manually submitted via the NP2 portal. OPM restricts access to forms and fields to the minimum necessary for Personnel Security Staff to input the minimum amount of data required to perform authorized activities. Bureau background investigations activities are governed by Office of Personnel Security policy and standard operating procedures for performing all background investigation roles, to include the disclosure of information to OPM.

Following a similar submission process, the Bureau shares collected background information with GSA to aid in the background investigation process. Personnel Security Staff are granted access to the USAccess by GSA for the purposes of initiating fingerprinting checks. Access to the USAcess is strictly managed by both GSA and the Bureau. Any disclosure of information to GSA is manually submitted via USAaccess. GSA restricts access to forms and fields to the minimum necessary for Personnel Security Staff to input the minimum amount of data required to perform authorized activities. Bureau background investigations activities are governed by Office of Personnel Security policy and standard operating procedures for performing all background investigation roles, to include the disclosure of information to GSA.

Specific to contractor candidates who are subjects of investigation, the Bureau employs a third-party MFA process to securely provide the contractor candidate a PIN number and a secure weblink for accessing the EIC so the candidate can verify their identity and submit their PII

electronically. This MFA process only uses a phone number to either text or receive a voicemail with the PIN.

Document control

Approval

Christopher Chilbert

Chief Information Officer

Date

Christopher Chilbert

Digitally signed by Christopher Chilbert
Date: 2021.03.26 12:09:39 -04'00'

Tannaz Haddadi

Chief Privacy Officer

Date

TANNAZ HADDADI

Digitally signed by TANNAZ HADDADI
Date: 2021.03.26 12:13:56 -04'00'

Kathleen Horan

Personnel Security Team Lead

03/25/2021

KATHLEEN HORAN

Digitally signed by KATHLEEN HORAN
Date: 2021.03.25 21:44:34 -04'00'