Antitrust Division

Privacy Impact Assessment
for the
Antitrust Division Azure Infrastructure as a Service
(ATR Azure IaaS)

Issued by:
Dorothy Fountain
Office of the Chief Legal Advisor
Senior Component Official for Privacy

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

Date approved: February 3, 2022

(May 2019 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.)

The Antitrust Division Azure Infrastructure as a Service (ATR Azure IaaS) is a Microsoft Azure IaaS cloud offering, used to provide general services via the Government Community Cloud (GCC). ATR Technology Support Section (TSS) has procured its own dedicated cloud service instance, using the Department's Microsoft Azure GCC Enterprise License. ATR Azure IaaS supports ATR's criminal and civil investigation and litigation functions, as well as internal ATR administrative functions. ATR's goal is to migrate the majority of its data and application processing into the cloud. Secure connectivity is provided in accordance with the DOJ Cloud Secure Configuration Guide, which requires ATR to leverage Justice Unified Telecommunications Network (JUTNet) Voice Services System (JUTNet) and the DOJ Justice Cloud Optimized Trusted Internet Connection (TIC) to ensure secure connections to the external Microsoft GCC.

Microsoft Azure GCC delivers a certified, approved and authorized service platform built upon the Federal Information Security Management Act (FISMA) foundational principles of security, privacy & control, compliance, and transparency.[1] All government entities that participate in the cloud receive a physically isolated and separate instance of Microsoft Azure within the GCC. These services include the Federal Risk and Authorization Management Program (FedRAMP) and Department of Defense (DoD) compliance certifications, the FBI's Criminal Justice Information Services (CJIS) state-level agreements, and the ability to issue Health Insurance Portability and Accountability Act of 1996 (HIPAA) Business Associate Agreements. All systems are operated by screened U.S. persons and designed to support multiple hybrid scenarios for building and deploying solutions on-premises or in the cloud. Microsoft Azure GCC has been FedRAMP High Impact certified by trusted authorities and registered on the FEDRAMP Marketplace.

The Microsoft Azure GCC ATR subscription includes the core components of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). These services consist of infrastructure, network, storage, data management, and identity management, among others. PaaS and SaaS functions and services have been integrated into the separate system boundaries of Application Management System (AMS), Web Services System (WSS), and Email Collaboration System (ECS) and will not be addressed within this PIA.

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

[1] For more information, see https://csrc.nist.gov/projects/risk-management/fisma-background.

previously unknown areas of concern or patterns.

ATR Azure IaaS is ATR's primary cloud system that provides on demand computing functions for ATR's cloud-enabled applications, files, and office processing. ATR Azure IaaS is accessible to all ATR personnel and processes, stores, and transmits all ATR information in support of ATR's mission to enforce antitrust laws. Data types include investigation and litigation materials collected through issuance of civil investigative demands, search warrants, subpoenas, and discovery requests. These materials may contain a variety of PII about members of the public, including personal contact information, date of birth, and employment information. They may also contain medical or health information, tax identification numbers, and other sensitive information, if relevant to a particular matter. ATR Azure IaaS also processes, stores, and transmits internal human resources information, which may contain personal contact information, date of birth, social security numbers, employment history and performance ratings, and, if relevant, medical or health information. ATR TSS is responsible for administration, operation, and management of Azure functional services.

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
X	Statute	This project is authorized under the Antitrust Division's statutory jurisdictional authorities, which are discussed in Chapter II of the Antitrust Division Manual, Fifth Edition, available at https://www.justice.gov/atr/file/761166/download.
	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.***

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	
Date of birth or age	X	A, C and D	
Place of birth	X	A, C and D	
Gender	X	A, C and D	
Race, ethnicity or citizenship	X	A, C and D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, C and D	SSNs are collected for DOJ personnel. SSNs may also be included in case information from outside entities, although SSNs are not actively collected or requested.
Tax Identification Number (TIN)	X	A, C and D	
Driver's license	X	A, C and D	
Alien registration number	X	A, C and D	
Passport number	X	A, C and D	
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, C and D	
Personal e-mail address	X	A, C and D	
Personal phone number	X	A, C and D	
Medical records number	X	A, C and D	
Medical notes or other medical or health information	X	A, C and D	
Financial account information	X	A, C and D	
Applicant information	X	A, C and D	
Education records		A, C and D	
Military status or other information	X	A, C and D	
Employment status, history, or similar information	X	A, C and D	The collection of this group of information will include business addresses.

(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
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, C and D	
Certificates	X	C and D	
Legal documents	X	C and D	
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C and D	
Foreign activities	X	C and D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	
Whistleblower, e.g., tip, complaint or referral	X	C and D	
Grand jury information	X	C and D	Grand jury information collected is limited to authorized individuals.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C and D	Access to this information is limited to authorized individuals.
Procurement/contracting records	X	C and D	
Proprietary or business information	X	C and D	
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	
- **Video containing biometric data**	X	C and D	
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	C and D	
- **Scars, marks, tattoos**	X	C and D	

(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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	Azure IaaS is operated and administered by DOJ government and contractor personnel.
- **User ID**	X	A	All administrators are provided unique user IDs.
- **User passwords/codes**	X	A	All administrators use unique passwords and Personal Identification Verification (PIV) cards issued in accordance with HSPD-12. [2]
- **IP address**	X	A	IP address information is contained within the system.
- **Date/time of access**	X	A	Access logs with date and time of access are maintained within the system and are generally limited to the user and administrators.
- **Queries run**	X	A	Query runs are maintained within the system and are generally limited to the user.
- **Content of files accessed/reviewed**	X	A	Audit logs of files accessed are stored and reviewed by administrators.
- **Contents of files**	X	A	Contents of all files are available to administrators.
Other (please list the type of info and describe as completely as possible):	X	C and D	Additional personal information could be collected or received through investigations and litigation.

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	✓
Phone	✓	Email	✓		

[2] All administrators use unique passwords and multi-factor authentication. For more information, see https://www.dhs.gov/homeland-security-presidential-directive-12 (HSPD-12).

Other (specify):

Government sources:					
Within the Component	✓	Other DOJ Components	✓	Online	✓
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	✓
Commercial data brokers	✓				
Other (specify):					

Section 4: Information Sharing

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

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	✓		✓	ATR will share information among ATR offices on a case-by-case basis. ATR generally will provide access to data via an Azure IaaS account upon Section Chief/Assistant Chief approval. The requester's access is limited to only authorized data.
DOJ Components	✓		✓	ATR will share Azure IaaS information with other DOJ components on a case-by-case basis. ATR generally will provide direct access to data via an ATR Azure IaaS account upon Section Chief or OCLA approval. The requester's access is limited to only the requested data. Access to, and duration of access to the data will vary based on the data owner or case manager's discretion.

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.**
Federal entities	✓		✓	ATR will share information on a case-by-case basis with federal entities with legitimate reasons for access and approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access. The requester's access is maintained until termination is directed by the legal staff or until the end of a case.
State, local, tribal gov't entities	✓		✓	ATR will share information on a case-by-case basis with state, local, tribal government entities with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via an approved remote account, utilizing a government furnished equipment (GFE) and/or RSA token through VPN, for direct log-in or using the Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
Public	✓			Records submitted to courts are generally publicly available according to court rules.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector	✓		✓	ATR will share Azure IaaS information on a case-by-case basis with the private sector with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via an approved Azure IaaS account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using the Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.

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.**
Foreign governments	✓		✓	ATR will share Azure IaaS information on a case-by-case basis with foreign governments with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via an authorized account, utilizing a GFE and/or RSA token through VPN, for direct log-in. The requester's access is limited to only the requested data. Foreign governments with read access to ATR Azure IaaS are litigating partners in criminal or civil matters. The requester's access is maintained until termination is directed by the legal staff.
Foreign entities				

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.

ATR provides only statistics and case filings to the "Open Data" site (www.data.gov). ATR's public case filings may properly contain PII.[3]

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.

An ATR SORN provides generalized notice to the public.

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

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

[3] ATR provide links on data.gov to ATR's DOJ webpage. Case filings are here: https://www.justice.gov/atr/antitrust-case-filings-alpha. ATR statistics do not contain PII. See: https://www.justice.gov/atr/file/788426/download.

collection or specific uses of their information? If no opportunities, please explain why.

Individuals involved in investigations and litigation are properly notified in accordance with Federal criminal and civil procedures and court rules. ATR obtains the majority of the information stored in Azure IaaS hosted systems through subpoenas, discovery requests, search warrants, civil investigative demands, or second requests under the Hart-Scott-Rodino Antitrust Improvements Act ("HSR" Act).[4] For these information-gathering mechanisms, individua ls do not have the opportunity to decline to provide the requested information and documents. Certain information collected in Azure IaaS hosted systems may be provided voluntarily;[5] however, for information collected from public sources, notice is not provided to individuals because their information is publicly available.

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.

ATR's Privacy Program Plan captures policy and procedures to ensure compliance with Federal and Department FOIA and Privacy Act guidelines regarding requests for information or amendment. All such requests are submitted to the ATR's FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written securityand privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guide lines, 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):** 9/21/2020 **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**

[4] The HSR Act, 15 U.S.C. § 18a, requires parties to certain transactions to notify ATR and the Federal Trade Commission of the transaction and to provide certain documents, and it permits the agencies to make a request for additional information and documents (a "second request").

[5] For example, during the initial waiting period of an ATR investigation under the HSR Act, ATR makes the requests and parties typically voluntarily submit certain information and documents.

	provide a link to the applicable POAM documentation: There are no POAMs that impact privacy within the profile.
n/a	**This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:**
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ATR Azure IaaS has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. The system has been fully incorporated within the ATR General Support System boundary, where it is subject to full system monitoring and audit in accordance with ATR and Department guidelines. All system documentation supporting these activities is maintained within the Department's system of record, Cybersecurity Assessment and Management (CSAM).
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:** ATR Azure IaaS compiles audits at multiple layers, including the network and application processing levels. All logs are reviewed weekly by onsite administrators and then gathered and centrally managed using the Department's audit analysis solution, SPLUNK.[6] All logs are forwarded to the DOJ Security Operations Center (JSOC) for automated analysis and review.
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**. Pursuant to Department policy, contractors are generally required in their contracts to comply with the Privacy Act and other applicable laws. All contractors granted access to ATR Azure IaaS are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All Azure IaaS users are subject to onboarding training that includes computer security awareness and

[6] The Department's Splunk Instance captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

	privacy training, which is an annual requirement thereafter. Additional cloud application level training is offered periodically, as needed for particular functions or users.

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?

All Azure IaaS users are required to use multi-factor authentication or unique username and passwords to access their ATR accounts. Data access is highly restrictive; users require formal approval and authorization to access information on a case-by-case basis. Users can access only data for which they are authorized. All users are required to undergo training and sign formal Rules of Behavior prior to being granted access to the Azure IaaS cloud data.

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.)

Information is disposed of or retained in accordance with Directive ATR 2710.1, "Procedures for Handling Division Documents and Information," ATR Agency Record Schedule or the General Records Schedule consistent with National Archives and Records Administration regulations and records schedules.

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:

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

Section 8: Privacy Risks and Mitigation

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

being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

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

The privacy risks associated with information collected within ATR Azure IaaS primarily relate to the loss of confidentiality, integrity, and availability of data. Access by unauthorized entities to sensitive data, including personal information collected for investigations or litigation, potentially could lead to destruction of that data, compromised identities, exposure of sensitive and personal data, and/or disruption to an ongoing investigation or litigation. ATR Azure IaaS is a FEDRAMP certified government only cloud environment. ATR uses a number of proven protection methods, including secure communications (e.g., JUTNET), malicious code protection and intrusion detection software, active monitoring controls, encryption, and enhanced access control techniques designed to ensure data is protected to the extent possible and in accordance with DOJ Secure Configuration Guidelines and IT security standards.[7]

Additionally, all data collected within Azure IaaS is protected by encryption and file permissions and is viewable only by authorized individua ls, who must authenticate and be given direct permission for each dataset. Some data that is deemed sensitive by the appropriate authorities may be redacted to prevent unauthorized viewing and to render the information unsearchable. All user activity is monitored and audited based on user actions and accesses. Azure IaaS internal user management module manages user access and only allows users the ability retrieve data based on each user authorized role and rights.

To avoid over-collection, data collected is associated with authorized user identities. All other data is processed within other system boundaries that reside within the Azure IaaS cloud, such as Relativity Database Management System, Application Management System, Web Services System, and Email Collaboration System. ATR provides privacy notices through system of records notices (SORNS), published on DOJ's system of records website (https://www.justice.gov/opcl/doj-systems-records), and PIAs

[7] ATR adheres to DOJ continuous monitoring requirements, including encryption for data at rest. For example, any PII datasaved locally to an ATR laptop is protected at rest by FIPS compliant encryption technology. Any laptop device that is not able to be supported by FIPS compliant encryption is defined, and requires use of ATR provided, self-encrypting external hard drives or network attached storage devices. Any ATR use of external hard drives or network attached storage devices must be authorized, strictly controlled, and supported by approved FIPS140-2 encryption standards. Second, ATR assesses DOJ defined core controls annually and all controls at least every three years. Finally, ATR adheres to the OIG schedule for routine FISMA assessment.

(https://www.justice.gov/opcl/doj-privacy-impact-assessments). Additionally, personnel are required to take Computer Security and Awareness Training (CSAT), which incorporates privacy.

Furthermore, privacy specific analysis and reporting is maintained within an authorized DOJ Cybersecurity Assessment and Management (CSAM) profile. The capability to generate reports from Azure IaaS is controlled by permission and limited to authorized personnel in support of the ATR litigating mission.