Template Version Number: 01-2021

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
Agency Administrative Support System (AASS)

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 5/5/2022

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO Agency Administrative Support System (AASS)

Unique Project Identifier: PTOC-002-00

Introduction: System Description

Provide a brief description of the information system.

Agency Administrative Support System (AASS) is a major application. It is designed to serve many purposes within the USPTO such as consolidating document imaging, providing a visual representation of the IT facility and resources, providing a centralized repository of information about USPTO IT facilities. It also provides automatic discovery of software, hardware, configuration file, and network devices, managing and tracking automated and software assets, providing USPTO enterprise-wide solutions to identify and track strategic goals and business and organizational information, providing a solution to store data and perform statistical analysis in a secured environment, and collecting, storing, and displaying organizational and performance metric data.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
AASS is a major application.

(b) System location
AASS is located at 600 Dulany Street, Alexandria, VA 22314

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
AASS interconnects with the following systems:

Network and Security Infrastructure System (NSI) is an infrastructure information system and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

Enterprise UNIX Services (EUS) consists of assorted UNIX operating system variants (OS), each comprised of many utilities along with a master control program, the kernel.

Service Oriented Infrastructure (SOI) provides a feature-rich and stable platform upon which USPTO applications can be deployed.

Database Services (DBS) is an infrastructure information system and provides a database infrastructure to support the mission of USPTO database needs.

Consolidated Financial System (CFS) - CFS is a Master System composed of the following four (4) subsystems: 1) Momentum 2) Concur Integration, 3) E-Acquisition (ACQ) and 4) VendorPortal.

Enterprise Desktop Platform (EDP) is an infrastructure information system which provides a standard enterprise wide environment that manages desktops and laptops running on the Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

Security and Compliance Services (SCS) provides a centralized command and control console with integrated enterprise log management, security information and event management network behavior analysis, and reporting through the collection of events, network/application flow data, vulnerability data, and identity information.

Enterprise Windows Servers (EWS) is an infrastructure information system and provides a hosting platform for major applications that support various USPTO missions.

Enterprise Software Services (ESS) provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, PTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc.

Intellectual Property Leadership Management System (IPLMSS) is a master system and facilitates grouping and managing of seven general support subsystems that collectively support the USPTO Director; Deputy Director; Office of the General Counsel (OGC), including OGC's components, the Office of General Law (OGL), Office of the Solicitor, and Office of Enrollment and Discipline (OED); Trademark Trial and Appeal Board (TTAB); Patent Trial and Appeal Board (PTAB); Office of Patent Training (OPT); and Office of Policy and International Affairs (OPIA).

Patent Capture and Application Processing System-Examination Support (PCAPS-ES) consists of several applications that enable patent examiners and public users to search and retrieve application data and images and patent examiners and patent applicants to identify individuals and organizations with intellectual property, pre-grant, and published applications.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

AASS is a major application composed of the following subsystems:

Corporate Imaging Document Management System (CIDM) is a consolidation of all imaging document systems in Corporate Systems Division (CSD) that meets user requirements and conforms to USPTO system infrastructure requirements specified by the Chief Information Officer (CIO) for Automated Information Systems (AISs). CIDM provides similar content management requirements and functionalities to several offices including Vendor Management Division (VMD), Office of Commissioner for Patents (PEO), Office of Enrollment and Discipline (OED), Office of Patent Information Management (OPIM), and the Deputy Undersecretary (DUS).

Collection of Economic Analysis Tools (COEAT) is a COTS product that contains tools needed for data analysis, data management, and graphics and is used by OPIA and USPTO to respond to official requests related to various data sets. COEAT is used by the Chief Economist's office of the USPTO to store data and perform statistical analysis in a secured environment and is fully integrated with the current Windows desktop environment and is accessible to users via the USPTO Intranet (PTONet). COEAT includes hundreds of statistical tools and many data-management commands that provide complete control of all types of data that include byte, integers, long, float, double, and string variables. COEAT generates publication-quality, distinctly styled graphs using an integrated graph editor. To ensure that no unauthorized users access the system, the COEAT applicant has built-in security controls. COEAT collects and maintains PII related to patent examiners and applicants such as age, race, national status, disability status, veteran status, sex, length of service, etc.

Data Center Facilities Management System (DCFMS) creates a centralized repository of information about USPTO IT facilities. Aperture Vista 600 provides a visual representation of the IT facility that is linked to detailed information about the IT resources within that facility. Aperture Vista 600 will allow the IT facility manager to document and track equipment locations, network connectivity, Heating, Ventilation, and Air Conditioning (HVAC) requirements and capacity, and electronic connectivity and capacity. DCFMS is based on Aperture commercial off-the-shelf (COTS) products by Emerson Network Power. DCFMS does not collect, maintain, or disseminate any PII.

Global Enterprise Architecture Repository System (GEARS) provides a holistic view of the USPTO enterprise and helps identify and track strategic goals, business functions, business processes, roles, organizational structures, business information, key performance metrics to technologies including software applications, services, platforms, and network infrastructure. GEARS presents views, roadmaps, and analytics of the current as-is and future to-be state of the enterprise. GEARS supports Enterprise Architecture Division which extends the enterprise interests and relationships to key partners, suppliers, and customers. GEARS is developed using a Commercial-off-the-Shelf (COTS) product called TrouxTM. The repository offered by Troux

allows for a flexible foundation to store data about the agency's business objectives, capabilities, and processes, along with the business linkages to the supporting IT assets. Additionally, Troux ships with a pre-built web front end application that allows users to analyze data relationships, execute and view reports, and (if given sufficient privilege) add or update repository data. GEARS does collect, maintain, or disseminate PII, for example internal names of product owners.

OCIO Data Driven Dash Board (OCIO-DDD) is an intranet only web application that collects, stores and displays organizational and performance metric data for the OCIO office. OCIO-DDD consists of a .NET custom code base. Users have varying levels of permission to view, add, and update metrics and measurements and to view various metric status charts. OCIO-DDD does not collect, maintain, or disseminate any PII.

(e) How information in the system is retrieved by the user

Information in AASS is retrieved via USPTO intranet access, dashboard, SharePoint, and registered accounts.

(f) How information is transmitted to and from the system

Information is encrypted and transmitted to AASS via HTTPS (TLS 1.2) and SSH.

(g) Any information sharing

AASS shares PII within the bureau and DOC bureaus on a case by case basis. AASS shares PII on a case-by-case basis and via bulk transfer with the public. AASS shares PII via bulk transfer with foreign government.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- Title I of the Ethics in Government Act of 1978 (5 U.S.C. app. 101)
- Executive Order 9397
- Executive Order 12674 (as modified by Executive Order 12731)
- 5 CFR Part 2634, Subpart I, of the Office of Government Ethics (OGE) regulations
- Privacy Act at 5 U.S.C. 552a(b)(1).
- GE/GOVT-2 Executive Branch Confidential Financial Disclosure Reports Privacy Act system of records
- 35 U.S.C. 5
- 35 U.S.C. 2
- 5 U.S.C. 301

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

AASS is a Moderate system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☒ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☒
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☒	j. Financial Account	☒
b. Taxpayer ID	☒	g. Passport	☒	k. Financial Transaction	☒
c. Employer ID	☒	h. Alien Registration	☒	l. Vehicle Identifier	☒
d. Employee ID	☒	i. Credit Card	☒	m. Medical Record	☒
e. File/Case ID	☒				
n. Other identifying numbers (specify): Credit card includes just the last 4 digits of the credit card number. The system may include other PII that users have voluntarily submitted, but any instances of PII not requested have been redacted.					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)

a. Name	☒	h. Date of Birth	☒	o. Financial Information	☒
b. Maiden Name	☒	i. Place of Birth	☒	p. Medical Information	☒
c. Alias	☐	j. Home Address	☒	q. Military Service	☒
d. Gender	☒	k. Telephone Number	☒	r. Criminal Record	☒
e. Age	☒	l. Email Address	☒	s. Marital Status	☒
f. Race/Ethnicity	☐	m. Education	☒	t. Mother's Maiden Name	☒
g. Citizenship	☒	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☒	f. Salary	☒	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	☒	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☒		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☒
b. Palm Prints	☐	g. Hair Color	☒	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☒	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☒	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☒	o. Dental Profile	☐
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☐	f. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains

In Person	☒	Hard Copy: Mail/Fax	☒	Online	☒
Telephone	☒	Email	☒		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☒
State, Local, Tribal	☒	Foreign	☒		
Other (specify):					

Non-government Sources					
Public Organizations	☒	Private Sector	☒	Commercial Data Brokers	☒
Third Party Website or Application			☒		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

AASS is secured using appropriate administrative, physical and technical safeguards in accordance with the NIST security controls (encryption, access control, auditing). Mandatory IT Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0012 0651-0017 0651-0080 0690-0035
☐	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☒
For litigation	☒	For criminal law enforcement activities	☐
For civil enforcement activities	☒	For intelligence activities	☒
To improve Federal services online	☒	For employee or customer satisfaction	☒
For web measurement and customization technologies (single-session)	☒	For web measurement and customization technologies (multi-session)	☒
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated

will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

AASS collects, maintains, and disseminates PII about employees, contractors, and members of the public for administrative matters, litigation, civil enforcement activities, to improve federal services online for web measurement and customization technologies (multi and single session), to promote information sharing initiatives, for intelligence activities, for employee or customer satisfaction.

In terms of intelligence activities and information sharing, AASS is a repository for registered patent practitioners and trademark practitioners. Through AASS, OED administers the registration exam and maintains a roster of current patent practitioners. OED also investigates grievances submitted against practitioners, provides public information about disciplinary actions against practitioners, coordinates a nationwide Patent Pro Bono Program for under-resourced inventors seeking free legal help, and administers a Law School Clinic Certification Program where law students gain experience in intellectual property law.

COEAT, GEARS and OCIO-DDD aid in the improvement of federal online services and provide web measurement and customization technologies. COEAT includes hundreds of statistical tools and many data-management commands that provide complete control of all types of data that include byte, integers, long, float, double, and string variables. COEAT generates publication-quality, distinctly styled graphs using an integrated graph editor. GEARS provides a holistic view of the USPTO Enterprise and helps identify and track strategic goals, business functions, business process, roles, organizational structures, business information, key performance metrics to technologies including software applications, services, platforms and network infrastructure. OCIO-DDD is an intranet only web application that collects, stores and displays organizational and performance metric data for the OCIO office.

CIDM system provides content management requirements and functionalities and DCFMS creates a centralized repository of information about Information Technology (IT) facilities of the USPTO. CIDM aids employees by providing content managing and imaging. DCFMS aids in employee satisfaction by providing HVAC services, IT services, and other facility services.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

USPTO has also identified and evaluated potential threats to PII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility and integrity of information. Users are provided one-on-one, weekly, and monthly training. All users have access restriction or permissions based on the built-in security controls of the system. Furthermore, the system has the ability to password protect any sensitive data for added protection. Data retention is managed automatically using IQ Archivist in accordance with records management retention policy. System access to PII/BII data is limited to a restricted set of users.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☐	☐
DOC bureaus	☒	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☒	☒	☐
Private sector	☐	☐	☐
Foreign governments	☐	☒	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: AASS interconnects with the following systems: • Consolidated Financial System (CFS) • Security and Compliance Services (SCS) • Enterprise Software Services (ESS) • Intellectual Property Leadership Management System (IPLMSS) • Patent Capture and Application Processing System- Examination Support (PCAPS-ES) The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized account. The USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, and there is utilization of Active Directory security groups to segregate users in accordance with their functions.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☒	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: Policy: http://www.uspto.gov/privacy-policy	
☐	Yes, notice is provided by other means.	Specify how:

☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Yes, submitting personal information is voluntary. USPTO does not collect PII from applicants, practitioners, or members of the public unless an individual chooses to provide personal information.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Yes, individuals have the opportunity to consent to particular uses of their PII. Individuals consent by choosing to provide information. Submitting personal information is voluntary.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Yes, individuals have the opportunity to review/update their PII pertaining to them. OED forms can be used by applicants and practitioners to update their information. Employees may update their profile information using MyUSPTO.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☐	All users signed a confidentiality agreement or non-disclosure agreement.
☐	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit Logs

☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): ___September 19, 2021___ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☒	Other (specify): Employees and contractors sign a confidentiality agreement or non-disclosure agreement and are subject to a Code of Conduct that includes the requirement for confidentiality.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

All access has role-based restrictions and individuals with access privileges undergo vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. The data is encrypted in transit and at rest. Additionally, AASS is secured by various USPTO infrastructure components, including the NSI system and other OCIO established technical controls to include password authentication at the server and database levels.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: • COMMERCE/DEPT-3: Conflict of Interest Records, Appointed Officials. • COMMERCE/DEPT-10: Executive Correspondence Files. • COMMERCE/PAT-TM-4: Government Employee Invention Rights. • COMMERCE/PAT-TM-7: Patent Application Files. (Note: This notice is broken down, where indicated, into three subsystems relating to the status of the files: a. Pending; b. Abandoned; and c. Patented). • COMMERCE/PAT-TM-23: User Access for Web Portals and Information Requests • COMMERCE/PAT-TM-1: Attorneys and Agents Registered or Recognized to Practice Before the Office • COMMERCE/PAT-TM-2: Complaints, Investigations and Disciplinary Proceedings Relating to Attorneys and Agents Registered or Recognized to Practice Before the Office. • COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: GRS 5.1:020: Non-recordkeeping copies of electronic records. Temporary. Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use. GRS 3.2:020, Computer security incident handling, reporting, and follow-up reports. Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use. GRS 3.2:010, System and data security records. Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. GRS 3.2:030 and 031, System Access Records. Temporary. Destroy when business use ceases.
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☒	Overwriting	☐
Degaussing	☐	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: AASS collects, maintains, or disseminates PII about DOC employees, contractors, and the public. The types of information collected, maintained, used or disseminated by the system includes identifying numbers, Employee ID for example which uniquely identify an individual.
☒	Quantity of PII	Provide explanation: The number of records collected generate an enormous amount of PII. There are approximately 60,000 patent practitioners active. The cases and customers not registered but that access AASS is much larger.
☒	Data Field Sensitivity	Provide explanation: The types of identifying numbers such as credit card and name as well as information about disciplinary action regarding practitioners can be sensitive.
☒	Context of Use	Provide explanation: AASS contains PII regarding grievance investigations submitted against practitioners and provides public information about disciplinary actions against practitioners which if breached could lead to embarrassment and loss of trust.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected, USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with

		NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized accounts. Authorized privileged users access the applications for administrative functions only, and authorized non-privileged users access some applications as required for their roles within their group. The strict access to and secure location of PII lower the PII Confidentiality Impact rating.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

USPTO has also identified and evaluated potential threats to PII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility and integrity of information. Users are provided one-on-one, weekly, and monthly training. All users have access restriction or permissions based on the built-in security controls of the system. Furthermore, the system has the ability to password protect any sensitive data for added protection. Data retention is managed automatically using IQ Archivist in accordance with records management retention policy. System access to PII/BII data is limited to a restricted set of users.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.