Federal Bureau of Investigation

Privacy Impact Assessment
for the

FBIJobs.gov and FBI Candidate Gateway (CG)

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: September 30, 2022

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The FBIJobs.gov and Candidate Gateway (collectively known as "FBICG") supports the Federal Bureau of Investigation (FBI)'s public-facing recruiting, hiring, and the job application and staff reviewing processes. The system allows individuals, using the Internet, to research, submit interest, apply for, and receive communications about FBI employment. The FBICG also integrates with several Human Resources Branch (HRB) systems, including HR Source (which resides on FBINet, the Bureau's secure network), by means of an accredited Cross Domain Solution (CDS). FBICG consists of FBIJobs.gov, the website for general FBI employment information, and Candidate Gateway (CG), the job application submission website.

This PIA is conducted pursuant to Section 208 of the E-Government Act of 2002, P.L. 107-347, which requires that agencies conduct PIAs on information technology systems that collect and maintain personally identifiable information (PII) about individuals. A PIA required for FBICG because it contains sensitive but unclassified PII about individuals applying for FBI employment including, but not limited to: name, Social Security number (SSN), and date of birth (DOB); eligibility for veterans preference; gender, and citizenship.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

Information collected and maintained by FBICG supports the FBI's recruiting, hiring, and job application and staff reviewing processes. FBICG is web-based, meaning it is accessible from the Internet. It is hosted on virtual machines, without physical hardware, provided by Amazon Web Services Government Cloud (AWS GovCloud). To achieve its purpose, FBICG employs the following: public-facing websites by which end users access FBICG; integration with HR Source to complete the FBI's hiring process; and a PeopleSoft[1] database for storing FBICG data. FBICG will primarily operate using three software products: Oracle PeopleSoft HRS 9.2, Oracle Database 19c, and Drupal. Both Oracle products are commercial off the shelf (COTS) software; Drupal is an open-source content management platform that will be used to create and manage the FBIJobs website.

As noted above, the FBIJobs.gov public website is accessible via Internet. FBIJobs.gov contains general FBI employment information viewable by all site visitors and will not include PII. The home page contains links to information for potential applicants, students, and veterans, among others who may be interested in learning more about positions at the FBI. FBIJobs.gov also contains links that route to the CG secure portal for job application submissions.

[1] Peoplesoft is a suite of applications owned by Oracle Corporation that are designed to address complex business requirements.

CG is a sub-domain of FBIJobs.gov. It is accessible via FBIJobs.gov or www.apply.fbijobs.gov. It allows internal and external candidates to search, apply for, and track job opportunities. It also operates on FBINet, allowing internal candidates to apply for positions available only to FBI employees. It provides step-by-step guidance to help applicants successfully complete and submit their applications to job postings.

Individuals wishing to access the CG portal must first create a user account with a unique username and password, and a user profile containing basic contact information such as name, address, telephone number, and email address. They can also "opt in" if they wish to receive text and email messages.[2] They can later choose to opt out if they no longer wish to continue receive messages.

Once logged in, CG users can:

- Search FBI postings / Save search queries / Save jobs;
- Apply to a job posting;
- Upload supporting documents needed during the job application process; and
- Respond/View communications from a recruiter or staffing professional at the FBI (communications may include requests to complete a questionnaire, status updates, canned and ad-hoc email messages, or job offers).

The CG maintains (a) general information pertaining to FBI employment, including position descriptions and postings, that may be viewed by any general user at any time; (b) PII provided by users applying for a talent pool or applying for employment;[3] and (c) aggregate statistical data for web performance measurement, customization of web visitor experience, and website improvements, using Google Analytics and Google Tag Manager, as discussed later.

Information entered by a user is encrypted and stored within the FBICG portal. Applicant information is temporarily stored in the system when an applicant creates an account in FBICG and begins to enter their personal information. Once an applicant submits a completed job application, PII is ultimately transferred across domains to the FBINet and into HR Source, where the information is accessible by FBI Human Resources Division (HRD) personnel and retained in accordance with a National Archives and Records Administration-approved records retention schedule. After the data has been transferred from the FBICG to the HR Source, the PII is purged from the FBICG system, limiting the time an individual's PII is contained in the FBICG.[4] If an individual is selected and hired, the information provided on the job application in FBICG becomes a part of their employee record and may be used for administrative purposes until their retirement.

On the classified domain, CG is accessible via HR Source for FBI employees only. FBI employees automatically have an HR Source account, which is linked to the FBINet CG module. Therefore, they

---

[2] As used herein, the term "user" refers to individuals who have registered for a user account on the CG portal. These individuals are considered "general" (i.e., non-privileged) system users and have access to only PII they provide via the portal. The limited number of FBI personnel with access to FBICG, serving as system administrators, are "privileged" users of the system.

[3] As used herein, the term "talent pool" refers to users who have provided the FBI, through the CG, with information about their employment qualifications to be considered for future job vacancies.

[4] The period of time for which PII may remain in the FBICG, for purposes of verifying the integrity of data transferred to the HR Source, is one year from the point the user is no longer accessing or reviewing posting and application information.

can browse and select job postings, and complete and submit job applications without creating an additional user profile in CG.

FBICG populates HR Source, specifically: vacancy creation and posting, talent sourcing, job application evaluation, applicant selection, sending job offers and internal transfer orders, and hiring. Several times daily, information pertaining to FBI employment, vacancy announcements, employment applications, screening, rating and selection functions is transferred between the FBICG (residing on the Internet) and the HR Source (residing on FBINet) via separate one-way CDS. The data elements transferred between the two domains consist of:

<u>High Domain to Low Domain Transfer</u> (i.e., from HR Source to FBICG)

- Posting information
- Application Data
- Employment-related questionnaires
- Email communications from FBI recruiters or HRD staff to users (i.e., applicants/potential recruits)
- Responses to email communications from users
- Offers and Transfer Orders

<u>Low Domain to High Domain Transfer</u> (i.e., from FBICG to HR Source)

- CG user account profile data (Name, Address, Telephone, etc.)
- Completed applications
- Completed employment-related questionnaires
- Email messages sent by users to FBI recruiters or staffing personnel
- Offers and Transfer Orders

To initiate a job posting, hiring managers submit a Human Resources Exchange (HRX) form online through HR Source. Once the HRX form is submitted and approved, a talent specialist creates the vacancy announcement. Job opening information is transferred from FBINet to UNet via CDS and posted directly to the public CG website. Some positions that are open to internal FBI candidates only, like Voluntary Rotational Transfers, are posted to the CG module within HR Source on FBINet. Once a posted job vacancy has closed, talent specialists use HR Source to complete the hiring process, notify the hiring manager, and generate a conditional job offer for the candidate. The CDS transports the job offer from HR Source to CG. Talent specialists also use HR Source to generate and transport final job offers from HR Source via CDS to CG. Again, the transactions that occur between HR Source and the CG module on HR Source do not move via CDS because they exist in the same domain. Additional details are provided in the HR Source privacy documentation.

FBIJobs.gov and CG websites use Google Analytics and Google Tag Manager[5], which are free,

[5] Google Marketing Platform, which includes Google Analytics and Google Tag Manager, was approved under the OCIO's Procurement Risk Assessment (PRA) process. The PRA process involves OCIO, Security Division, and Finance and Facilities Division assessing potential threats and risks and mitigation steps associated for each product. Mitigation steps and recommendations may include but are not limited to: scanning for malicious codes in a test environment or sandbox

external, third-party hosted, website solution that collects data that can be used for website performance measurement, customization of user experience on the website, and improvements to the website. Google Analytics also provides a dashboard view and analytical reports discussed later. FBI does not use Google Analytics to track individual user-level activity on the Internet outside of the FBICG websites; or cross-reference any data gathered from Google against PII to determine individual user-level online activity. Google will not access or use data collected on FBICG for commercial purposes.

Google Tag Manager provides a snippet of code, such as Google Analytics tracking code, to incorporate into FBICG and FBIJobs.gov code that places a web beacon on the FBIJobs.gov or FBICG page.[6] Web beacons are sent out remotely via a Google Tag Manager page. When a user then "starts" an application on FBICG, the web beacon collects the below anonymized data. Limited HRB personnel may access aggregated statistical data based on the following data, but the FBI does not have access to individual user data:

- The internet domain name;
- The originating Internet Protocol (IP) address: although the full IP address may be collected initially, Google anonymizes it prior to use and storage, and only stores a truncated IP address. Google will only provide the FBI non-identifiable aggregated information in the form of custom reports.
- Information about the visitor's computer or mobile set-up (e.g., type and version of web browser, operating system, screen resolution, and connection speed);
- The pages on FBICG visited (i.e., starting an application, the pages of the application that are filled out, when the application is submitted, and any interactions such as links clicked within the site with);
- The internet address, or URL, of the website that connected the visitor to FBICG, if he or she accessed via a link on another page (i.e., "referral traffic");
- The amount of data transmitted from FBICG to the visitor's computer;
- Job opening numbers for which applicants are applying;
- Applicant ID number with which users have logged into the system with to avoid double-counting report totals (e.g., a user may visit the application page using different devices, resulting in inaccurate statistics). Google does not have access to nor does it collect any other information that would link applicant ID numbers to individual profiles.

In addition to adding a web beacon on FBIJobs.gov and FBICG websites, a web beacon will be added to emails that are sent to a) applicants that apply to jobs; or b) have submitted interest in applying via a form on apply.fbijobs.gov and have voluntarily provided their email addresses to be contacted about upcoming events or jobs that meet their interests. Users consent before they submit their interest/application forms. A web beacon would be added into the HTML of the email, and it will send data from the email to the Google Analytic servers. The web beacon is intended to measure the effectiveness emails by tracking if the email was received or bounced back due to an incorrect email

---

before installing on FBI network; purchasing, installing, or updating the most recent or secure version; allowing only authorized personnel use of OSS; following security best practices to identify, protect, and respond to security incident(s). If the PRA process is successfully completed, OSS is authorized to be procured.

[6] A web beacon is a minute image on the display screen, which is transparent to the user, placed in a webpage or HTML email to record when the content was loaded.

address; whether the email was opened; whether links within the email were clicked; and the recipient's email client and internet domain name. Data is collected in aggregate. Limited HRB personnel may access aggregated statistical data based on the data listed below, but the FBI does not have access to individual user data.

Google Analytics makes aggregated data available via a website that allows for user-controlled access. It is displayed in a dashboard for a limited number of authorized HRB personnel to review. The dashboard displays aggregated statistical data, such as percentage breakdown of referring website (e.g., Google, Bing, LinkedIn, etc.), the number of users that have visited the site, and percentage of visits that were conversions (i.e., the visitor completed a task of applying on FBICG or submitting interest) over a period of time (day, week, month, or year). Administrator accounts are created and maintained by team members in HRB. Reports may be shared with the HRB team members, senior leadership, and FBICG's content providers in HRD so they can make better business decisions as to what products they produce. Reports can be exported to an external source (e.g., HR Source) for additional aggregated reporting. Metrics can be shared in an Excel spreadsheet with those individuals who have a need to know with regard to these metrics in the performance of their duties. Other export formats for Google Analytics include PDF, CSV, XML, and TSV.

All captured FBICG and FBIJobs.gov data will only be retained for two months for proper analysis and optimization of the websites. The privacy policy is posted on FBICG and FBIJobs.gov websites along with instructions on how to opt-out of the capture of data via Google Analytics.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	5 U.S.C. § 2103; 28 U.S.C. § 536
Executive Order	E.O. 13571
Federal regulation	5 C.F.R. Part 0.138; 5 C.F.R. Part 302
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	The President's Memorandum on Transparency and Open Government Memorandum (January 21, 2009)[7] and OMB Memorandum M-10-06, Open Government Directive (December 8, 2009)[8] direct federal departments and agencies to harness new technologies to engage the public and serve as one of the authorities for HRB's efforts to use Google Analytics; OMB

[7] *The President's Memorandum on Transparency and Open Government* (Jan. 21, 2009), *available at* https://www.archives.gov/files/cui/documents/2009-WH-memo-on-transparency-and-open-government.pdf.
[8] OMB Memorandum M-10-06, *Open Government Directive* (Dec. 8, 2009), *available at* https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-06.pdf.

	Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010);[9] OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010);[10] OMB Memorandum M-11-24, Streamlining Service Delivery and Improving Customer Service;[11] OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services;[12] OMB Memorandum M-17-06, Google Terms of Service;[13] Google Privacy Policy.[14]

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

FBICG collects a variety of PII related to candidates interested in applying and applicant information as noted in the table below. Audit log information, including IP addresses, internet browsers, dates/times of visit, pages reviewed during visit, and referring sites are also collected and maintained.

The table below only reflects the types of PII that the FBI collects directly from FBICG.

[9] OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* (June 25, 2010), *available at* https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf.
[10] OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf.
[11] OMB Memorandum M-11-24, *Streamlining Service Delivery and Improving Customer Service* (June 13, 2011), *available at* https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-24.pdf.
[12] OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services (Nov. 8, 2016), *available at* https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-06.pdf.
[13] Google Terms of Service is available at: www.google.com/accounts/TOS.
[14] Google Privacy Policy is available at: https://support.google.com/analytics/answer/6004245.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	
Date of birth or age	X	A, B, C, D	
Place of birth	X	A, B, C, D	
Gender	X	A, B, C, D	
Race, ethnicity, or citizenship	X	A, B, C, D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C	
Tax Identification Number (TIN)			
Driver's license			
Alien registration number		D	
Passport number			
Mother's maiden name	X	A, B, C, D	
Vehicle identifiers			
Personal mailing address	X	A, B, C, D	
Personal e-mail address	X	A, B, C, D	
Personal phone number	X	A, B, C, D	
Medical records number			
Medical notes or other medical or health information	X	A, B, C, D	
Financial account information			
Applicant information	X	A, B, C, D	
Education records	X	A, B, C, D	
Military status or other information	X	A, B, C, D	
Employment status, history, or similar information	X	A, B, C, D	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	
Certificates	X	A, B, C, D	
Legal documents			
Device identifiers, e.g., mobile devices	X	A, B, C, D	
Web uniform resource locator(s)	X	A, B, C, D	
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B, C, D	FBICG allows users to set a user ID for their account
- **User passwords/codes**	X	A, B, C, D	Hash password[15]
- **IP address**	X	A, B, C, D	
- **Date/time of access**	X	A, B, C, D	

[15] Hashing performs a one-way mathematical transformation of a password, turning the password into another string text, called the hashed password that is practically impossible to convert back to the original password.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			For FBIJobs.gov, internet browser; type of the device that accessed the website; and if linked to FBIJobs.gov from another site, the address of that site.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Other federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component		X		Information about potential applicants/recruits in the FBICG cannot be shared within the FBI directly from the FBICG. The data must first be batch transferred from the system across domains to the HR Source, which resides on the Secret Enclave, before it can be accessed by FBI HR personnel.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Privacy Act 5 U.S.C. § 552a(e)(3) notices are displayed throughout FBIJobs and CG. Notice is provided on FBIJobs.gov and is the overarching online privacy policy for the site. Notice is also

provided on CG for users creating an account and starting a job application. Additionally, general notice is provided through the following systems of records notices: OPM/GOVT-5, Recruiting, Examining, and Placement Records, 65 Fed. Reg. 24731 (Apr. 27, 2000), as amended; OPM/GOVT-7, Applicant Race, Sex, National Origin, and Disability Status Records, 71 Fed. Reg. 35356 (June 19, 2006), as amended; FBI-008, Bureau Personnel Management System, 58 Fed. Reg. 51875 (Oct. 5, 1993), as amended; DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999), as amended; and DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 4, 2001), as amended.

The FBICG privacy policy provides notice regarding use of website measurement technology, including instructions on how to opt out. The Google Analytics privacy policy can be found at the following website: Safeguarding your data - Analytics Help (google.com).

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals may decide whether to create a user account on FBICG. Once they create their accounts, users can choose whether, and to what extent, to submit information beyond what is required to create a new account. Further, users voluntarily decide to start and submit a job application. Users may decide not to provide information required by the application; however, those users will not be able to submit an application for employment consideration. Additionally, users are requested to accept Terms and Conditions of Use when they (1) create a user profile; (2) submit basic eligibility questionnaire; and (3) submit an employee application.

When new and existing users are building/updating their accounts, they have the option to opt-in or out of messages that are sent out through FBICG. If users opt out, they will still receive auto-communications related to password resets and when an offer or transfer orders are available for review.

Users are provided directions on FBICG privacy policy on how to opt out of data collection by Google Analytics. Because the information is transferred in aggregate, users will not have the ability to consent to a particular use of the information. However, users can opt out by following the instructions provided in the privacy policy.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals can log into their FBICG account to view information related to their account (applications, application status, profile information, and offers/transfer orders). Individuals can also correct and update their basic contact information on their user profile. Once a job application is submitted, individuals can reach out to their HR point of contact or applicant coordinator to correct

their information.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** October 8, 2021 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** IA-02-E01 – Network Access to Privilege Accounts – the operating system and database level of FBICG can only be accessed via a UNet workstation by a privilege user, which requires the user to authenticate with their username and RSA token/PIV card. The privileged user can then access the backend terminal server with their username and password. The public facing site for public users does not enforce multi-factor authentication so an applicant or candidate's account is only enforced using username and password**.**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Category is High. The system contains information that requires protection from unauthorized disclosure.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The Information System Security Officer (ISSO) will conduct weekly reviews of the security audit logs and a quarterly automatic scan of the entire system will also be performed to ensure system security.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The PeopleSoft System to be used for the FBICG contains built-in auditing and data monitoring capabilities. In addition, all activity occurring on AWS GovCloud network (on which the FBICG will operate) is monitored 24/7 and 365 days for breaches and other

	anomalies. Access and activity logs will be reviewed in accordance with DOJ and FBI policy.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All FBI personnel are required to complete annual information security and privacy trainings.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

FBICG operates on the AWS GovCloud, a secure network accredited to handle at the FedRAMP-High level. No information will be held by FBICG AWS outside of the United States. Information will be logically separated (virtual servers) from the information of other organizations, and only certified Federal Government IT systems are located in the same physical space. The NIST 800-53 security control baseline is anticipated to be at the LOW impact level of assurance. Security controls will be continually assessed during life cycle management for compliance and to ensure appropriate mitigation strategies have been implemented commensurate with the LOW impact level of assurance. In addition, the FBICG system itself has a security layer imposing role-based access restrictions to ensure that only FBI employees with a specific need to know (based on their official duties) can access the system.

FBICG also utilizes a robust auditing capability to protect privacy and to detect any unauthorized access to the system. The specific activities or events audited in FBICG are successful and failed logons and logoffs, acceptance of electronic banners and warnings, requests for access to Reports Server resources, becoming a root or a privileged user, and any changes in a user's access permissions. Application level audit trails are kept according to applicable records management policies, but in no event will retention be less than 90 days. Audit logs are reviewed weekly by the system ISSO. A quarterly automatic scan of the entire system is also performed to ensure system security.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

User account data (e.g., user name and password) are retained in the CG indefinitely, to allow individuals to more readily apply for subsequent FBI employment vacancies. Other PII contained in employment applications and supporting documents is batch transferred from the system across

domains to HR Source daily. Information transferred to HR Source will be retained in accordance with applicable records retention disposition schedules, as noted in the HR Source privacy documentation. If an applicant has an inactive job application, all PII (other than the user account data) from the application will remain in the FBICG system for up to one year for purposes of data integrity verification and then will be automatically purged from FBICG.

Additionally, the following records retentions schedules apply:

Record Type	Disposition Information
Information related to FBI job description	Destroy after 2 years after position is abolished or description is superseded, but longer retention is authorized if required for business use.
	Destroy when position description is final but longer retention is authorized if required for business use.
Information related to FBI organization and management	Destroy when superseded, obsolete, or no longer needed for business, whichever is later.
Information related to hiring and recruitment	Various dispositions

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

The information contained in the FBICG is encompassed by published Systems of Records Notices for the following systems: OPM/GOVT-5, Recruiting, Examining, and Placement Records, 65 Fed. Reg. 24731 (Apr. 27, 2000), as amended; OPM/GOVT-7, Applicant Race, Sex, National Origin, and Disability Status Records, 71 Fed. Reg. 35356 (June 19, 2006), as amended; FBI-008, Bureau Personnel Management System, 58 Fed. Reg. 51875 (Oct. 5, 1993), as amended; DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999), as amended; and DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 4, 2001), as amended.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation

measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

Because FBICG collects significant amounts of sensitive PII about applicants and employees, privacy risks associated with the collection, use, access, dissemination, and maintenance of this information include unauthorized access, misuse, and disclosure. Further, disclosure of FBICG information might compromise the identities of individuals applying to positions at the FBI.

Unauthorized access and unauthorized disclosure to potential candidates' PII are mitigated through role-based access control and regular purging of application-related PII. Individuals wishing to apply for FBI employment can create user accounts and may view information contained in their user profile and job applications, but will not be able to access information about other individual users. The PII in the CG is accessible only by the individual user who provided the information and by a handful of HRB administrators responsible for support and maintenance of the system. Other HRD personnel, including Talent Specialists, do not have access to CG itself.

The PII within the system is encrypted both while in transit and while at rest in the system's database. While user accounts remain active indefinitely, PII provided as part of an application is purged from the CG database at regular interval, reducing the time the data is exposed to possible compromise while within the system.[16]

To ensure the integrity of data and software within the FBICG, system backups and audit logs are maintained. System backups ensure that data is recoverable in the event of a disaster. Audit logs provide a trail identifying who has accessed the system, what they have accessed, and when the access occurred. Audit logs, which cannot be modified, will be reviewed weekly by the ISSO. A quarterly automatic scan of the entire system is also performed to ensure system security. All activity occurring on the AWS GovCloud network (on which the FBICG will operate) is monitored 24/7 and 365 days for breaches and other anomalies. Access and activity logs will be reviewed in accordance with DOJ and FBI policy

The risk of PII misuse is mitigated because privileged users must acknowledge their responsibilities to protect PII prior to receiving access to the system by signing the FBI Information Technology and Information Systems Rules of Behavior for Privileged Users (Form FD-889a). These forms remind personnel that they are prohibited from accessing PII about other United State spersons contained in FBI (or other government information systems) unless they have a valid need-to-know pertaining to the information to carry out authorized tasks or perform mission-related functions. Users also

[16] As discussed above, application related PII ultimately reside in the HR Source after being transferred across domains from the FBICG.

acknowledge their obligation to maintain, process, and protect information about other individuals with sufficient care to ensure the security and confidentiality of the information and protect it from inadvertent or unauthorized disclosure. Additionally, FBI personnel receive annual information security awareness training and privacy training.

To minimize risk of unauthorized access to Google Analytics data, only a limited number of pre-approved HR personnel will have access to the Google Analytics dashboard and aggregated data. To minimize any possible privacy risks to visitors to FBICG, FBI will not use Google Analytics to track individual user-level activity on the Internet outside of the FBICG websites; or cross-reference any data gathered from Google against PII to determine individual user-level online activity. Further, FBI will not share Google Analytics data with any of the Google products. This decision to opt-out means that the information is not shared with any Google products (such as AdWords, AdSense). This is set within the Google Analytics settings "Edit Account and Data Sharing Settings." The only information that is available is the aggregated information in the Google Analytics dashboard that is exclusively available to a limited number of HRB personnel. Additionally, FBICG privacy policy provides notice to visitors and includes information on how to opt-out.[17] Google's data protection and safeguarding information is provided on the following website: https://support.google.com/analytics/answer/6004245.

[17] Visitors are provided a link to Google Analytics Opt-out Browser Add-on Download Page.