Drug Enforcement Administration

Privacy Impact Assessment
for the
Firebird General Support System Environment

Issued by:
Robert McGovern
DEA Senior Component Official for Privacy (Acting)

Approved by: Kameron Cox
Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: October 15, 2026

(July 2023 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

Firebird is an on premises/cloud hybrid, General Support System (GSS) environment that is the primary enterprise information technology (IT) infrastructure of the Drug Enforcement Administration (DEA) and is overseen by the DEA Information Systems Division (TC). Firebird GSS supports DEA's Sensitive-But-Unclassified (SBU) information systems that assist more than 16,000 DEA personnel complete their mission. Firebird GSS provides network infrastructure to host multiple internal DEA information systems that reside on Firebird GSS and has several "strictly limited" interfaces/connections to non-Department of Justice (DOJ)/DEA resources or external networks that interface with Firebird GSS (hereinafter "Hosted Systems"); meaning interfaces are controlled through properly configured network security devices. Firebird GSS also maintains several "Core Systems" for information management functionality.

Hosted Systems: The purposes of the systems hosted on Firebird GSS may differ in which aspect of DEA operations is supported, but Firebird as a whole supports the full range of DEA primary business lines: Law Enforcement Investigations and Operations; Diversion Control Operations, Intelligence Activities; Forensic Science Laboratories, the Training Academy, Inspections Division operations; and administrative functions, including TC Division. A listing of each separate application on Firebird can be found in the attached Appendix A. However, any of these "Hosted Systems" that requires a Privacy Impact Assessment will be discussed in separate privacy documentation for each system.

Core Systems: Several applications are contained in Firebird GSS that are integral to its information management function. These core applications control directory and file Services (including the Microsoft Active Directory) that support authentication/authorization of users; monitoring of infrastructure components and mission-critical applications; release management (i.e., deployment of approved operating systems, software, and patches); relational database management functions; and backup and recovery services of individual home directories, shared storage for groups, and files and applications.[1]

Also included as Core systems are Enterprise Storage Management functions; Mobility Services (remote access options and mobile devices); Network Services (connectivity, communication, and management of the Firebird enterprise) and Deskside access (workstations that provide DEA users access to a standard suite of office automation tools and DEA business applications). Additionally, Firebird GSS also hosts DEA's Enterprise-wide operating system, MS Office 365, and included applications MS Word, Excel, and PowerPoint; as well as a slate of various Electronic Collaboration

[1] Any privacy analysis regarding Firebird's backup services of applications will be assessed with the substantive systems, applications, and databases being backed up, including backups from those applications in individuals' personal or One Drives (e.g., working copies). *See* Appendix B.

Services (ECS) that are common to all DEA users.[2] This Privacy Impact Assessment (PIA) will be published on DEA PIA webpage in accordance with DEA policy. See https://www.dea.gov/foia/privacy-impact-assessment.

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.

Firebird GSS is the primary enterprise information technology (IT) infrastructure of the DEA that provides computing, networking, storage, and other relevant services. Firebird GSS is categorized as a "General Support System" since it provides office automation and application services to all DEA personnel and contractors including overall authentication services (and some authorization services for certain systems/applications accessible on it). Firebird GSS is a cloud hybrid environment with strictly limited interfaces/connections to non-Department of Justice (DOJ)/DEA resources or external networks with some system on servers in DEA contracted locations. Overseen by TC Division, Firebird GSS utilizes the DOJ Justice Unified Telecommunications Network (JUTNet) for Wide Area Network (WAN) connectivity.

Hosted Systems: Firebird GSS provides network infrastructure supporting multiple internally connected DEA Sensitive-But-Unclassified (SBU) information systems (such as the CONCORDE system of investigative case management and administrative applications, the Castle premises access system, or the Laboratory Information Management System) and to several systems connected externally (such as connections to the State Department, other DOJ entities, or local law enforcement agencies). Firebird manages user access and data transfer with these hosted systems through secure connections. Rather than list the attributes of each of these "Hosted Systems" in this Firebird GSS PIA, each system listed in Appendix A that will require a PIA will be analyzed in greater depth in separate privacy documentation either individually, or grouped into relevant, multi-system documentation. However, the purposes of the Hosted Systems on Firebird GSS can be summarized as providing operational or administrative information management support for one or more of the following lines of business, functional areas, or aspects of DEA operations:

- **Law Enforcement Investigations and Operations** - This business line includes all criminal investigation, apprehension, and prosecution case management for both Operational Management (OM), domestic operations (OD) and foreign activities (OF). Firebird GSS Hosted Systems supporting this business line includes the case management applications contained in the CONCORDE application environment, such as the Investigative Management Program and Case Tracking System (IMPACT); the Narcotics

[2] Use of ECS is covered in separate compliance documentation. *See* Justice Management Division Email and Collaboration Services (ECS) Privacy Impact Assessment. https://www.justice.gov/opcl/media/1383331/dl?inline

and Dangerous Drugs Information System (NADDIS); the Centralized Evidence Tracking System, (CERTS) and Confidential Source System on Concorde (CSSC), among others.

Several other Firebird GSS systems support this business line as well, including several criminal surveillance/communications collection systems operated through the Office of Investigative Technologies on the STRATegic Unified Services General Support System infrastructure (e.g., Internet Intercept and Delivery System (IIDS) and the Translation and Transcription Support System (T2S2)) as well as other enforcement related applications on Concorde such as the Sensitive Investigative Units Network (SIUNET) supporting DEA's vetted foreign unit partners, the Investigative Support Section (ISS) system for task force officer and local law enforcement joint investigation efforts, and various operations support systems.

- **Diversion Control (DC) Operations** - This business line establishes Diversion Control Policy (DP) and covers DEA's efforts to prevent, detect and investigate the diversion of pharmaceutical controlled substances and "listed chemicals" from legitimate channels: including sectorial sections established for: Chemicals (DOC), Pharmaceutical Investigations (DOP), Targeting and Special Projects section (DOI), and Drug & Chemical Evaluation (DOE). This business line also includes regulatory-related activities to ensure an adequate supply of pharmaceutical controlled substances and listed chemicals to meet legitimate medical, commercial and scientific needs through prescriber registrations and manufacturer regulations: Regulatory (DRG); Import/Export (DRI); UN Reporting & Quota Setting (DRQ); Registration & Program Support (DRR). Firebird GSS Hosted Systems supporting this business line include, but are not limited to, the over two dozen applications on the DEA Registrant Support Network (RSN) and the Prescription Drug Monitoring Program Analysis System (PDMPAS).

- **Intelligence (NC) Operations and Analysis** - This business line involves Sensitive But Unclassified/Controlled Unclassified Information (SBU/CUI) systems for DEA intelligence collection operations, intelligence analysis, fusion center and associated information sharing efforts (e.g., Organized Crime Drug Enforcement Task Force management [OCDETF] and El Paso Intelligence Center applications) that support Law Enforcement investigations and operations. Firebird GSS Hosted System include, but are not limited to, the Real-Time Analysis Intelligence Database (RAID); Trends in the Traffic Reporting System (TTRS), the Document and Media Exploitation System (DOMex) on Concorde; and the El Paso Intelligence Center Seizure System (ESS) (that is in the process of changing names to the EPIC Inquiry System as of FY2024). Also included are systems dedicated for Special Operations Division (SOD) activities: The Defiance Application Suite, the SOD Operations system, and several systems on the Speedway/U General Support System.

- **Forensic Science (SF) Laboratory Activities** – This business line comprises Chemical Analysis and Fingerprint Forensics, Clandestine Laboratories Opinion and Analysis, Comparative Analysis through the Special Testing and Research Laboratory and Reverse Undercover Controlled Substance Assistance (Digital Forensics and Environmental

Management Services (EMS). The primary Firebird GSS system supporting this group is the Information Laboratory Management System.

- **Training and DEA Academy Activities -** Includes DEA Academy and internal DEA training programs and other employee development efforts. Relevant Firebird GSS Hosted Systems include, but are not limited to, the Personnel Data Verification (PDV) system; the Academy Information Systems (ACADIS)

- **Inspections Division (IG) Operations** - This division includes three offices: The Office of Professional Responsibility, Office of Inspections, and Office of Security Programs. Together these offices comprise of DEA's integrity system and provide innovative support to DEA Headquarters and field offices. The IG Operations conduct inspections, audits, and management reviews to ensure compliance with laws, regulations, and DEA policies and procedures. Firebird GSS systems include, but are not limited to, the Castle controls system and the other systems that may support the insider threat and personnel protection sections.

- **Information Systems (TC) Endeavors -** Encompass all the IT systems support, Enterprise Architecture, IT management improvement, and capital planning undertakings. TC responsibilities include System and network monitoring; help desk services and customer services, information/cybersecurity, information technology change management, system development, infrastructure maintenance, inventory management; and information technology continuity of operations/service recovery. Hosted or supported systems for this business line include DEA Amazon Web Services (DAWS); Enterprise Service Manager; DEA Zscaler, DEA Enterprise Digital Identity System (DEDIS) SailPoint, DEA Landing Zone, Internet Facing Architecture, the Depot Tracking System and the Development Security Operations (DevSecOps) Pipeline System, among others. TC also deploys those Firebird GSS IT applications that are core to its functionality, such as directory and network services as well as the Microsoft (MS)365 Office-Email-Collaboration Services and SharePoint services such as MS TEAMS and MS Outlook.

- **Administrative Activities,** all non-TC administrative support including:

    - **Finance (FN) Functions -** Includes accounting, collections receivables, and financials (budget execution, budget formulation and budget development and contracting, procurement, goods and services acquisition). Hosted Systems on Firebird GSS applicable to this business line include, but are not limited to, the DEA connection to the Unified Financial Management System (D-UFMS) and the Financial Information and Reporting System (FIRST) on Concorde GSS.

    - **Administrative Services (FS) -** Includes Administrative Operations, Facilities, Records Management, Policy and guidance development, disaster preparedness, planning, repair and restoration. Some of the systems supporting administrative

activities are contained with MS365 Office-Email-Collaboration Services and SharePoint sites and others are applications on the Concorde GSS.

- **Congressional Liaison Operations (CP)** - Legislation tracking, testimony, and legislation proposal development, as well as public affairs, correspondence and digital presence.

- **Human Resources (HR) Functions** - Activities that include benefits and compensation management, employee performance management, employee relations, recruiting, staff acquisition and onboarding, workforce planning, workplace policy development and management and employee travel and relocation. Most HR systems are found within the Concorde GSS application environment on Firebird.

- **Legal and Compliance Activities** - Activities that include legal advice, review, and litigation where DEA is a party (CC), Hearing and decisions by Administrative Law Judges (OALJ) and Compliance (AC). Many support systems for this grouping also are found within Concorde and MS365 Office-Email-Collaboration Services.

Core Firebird GSS Systems: Firebird GSS does provide several critical "core" functions as part of the TC sphere of operations that are provided to or encompass all DEA users. These "Core Firebird" systems consist of the following:

- **Directory and File Services** - File and directory services organize, store and provide access to information in the Firebird GSS Enterprise. Directory Services include Microsoft Active Directory (AD) in support of authentication and authorization of users, file and print servers as well as Microsoft Exchange. File services on the Firebird GSS network provide extended, protected and sharable storage for files. This storage is generally used for three purposes: 1) storage for individual files (home directory), 2) shared storage for groups of files (e.g., cases), and 3) shared storage of system files (e.g., applications). Microsoft Distributed File System Namespace (DFSN) is used to map user home directories, cases and share drives for all sites and users in the SBU domain.

- **Monitoring** – This includes a critical service that helps to ensure the health and well-being of infrastructure components and mission-critical applications. Data collected during monitoring allows Operations Management to identify and resolve performance or configuration issues, determine trends and make strategic operational decisions.

- **Release Management** - Release Management service manages deployment of approved operating systems, software, and patches within Firebird GSS.

- **Database** - There are several Relational Database Management Systems (RDBMSs) in Firebird GSS to include Oracle, Microsoft Structured Query Language (SQL) Server and Microsoft Access. The database tenants are responsible for ensuring applicable controls are implemented to protect PII.[3]

[3] *See* Appendix B for a complete listing of databases in Firebird's Relational Database Management System (RDBMS).

- **Backup and Recovery** - A comprehensive backup strategy has been implemented to provide data recovery of individual files (home directory), shared storage for groups of files (e.g., cases), and shared storage of system files (e.g., applications). This includes Division and Resident/District Office that utilize Symantec Backup Exec 2010, and Datacenter Backup that employs Microsoft Data Protection Manager.[4] With respect to the mechanics of backup as a whole, the specifics relevant to privacy are addressed in this PIA. See Appendix B for listing of databases in Firebird GSS's Relational Database Management Systems (RDBMS) that are also backed up as part of the backup strategy in Firebird GSS.

- **Enterprise Storage Management** – Firebird GSS enterprise storage management provides storage solutions including provisioning, monitoring, and reporting. This includes Enterprise Storage Arrays that utilize EMC, HP and Dell technology infrastructure as well as a Storage Area Network Fabric to include switches and devices allowing hosts access to storage arrays available to the infrastructure.

- **Mobility Services** – Firebird GSS provides users with several remote access options including Firebird laptop, Azure Virtual Desktop (AVD) interface formerly known as Firebird Anywhere (FBA), and other mobile devices (e.g., phones and tablets).

- **Network Services** - The Firebird GSS network infrastructure consists of hardware and software resources that enable network connectivity, communication, and management of the Firebird enterprise.

- **Deskside Access** – Firebird GSS workstations are located throughout all DEA Field Divisions, Foreign Office sites, and at DEA HQ. The Firebird GSS workstations provide DEA users access to a standard suite of office automation tools and DEA business applications.

- **Enterprise-wide operating system** - Firebird GSS also contains DEA's Enterprise-wide operating system, MS Office 365 and included applications MS Word, Excel and PowerPoint as well as a slate of various Electronic Collaboration Services (ECS) that are common to all DEA users.[5] Dedicated TC personnel assigned to Firebird GSS are responsible for configuration of these services and applications in accordance with Defense Information Systems Agency (DISA) Security Technical Implementation Guide but are not responsible for the collection, processing or dissemination of the underlying data. These services include:

---

[4] For purposes of this PIA, any privacy analysis regarding Firebird backup data for each individual system, application or database on Firebird will be assessed with the PIAs for each substantive system, application, and/or database being backed up by Firebird GSS, including backups of data from those applications in individuals' personal or One Drives (i.e., working copies). *See Appendix A.*

[5] The privacy documentation for the MS Office, email, and other ECS aspects of Firebird can be found in separate privacy documentation for MS365 Office-Email-Collaboration Services. *See* Justice Management Division Email and Collaboration Services (ECS) Privacy Impact Assessment. https://www.justice.gov/opcl/media/1383331/dl?inline

- Messaging (e.g., Jabber, MS Teams, Slack)
- Email (i.e. MS Outlook)
- Collaboration document production (e.g., SharePoint, MS Teams, and shared files and folders that are a software collaboration tools)
- Web Services and internet access
- Video conferencing (e.g., WebEx and MS Teams)

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	Controlled Substances Act, 21 United States Code (U.S.C.) § 801, et seq.;
Executive Order	
Federal Regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

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.

Firebird GSS serves mainly as an application environment interface and General Support System that collects and processes limited amounts of PII for the authentication and authorization functions it provides. Most PII in Firebird GSS is accessed on the Hosted Systems, which have their own Privacy Impact Assessments (PIA), if so required. Thus, this PIA will employ a bifurcated analysis for all "Hosted Systems" in general and group the key "core systems" containing the main functions of the Firebird GSS infrastructure or centralized services. Thereafter, this PIA will only focus on Core systems—all in depth privacy analysis of the Hosted Systems will be found in the individual PIA for each Hosted System or groups of such system, as appropriate.

(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 – Firebird Hosted System	X	A, B, C and D	Hosted Systems contain name information of DEA and other federal GOV personnel/users and/or third parties (USPER & non-USPER). (See relevant Hosted System PIAs were applicable.)
Core Firebird GSS	X	A and B	Core Firebird GSS Systems maintain identity information of users, including names for DEA and other federal GOV personnel/users
Date of birth or age – Firebird GSS Hosted Systems	X	A, B, C and D	Many Hosted Systems contain business contact information to include date of birth of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	Hereafter, an "N/A" will identify PII categories that **Core Firebird GSS** authentication/networking functions do not use or maintain.
Place of birth – Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain business contact information to include place of birth of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Place of birth – Core Firebird GSS	N/A	N/A	N/A
Gender – Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain information of the gender of members of the public (USPER & non-USPER), such information may also be inferred from other information present, and may contain gender information of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable)
Gender – Core Firebird GSS	N/A	N/A	N/A

(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
Race, ethnicity or citizenship – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain information to include race, ethnicity or citizenship of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Religion – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain religious information to include religion of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Social Security Number (full, last 4 digits or truncated) – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Many Hosted Systems contain Social Security Number information of DEA and other federal GOV personnel and/or members of the public (USPER and on-USPER). (See relevant Hosted System PIAs where applicable) N/A
Tax Identification Number (TIN) – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems contain TIN of members of the public (USPER and on-USPER). (See relevant Hosted System PIAs where applicable) N/A
Driver's license- Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems contain driver's license numbers of members of the public (USPER and on-USPER). (See relevant Hosted System PIAs where applicable) N/A
Alien registration number – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems contain alien registration numbers of members of the public (USPER and on-USPER). (See relevant Hosted System PIAs where applicable) N/A

(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
Passport number – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems contain passport numbers of members of the public (USPER and on-USPER). (See relevant Hosted System PIAs where applicable) N/A
Mother's maiden name – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems contain Mother's maiden name of members of the public (USPER and on-USPER). (See relevant Hosted System PIAs where applicable) N/A
Vehicle identifiers – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems contain vehicle identifiers of members of the public (USPER and on-USPER). (See relevant Hosted System PIAs where applicable) N/A
Personal mailing address – Firebird GSS Hosted Systems Core Firebird GSS	X X	A, B, C and D A and B	Many Hosted Systems may contain personal mailing address information of DEA and other federal GOV personnel/users and/or third parties (USPER & non-USPER). See relevant Hosted System PIAs were applicable Core Firebird GSS Systems maintain some personal mailing address information of users who are DEA and other federal GOV personnel/users

(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
Personal e-mail address – Firebird GSS Hosted Systems Core Firebird GSS	 X N/A	 A, B, C and D N/A	Many Hosted Systems contain personal email address information of DEA and other federal GOV personnel/users and/or third parties (USPER & non-USPER). See relevant Hosted System PIAs were applicable N/A Note: although dedicated Firebird personnel are responsible for configuration of MS Office 365 ECS (which maintains some personal e-mail addresses) , Core Firebird is not responsible for the collection, processing, or dissemination of the underlying data in that system .
Personal phone number – Firebird GSS Hosted Systems Core Firebird GSS	 X X	 A, B, C and D A and B	Many Hosted Systems contain personal phone numbers of DEA and other federal GOV personnel/users and/or third parties (USPER & non-USPER). See relevant Hosted System PIAs were applicable. Some Core Firebird GSS Systems maintain personal phone numbers of users who are DEA and other federal GOV personnel/users
Medical records number – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems may contain medical information of members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable N/A
Medical notes or other medical or health information – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems may contain medical information of members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable N/A
Financial account information Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems may contain financial account information of members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable N/A

(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
Applicant information – Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain applicant information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Education records – Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain education records information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Military status or other information – Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain military records information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Employment status, history, or similar information- Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain employment information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Employment performance ratings or other performance information, e.g., performance improvement plan Firebird GSS Hosted Systems	X	A and B	Some Hosted Systems contain employment performance information of DEA and other federal GOV personnel (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Certificates Firebird GSS Hosted Systems	X	A and B	Some Hosted Systems contain training information that could include certificates of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A

(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
Legal documents Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain legal documents and associated information regarding DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER) (See relevant Hosted System PIAs where applicable) N/A
Device identifiers, e.g., mobile devices – Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain mobile device identifiers of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Web uniform resource locator(s) Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain information of URL associated activity of members of the public (USPER & non-USPER) and may also contain identity of URL activity of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable) N/A
Foreign activities Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain information of foreign activities of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Criminal records information, e.g., criminal history, arrests, criminal charges Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain criminal records information on members of the public (USPER & non-USPER) and may contain identify information of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable) N/A

(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 Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain juvenile criminal records information of members of the public (USPER & non-USPER); and may include identity information of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable) N/A
Civil law enforcement information, e.g., allegations of civil law violations- Firebird GSS Hosted Systems Core Firebird	X N/A	C and D N/A	Some Hosted Systems may contain Civil law enforcement information of members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Whistleblower, e.g., tip, complaint, or referral Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain information concerning witness to criminal matters involving the public (USPER & non-USPER) and may contain identify information of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable) N/A
Grand jury information- Firebird GSS Hosted Systems Core Firebird GSS	X N/A	C and D N/A	Some Hosted Systems may contain Grand jury information of members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain information concerning witness to criminal matters involving the public (USPER & non-USPER) and may contain identify information of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable) N/A

(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
Procurement/contracting records Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain information concerning procurement and contracting involving DEA and other federal GOV personnel; other systems may contain contract information involving members of the public (USPER & non-USPER) (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Proprietary or business information Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain information concerning procurement and contracting involving DEA and other federal GOV personnel; and other systems may contain contracting information involving members of the public (USPER & non-USPER) (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Location information, including continuous or intermittent location tracking capabilities Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain information related to the locations of members of public (USPER & non-USPER) that may include tracking, and may also contain identify information of DEA and other federal GOV personnel. (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Biometric data:			
Photographs or photographic identifiers – Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain photos, videos, or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A
Video containing biometric data – Firebird GSS Hosted Systems	X	A, B, C and D	Some Hosted Systems contain photos, videos, or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable)
Core Firebird GSS	N/A	N/A	N/A

(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
Fingerprints Firebird Hosted System Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain photos, videos, or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Palm prints Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain photos, videos, or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Iris image Firebird Hosted System Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain voice recording or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Dental profile Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain photos, videos, or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Voice recording/signatures Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain voice recording or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A

(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
Scars, marks, tattoos Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain photos, videos, or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
Vascular scan, e.g., palm or finger vein biometric data Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain photos or video recording that could reveal scars or tattoos if visible of members of the public (USPER & non-USPER). Identifying information of DEA and other federal GOV personnel may also be collected. (See relevant Hosted System PIAs where applicable) N/A
- **DNA profiles** Firebird GSS Hosted Systems Core Firebird GSS	X N/A	A, B, C and D N/A	Some Hosted Systems contain photos, videos, or biometrics information of DEA and other federal GOV personnel and/or members of the public (USPER & non-USPER). (See relevant Hosted System PIAs where applicable) N/A
- **Other (specify)**			
System admin/audit data - - Firebird GSS Hosted Systems --and-- Core Firebird	X	A and B	System administrative and auditing data for both Hosted and Core Firebird GSS Systems include user identification and associated passwords, IP addresses and date/time of access and is used for troubleshooting applications, internal DEA and other federal GOV personnel (See relevant Hosted System PIAs where applicable)
- **User ID**	X	A and B	Same as above
- **User passwords/codes**	X	A and B	Same as above
- **IP address**	X	A and B	Same as above
- **Date/time of access**	X	A and B	Same as above
- **Queries run**	X	A and B	Same as above
- **Contents of files**	X	A and B	Same as above
Other (please list the type of info and describe as completely as possible):			

NOTE: System Admin/Audit Data: Auditing information as identified above is collected as part of the process of documenting activity within the software systems used across Firebird GSS. Audit logs record the occurrence of an event, the time at which it occurred, the responsible user or service and the impacted entity. All of the devices that encompass Firebird GSS components emit logs that may be used for auditing purposes. A series of the audit logs is called an audit trail because it shows a sequential record of all the activity that occurred on Firebird GSS. By reviewing the audit logs, system administrators can track user activity and the security teams (Incident Response Teams) can investigate breaches and ensure compliance with regulatory requirements such as National Institute for Standards and Technology (NIST) 800-53 Rev 5.[6]

Firebird GSS audit logs capture the following types of information:

- Event name as identified in the system.
- Easy-to-understand description of the event.
- Event timestamp
- Actor or service that created, edited, or deleted the event (user ID or API ID)
- Application, device, system, or object that was impacted (IP address, device ID, etc.)
- Source from where the actor or service originated (country, host name, IP address, device ID, etc.)

Operating systems automatically capture information which is then forwarded on to the appropriate security tool, (e.g., Splunk)

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			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
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		Public media, Internet		Private sector	

[6] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

Commercial data brokers					
Other (specify):					

NOTE: answers in preceding Section 3.2 provided only for Core Firebird GSS Systems

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.

NOTE: Many hosted systems may share information with components of DEA and/or other federal GOV personnel/agencies and/or members of the public (USPER & non-USPER). This information is covered within the hosted system's PIA, where applicable. The answers below are only regarding Core Firebird GSS.

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		X	System admin/Auditing data may be used/shared to troubleshoot issues with applications. Access control data is shared through Firebird GSS to other applications within DEA
DOJ Components	X			System admin/Auditing data information may be required by law enforcement from other organizations for investigations regarding cybercrimes.
Federal entities	X			System admin/Auditing data information may be required by law enforcement from other organizations for investigations regarding cybercrimes.
State, local, tribal gov't entities	X			System admin/Auditing data information may be required by law enforcement from other organizations for investigations regarding cybercrimes.
Public				

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			In accordance with criminal or civil discovery obligations or litigation preparations, if necessary.
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.

The Core Firebird GSS will not release data to the public for Open Data purposes.

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.

All Firebird GSS components provide the below generalized notice. All users are presented with the following banner notice prior to logging onto the Firebird GSS components. This banner explains to the user their rights as it pertains to using Firebird. The banner reads:

> You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
>
> The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, Communications Security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

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.

Firebird provides the network infrastructure and support to multiple internally connected DEA information systems (such as the CONCORDE system of investigative case management, support and administrative applications, the Castle premises access system, and the Laboratory Information Management System, etc.) and to several systems connected externally (such as connections to the State Department, other DOJ entities, or local law enforcement agencies). Generally, there are no opportunities for individuals to voluntarily participate in the collection of information in Hosted Firebird system, but for Core Firebird GSS Systems, much of the user information comes from data voluntarily provided by users. Functionally, Firebird provides overall authentication services (and some authorization services) for Hosted systems, but core Firebird functionality collects and processes limited amounts of PII for these authentication and authorization services—most PII is kept on the hosted systems, which are required to have their own PIAs as appropriate, and which may have their own notices in collection of information. Prior to gaining access to Firebird the users must acknowledge the collection of the PII data and agree to the Privacy Act Statement and Release of information, which is detailed in Section 5.1 above. The audit data collected is for system administrative/troubleshooting purposes. If a user requires auditing information the request should go through the proper channels to include utilizing the helpdesk.

NOTE: Hosted systems may respond differently to this question; however, this section of this PIA section pertains only to the Core Firebird GSS.

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.

Firebird users can modify their data using the various systems such as DEA Enterprise

Digital Identification System (DEDIS),[7] the Account Management System, DEA service desk or using DEA's Microsoft Identity Manager portal.

NOTE: Hosted systems may respond differently to this question; however, this section of this PIA only pertains to the Core Firebird GSS.

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).

NOTE: Hosted systems may respond differently to the below controls which are discussed within the hosted system's PIA. This PIA section only pertains to the Core Firebird GSS.

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):** The last ATO issued to Firebird was 5/20/2022. Firebird is in the ongoing authorization program) **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:**
	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: NOTE: Continuous monitoring will be conducted. As a standard procedure, the DOJ core controls will be evaluated annually.
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:** Firebird GSS maintains many different information types from both its core and hosted systems. The most sensitive of which would fall into the Type "Criminal Investigation and Surveillance Information" in NIST SP800-60 because it involves the collection of evidence required to determine responsibility for a crime and the monitoring of affected parties. The provisional confidentiality impact level for this type is MODERATE, however, given the nature of many of the crimes that are the responsibility of the DEA, the consequences

[7] DEDIS is covered by separate compliance documentation.

	associated with unauthorized disclosure of criminal investigation and surveillance information must often be assumed to pose a threat to human life or result in a loss of major assets. Information that reveals the identity and/or location of informants may be of particular concern. In such cases, the confidentiality impact level is high. As Firebird maintains information that can include victim, witness, and informant information, as well as the information of several different types of information (e.g., social security numbers, first/last name, birth dates and home address). DEA therefore assesses that unauthorized disclosure of this data could be expected to pose a threat to human life of a variety of persons, including agents, informants, targets, or witnesses. As such, DEA asserts the overall categorization of the system remains HIGH.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle. DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that affect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are required to be reviewed and assessed by the Senior Component Official for Privacy prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
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:** DEA Cybersecurity Operations, Response and Engineering Unit (TCVV) is responsible for reviewing and analyzing the Firebird GSS information system audit records on a daily and continuous basis for indications of inappropriate or unusual activity in accordance with the DEA Incident Response Plan. DEA's Cybersecurity Investigation and Response Unit (Response Unit) monitors Firebird GSS components using the Splunk event correlation tool[8] to identify and report findings to the ISSO for further investigations upon detection of suspicious activities. Splunk captures all of the audit logs from Firebird components. Any findings are reported to DOJ Security Operations Center using the Justice Management Division Remedy ticketing system.

[8] Splunk is covered by separate privacy documentation here: https://www.justice.gov/d9/2023-01/doj_laas_pia_final_for_publication_1.pdf.

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**. All contracts have the necessary, proper, and accurate privacy and security-related clauses (i.e., DOJ Clause 02, *Contractor Privacy Requirements*; and DOJ Clause 05, *Security of Information and Information System*) and language required listed in each contract awarded within DEA.
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:** Required training is distributed and tracked via the DEA Learning Management System – DEALS. This training includes general mandatory annual trainings for information systems like rules of behavior and cybersecurity awareness training that are applicable to all DEA component personnel

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?

Physical controls:

Core Firebird GSS has been deployed in a physical, DEA contracted, secure data center. The following controls are specific to Core systems, but the Firebird boundary technically covers all Firebird GSS Hosted Systems. This data center provides physical protection for all hosted systems to include servers, switches, and other devices employed to support the DEA mission. In addition, the data center supplies electrical and HVAC systems for the hosted components. The data center utilizes numerous safeguards to include guards who monitor the facility. Entry includes two sets of doors, the first utilizes a Personal Identity Verification (PIV) Card which is scanned for entry. The second door requires use of the PIV as well as the associated individual PIN. Viewing Cameras have been deployed at critical locations to include entry ways. Metal Detectors have been employed for any visitors that do not have a PIV. All physical controls for Firebird GSS are inherited from the data center. Although, many hosted applications are in Government Cloud environments at protected locations in the continental United States, Core Firebird GSS applications do not use cloud technology currently. However, in the future, some applications within Core Firebird GSS may also be migrated to a government cloud infrastructure.

Technical privacy and security administrative controls:

Numerous processes/controls have been implemented by DEA to ensure access to data is limited to those with a verified need-to-know for Core Firebird applications. These processes include:

- Identifying and selecting the following types of information system accounts to support organizational missions/business functions: individual, group/shared, service, guest/anonymous, and temporary/emergency accounts.
- Assigning account managers for information system accounts.
- Establishing conditions for group and role membership.
- Specifying authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
- Requiring approvals by for requests to create information system accounts.
- Creating, enabling, modifying, disabling, and removing information system accounts in accordance with DOJ Order 0904: Cybersecurity Program and applicable information system policy and procedures;
- Monitoring the use of information system accounts;
- Notifying account managers:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When individual information system usage or need-to-know changes;
- Authorizing access to the information system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated missions/business functions;
- Reviewing accounts for compliance with account management requirements.

To the extent some Firebird servers hosting applications have been or will be transferred to a Government Cloud platform, the cloud environment is considered Infrastructure as a Service (IaaS). All controls in the cloud context are still the responsibility of Firebird and DEA just as they are for all Firebird applications physically housed in DEA servers on premises.

Through the utilization of Microsoft AD, access to core system PII is controlled and limited to system administrators and personnel that have a need to know based on their position within the organization. This information is used to create access controls and segregations of duty. The Core Firebird GSS components also utilize the following technical controls to protect the data:

- Database encryption for data at rest
- Disk Encryption
- Transport Layer Security (TLS) for data in transit.
- Data Loss Prevention (DLP) software

Hosted systems have their own access requirements and controls listed in the relevant Joint Cybersecurity Authorization Management (JCAM) system profile and that will identify whether or not such controls have been implemented in accordance to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, revision 5.

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.)

In accordance with NIST 800-53 Rev 5 and the General Records Schedule 3.2, Information Systems Security Records Section Item 060 PKI administrative records for Core Firebird will be retained for a minimum of seven years, six months. Longer retention is authorized, if required, for business use.

NOTE: Hosted systems may respond differently to the above question; however, duration of retention period is discussed within the hosted system's separate privacy documentation.

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 following SORNS are applicable to Core Firebird GSS:

- JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021). https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf

- JUSTICE/DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 Fed. Reg. 60,110 (Nov. 7, 2019). https://www.govinfo.gov/content/pkg/FR-2019-11-07/pdf/2019-24246.pdf

The following SORNS apply to the various "Hosted Systems" or subsystems on Firebird:

- DEA-003, *Automated Records and Consolidated Orders System-Diversion Analysis and Detection System (ARCOS-DADS)*, 69 Fed. Reg. 51104 (Aug. 17, 2004)

- DEA-005, *Controlled Substances Act Registration Records (CSA)*, 52 Fed. Reg. 47182, 208 (Dec. 11, 1987)
- DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (April 11, 2012)
- DEA-010, *Planning and Inspection Division Records*, 52 Fed. Reg. 47182 (Dec. 11, 1987)
- DEA-011, *Operations Files*, 52 Fed. Reg. 47182 (Dec. 11, 1987) DEA-012, Registration Status-Investigation Records, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)
- DEA-013, *Security Files*, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)
- DEA-015, *Training Files*, 52 Fed. Reg. 47182 (Dec. 11, 1987)
- DEA-017, *Grants of Confidentiality Files (GCF)*, 52 Fed. Reg. 47182, 218 (Dec. 11, 1987
- DEA-020, *Essential Chemical Reporting System*, 52 Fed. Reg. 47182, 219 (Dec. 11, 1987)
- DEA -021, *DEA Aviation Unit Reporting System*, 65 Fed. Reg. 24986, 987 (Apr. 28, 2000)
- DOJ-001, *Accounting Systems for the Department of Justice*, 69 Fed. Reg. 31406 (June 3, 2004)
- DOJ-003, *Correspondence Management Systems (CMS) for the Department of Justice*, 66 Fed. Reg. 29992 (June 4, 2001)
- DOJ-006, *Personnel Investigation and Security Clearance Records for the Department of Justice,* 67 Fed. Reg. 59864 (Sept. 24, 2002)
- DOJ-009, *Emergency Contact Systems for the Department of Justice*, 69 Fed. Reg. 1762 (Jan. 12, 2004)
- DOJ-014, *Department of Justice Employee Directory Systems*, 74 Fed. Reg. 57194 (Nov. 4, 2009)
- DOJ-020, *DOJ Identity, Credential, and Access Service Records System*, 84 Fed. Reg. 60110 (Nov. 7, 2019)
- JMD-003, *Department of Justice Payroll System*, 69 Fed. Reg. 107 (Jan. 2, 2004)
- JMD-026, *Security Monitoring and Analytics Service Records*, 86 Fed. Reg. 41089 (July 30, 2021)
- OPM SORN GOVT-1, *General Personnel Records*, 77 Fed. Reg. 79694 (Jun. 19, 2006)
- OPM SORN GOVT-2, *Employee Performance File System Records*, 71 Fed. Reg. 35347 (Jun. 19, 2006)
- OPM SORN GOVT-3, *Records of Adverse Actions, Performance Based Reductions In Grade and Removal Actions, and Terminations of Probationers*, 71 Fed. Reg. 35350 (Jun. 19, 2006)
- OPM/GOVT-5, *Recruiting, Examining, and Placement Records*, 79 Fed. Reg. 16834 (March 26, 2014)
- OPM/GOVT-10, *Employee Medical File System Records*, 75 Fed. Reg. 35099 (June 21, 2010)
- USDA/OP-1, *Personnel and Payroll System for USDA Employees*, 63 Fed. Reg. 4213 (Jan. 28, 1998)

- GSA/GOVT-7, *HSPD-12 USAccess*, 80 Fed. Reg. 64416 (October 23, 2015)

Please note: Hosted Systems' applicable SORNs are further discussed within the relevant hosted systems' PIAs.

.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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

NOTE: Hosted systems have unique privacy risks associated with their collection, maintenance, and dissemination of PII, and so may respond differently to privacy risks and mitigations; however, each such risk is assessed for a particular hosted system within that hosted system's PIA.[9] But because there remains a specific privacy risk applicable to data gathering from the operation of multiple hosted systems, such a risk is listed here because such aggregation risks, by definition, exist beyond the operation of a single Firebird hosted application.

a. Potential Threats Related to Information Collection

Privacy Risk: Because some Firebird GSS hosted systems may each aggregate PII data from multiple sources, collected by multiple organizations, and because such aggregation also may occur across multiple hosted systems on Firebird GSS, there is a chance of overcollection of data or that some PII collected in this manner will not be directly relevant and necessary for the system to accomplish its purpose/mission.

Mitigation: This risk is partly mitigated. Regarding the "mosaic effect" from ingesting and assessing PII from multiple different hosted system, Firebird personnel do actively check with data owners from internal and external organizations to ensure owners have placed administrative controls on any ingested data to lesson this risk. Firebird GSS personnel also work with program managers/owners (PMOs) of datasets to develop processes to ensure data minimization is included as part of the onboarding of each dataset connection that utilizes Firebird GSS. A more detailed assessment of the privacy risks for hosted systems that have their data aggregated are set forth in those hosted systems' PIAs.

With respect to Firebird GSS Core systems, these applications do not aggregate data per se, with the exception of audit logs and queries and results of queries of such audit logs. Generally, Firebird GSS Core Systems limit the amount of PII they use to that which is necessary for Authentication and Authorization purposes, and therefore directly relevant

[9] *See* Appendix A for a list of hosted systems and whether they are covered by separate privacy compliance documentation.

for the Core system to accomplish its purpose/mission. Given the similar functions across the Firebird network, even aggregating Authentication and Authorization data across multiple systems will generally only replicate the same information multiple times.

In addition, controls referenced at Section 6.2 have been implemented. The data is controlled through defined access permissions whereby only authorized data is visible based on the role of the user/application/system.

NOTE: The remainder of this PIA Section on Privacy Risks only pertains to the Core Firebird GSS:

Privacy Risk: Individuals may be unaware Firebird is collecting their PII and cannot meaningfully consent to the collection of their PII by Firebird.

Mitigation: This risk for DEA users is mitigated using the mandatory banner at login. All DEA system users are presented with the same banner (which is described in detail above in Section 5.1) indicating that their PII is being collected by Firebird.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: System information may be susceptible, either at rest or in transmission, to compromise from an "Insider Threat" or technological/cyber breach (e.g., Hacking) resulting in a breach.

Mitigation: This risk is mitigated. Firebird GSS has implemented a Data at Rest and Data in Transit solution which has been validated utilizing security guides (i.e., NIST 800-53 and FIPS 140-2). Further there are numerous security tools deployed at critical locations within DEA to ensure any compromise is identified and the DEA Enterprise Incident Response Plan has processes to follow in the case of compromise. See also the measures described above in Sections 6.1 and 6.2.

Privacy Risk: Authorized DEA personnel may mishandle or fail to safeguard PII.

Mitigation: This risk is partially mitigated. Firebird GSS components utilize numerous security tools to ensure that the systems are securely configured and managed in accordance with policy. DEA's Response Unit monitors Core Firebird GSS systems using the Splunk event correlation tool to identify and report findings to the relevant Information System Security Officer for further investigations upon detection of suspicious activities. The Response Unit handles event correlation and then notifies appropriate personnel as needed in accordance with policy. However, there is still a possibility personnel may not handle the PII data appropriately. Additional mitigation includes mandatory annual training for the users. Users are expected to follow DEA IT Rules of Behavior that defines PII requirements to the users of DEA's IT systems. All users are required to review and provide signature or electronic verification acknowledging understanding of these rules. Failure to comply with the rules and responsibilities listed in the ROB may result in remedial training; loss of access to information systems; loss of a security clearance; verbal or written warning; termination of employment; or civil or criminal prosecution. In FY2025, DEA is expected to implement

annual role-based privacy training that will address safeguarding and proper dissemination of PII. Further, the roles and responsibilities as defined for both users and managers for Firebird Core Systems are validated annually to include not only applicability but to also ensure compliance.

Privacy Risk: Monitoring, testing, and evaluation of privacy and security controls may be insufficient or too infrequent and DEA may not appropriately audit, document, and review compliance of its PII rules on this Core system.

Mitigation: This risk is mitigated through the completion of the core control review as defined by DOJ, including the roles and responsibilities for included Core system, and the quarterly review of any outstanding POAMs as defined by DEA. These measures are described above in Sections 6.1 and 6.2. DEA has focused their attention specifically on those that pertain to PII data. The review, once completed, is documented within the JCAM record for Firebird GSS.

In addition, for newly built systems, DEA utilizes a standardized build process to ensure all auditing and security tools are implemented in accordance with approved guidelines. Further, DEA uses security tools, such as "Qualys," to help manage and monitor the configuration settings of the systems that will ensure that auditing is configured in accordance with the build standards. Validation and compliance with PII rules within hosted systems running on Core Firebird GSS is automatically performed through the Firebird GSS Systems/processes.

Privacy Risk: PII may be altered for potentially impermissible purposes, thereby affecting the accuracy and reliability of the information.

Mitigation: This risk is mitigated. Firebird GSS employs numerous tools to monitor the components. Therefore, if Core Firebird data is altered, the security tools would alert DEA's Cybersecurity Investigation and Response Unit. (See Section 6.1, explanation box re: monitoring, or Section 6.2). Alteration of information with hosted systems is the responsibility of the hosted system personnel.

Privacy Risk: Data may be retained longer than necessary, which may reduce the relevance and timeliness of the data.

Mitigation: This risk is mitigated for Firebird Core systems. Retention schedules are executed by the system automatically through archiving or overwriting the data at the tagged expiration date. Backup information is automatically deleted on a set schedule. In addition, the system administrators may conduct routine reviews and/or execute manual deletions. All activities executed on the system are captured in audit logs and routine backups are in place. Core Firebird GSS components have adopted a retention solution that follows applicable guidance.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: The potential exists for DEA personnel to share or disclose PII to an inappropriate party or for an improper use.

Mitigation: This risk for Core Firebird GSS PII is mitigated for dissemination to both improper parties and for improper uses.

Regarding Improper Uses: The limited information contained within Core Firebird GSS is mainly name, position, and business contact information of DEA personnel and contractors or detailees (See Section 3.1). Dissemination of Core Firebird System PII outside DEA would generally result in relatively limited harm. However, DEA personnel identities must still be disclosed outside DEA judiciously and in line with DEA policy. All users of Firebird GSS elements are required to review and provide signature or electronic verification acknowledging understanding the rules identified in the DEA IT Rules of Behavior including limitations on dissemination of PII that require recipients to have bona fide need to know for a use compatible with the purpose for which the information was collected.

Regarding Improper Parties: In addition, Qualys, along with other security tools, continues to monitor access to data that is available for use by Firebird GSS. The security tools working alongside user access and training help mitigate this risk. (See Section 6.1 and Section 6.2). Hosted systems are responsible for their own review. However, disclosure to parties outside DEA is tracked. DEA has its own form that personnel must file when making external disclosures of DEA information (DEA-381 Disclosure Account Record) that will keep track of disclosures. DEA also has deployed annual role-based refresher privacy training that addresses safeguarding and proper dissemination of PII to appropriate parties.

APPENDIX A – HOSTED SYSTEMS/APPLICATIONS AND INTERCONNECTIONS

The below systems have child and/or interconnection relationship with the Firebird GSS Systems at the time of signature for the Firebird GSS Environment PIA. This list will be updated no less frequently than every three years, or sooner if determined appropriate by the DEA senior component official for privacy. The known status of PII has been included for these systems/applications.

System Name	Connection	PII	Separate PIA
Academy Information Systems (ACADIS)	Internal	Yes	Yes
Account Management System	Internal	Yes	Yes
Authenticated Digital Asset Management System (ADAMS)	Internal	Yes	Yes
Aviation Maximo Maintence, Repair, and Overhaul (MRO)	Internal	Yes	Yes
AI Compute Cluster (AC2)/AI R and D Platform	Internal		
Castle	Internal	Yes	Yes
Cellebrite	Internal	Yes	In process
Central Tracking System (CTS)	Internal	Yes	Yes
Chameleon	Internal	Yes	In process
CONCORDE General Support System (GSS)	Internal	Yes	Multiple PIAs in process
Data Lake 2.0	Internal	Yes	In process
DEA Amazon Web Services Landing Zone (DALZ)	Internal	Yes	In process
DEA Disciplinary Management System	Internal	Yes	Yes
DEA Enterprise Digital Identity System (DEDIS) SailPoint	Internal	Yes	Yes
DEA Federal HR Navigator (FHRN)	Internal	Yes	In process
DEA Interview Room System (DIRS) formally Case Cracker Interview Room (CaseCracker)	Internal	Yes	Yes
DEA Microsoft Azure Government (MAG) Landing Zone (DMLZ)	Internal	Yes	No
DEA ProLaw	Internal	Yes	In process
DEA Video Teleconferencing System	Internal	No	No
DEA Zscaler	Internal	Yes	No

System Name (continued)	Connection	PII	Separate PIA
Defiance Application Suite	Internal	Yes	Yes
Diversion Customer Contact Center (DC3) formally Diversion Technical Operations Management Support System (D-TOMSS)		Yes	In process
DocuSign (DS)	Internal	Yes	No
Depot Tracking System	Internal	Yes	Yes
Development Security Operations (DevSecOps) Pipeline	Internal	Yes	No-See subsystem PIAs
Docket Master System (DMS)	Internal	Yes	Yes
Digital Evidence Laboratory Findings Network	Internal	Yes	Yes
Dynatrace (DT)	Internal	Yes	No
Employee Assistance Program Pro 360	Internal	Yes	No
Enterprise Service Manager	Internal	Yes	No
EPIC Inquiry System GSS (formerly EPIC Seizure System)	Internal	Yes	Yes
Financial Information Reporting & System Tool (FIRST)	Internal	Yes	Yes
FOIA Xpress	Internal	Yes	Yes
Internet Facing Architecture	Internal	Yes	In process
Internet Intercept and Delivery System (IIDS)	Internal	Yes	In process
Inventory Retrieval Management System (IRMS)	Internal	Yes	In process
IT Services Enclave	Internal	No	No
Jatom Systems Inc.	Internal	Yes	Part of PIA for T2S2
KnowBe4	Internal	Yes	In process
Laboratory Information Management System	Internal	Yes	In process
LabX	Internal	Yes	No
Lucid	Internal	Yes	In process
Medical Evaluation for Duty, Fitness, and Occupation Resources Concerning Employment (Medforce) formally DEA Electronic Health Records (EHR)	Internal	Yes	In process

System Name (continued)	Connection	PII	Separate PIA
MS360 Office-Email-Collaboration Services	Internal	Yes	Yes- See JMD PIA
Office of Training Internet Network (OTIN)	Internal	Yes	No
Openlab	Internal	Yes	No
Prescription Drug Monitoring Program Analysis System	Internal	Yes	Yes
Penlink on Firebird (FB-PLX)	Internal	Yes	In process
Polygraph Enterprise System (PES)	Internal	Yes	In process
Relativity	Internal	Yes	Yes
Slack	Internal	Yes	In process
SmarTrack	Internal	Yes	In process
Speedway/U GSS	Internal	Yes	In process
Spider Core	Internal	Yes	In process
STRATegic Unified Services GSS	Internal	Yes	No -See subsystem PIAs
Translation and Transcription Support System (T2S2)	Internal	Yes	In process
Unified Endpoint Management (UEM)	Internal	Yes	In process
Government Time and Attendance	Internal	Yes	USDA PIA
Controlled Substance Ordering System (CSOS) 2.0	Internal/External	Yes	
DEA Registrant Support Network (RSN)*	Internal/External	Yes	Yes
Consolidated Overseas Accountability Support Toolbox (COAST)—[Connects to Dept. of State's Secure HTTP Internet File Transfer System (SHIFTS) and DOJ's Unified Financial Management System-(UFMS)]	Internal/External	Yes	No
Enterprise Secure Chat (ESChat) - ESCHAT Push-to-Talk, Tactical Communications Platform (TCP) application	Internal/External	Yes	In Process – See TCP PIA
OKTA	Internal/External	Yes	
ONTIC	Internal/External	Yes	Yes
Tactical Communications Platform (TCP)	Internal/External	Yes	In Process

System Name (continued)	Connection	PII	Separate PIA
Commonwealth Law Enforcement Assistance Network (CLEAN)	External Connection	Yes	N/A (State DB)
DEA- Communications Automated Profiling System (CAPS)	External Connection	No	No
Department of State - Secure HTTP Internet File Transfer System (SHIFTS)	External Connection	Yes	DOS PIA
DHS Redundant Trusted Interconnection (RTIC)	External Connection	Yes	DHS PIA
DOJ - Justice Unified Network (JUTNET)	External Connection	Yes	DOJ PIA
Justice Automated Booking Service (JABS)	External Connection	Yes	DOJ PIA
Justice Consolidated Office Network - Common Office	External Connection	No	None
Automation Resources (JCON-COAR)	External Connection	Yes	DOJ PIA
Local and State Agencies – Law Enforcement Online	External Connection	Yes	N/A
National Business Center (Unified Financial Management System-UFMS)	External Connection	Yes	DOJ-PIA
Organized Crime Drug Enforcement Task Force Management Information System (OCDETF MIS)	External Connection	Yes	OCDEFT PIA

APPENDIX B – DATABASES AND ASSOCIATED APPLICATIONS

The below listing identifies the databases in Firebird's Relational Database Management Systems (RDBMS) and the purpose of these databases. These databases are also backed up as part of the backup strategy that Firebird employs. The databases as well as the backups of the data are covered by the privacy documentation for the underlying applications at issue. The database tenants are responsible for ensuring applicable controls are implemented to protect the PII maintained.

Microsoft Office365, One-Drives, SharePoint folders and personal network folders.

Microsoft Access - Microsoft Access is included in the Microsoft Office suite, which is part of the standard workstation image. Note that Microsoft Access should only be used for single-user database applications or a small, limited number of local users. Database applications that span multiple sites or have a large number of concurrent users (greater than 10) should be developed using an enterprise RDBMS such as Oracle or SQL server.

Microsoft Structured Query Language (SQL) Server - Microsoft SQL Server is the database system used for several COTS applications deployed enterprise wide. The database instances run on high performance multi-node clustered servers and use the SAN for storage. Each application has its own database instance, allowing each application to tailor its security settings without affecting the Authorization to Operate (ATO) of other instances on the same node. Other database instances run on standalone servers running SQL Server.

DEA implemented two four-node clustered SQL 2012 Farms to replace the older versions of SQL and the unsupported versions of Oracle. The SQL 2012 Farms are comprised of high-performance HP DL 580 series and BL460c servers and provides high performance, availability, and disaster recovery for the backend databases. Additionally, DEA maintains a SQL 2008 Farm comprised of Dell R710 servers for applications that are not compatible with SQL 2012.

Windows 2008 Enterprise R2 with Service Pack 1 (SP1) is the base operating system for each node within the SQL 2008 and 2012 non-blade clustered environments. Windows Server 2012 R2 is the base operating system for the SQL 2012 blade cluster. The database instances use shared SAN storage for storing database logs, software, and data while the operating system is installed on the local disks.

Both the SQL 2008 and 2012 Farms incorporate a baseline template that is the foundation for all new instances that are added to the environments. The database template is set up in accordance with Microsoft's Best Practices and the NIST 800-53 security controls.

Oracle - The Oracle product line is used by DEA to provide central relational database facilities for a variety of applications. Oracle 12c is the primary database version running in Firebird. Oracle database instances run on specialized HP Integrity series database servers and use the SAN for storage. Each application has its own database instance, allowing each application to tailor its security settings without affecting the ATO of the other applications on the same server. The HP Integrity series servers are based on the Itanium processor architecture. This provides the Web Infrastructure with the highest possible performance for its backend databases. The database servers use shared SAN storage for storing database software and data while the operating system is installed on local disks.

The Oracle database instances, if the application is designed to do so, allows for multiple front-end sources (i.e., Application servers) to interface with a single database instance. The baseline templates are the foundation for all new applications introduced to the Web Infrastructure. Database instance baseline templates will be setup in accordance with the NIST 800-53 security controls.

All Hosted Systems are also backed up if their data is held on servers other than Oracle or SQL or fully or partly saved in the Cloud.