[Executive Office for Immigration Review]

Privacy Impact Assessment
for the
[EOIR Guest Wireless Network System]

<u>Issued by:</u>
[Marta Rothwarf and Michelle Curry,
Senior Component Officials for Privacy]

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: June 4, 2019

(May 2015 DOJ PIA Template)

EXECUTIVE SUMMARY

The Department of Justice's Executive Office for Immigration Review (EOIR) Guest Wireless Network system (EOIR Guest Wi-Fi) provides wireless network endpoint communications within and between all EOIR sites. The EOIR Guest Wi-Fi system will be located at the non-detained Immigration Courts, i.e., those courts without facilities to detain individuals, and EOIR Headquarters locations to provide Wi-Fi access to EOIR/DHS employees, contractors, respondents (individuals in immigration proceedings), their attorneys or representatives of record, and members of the public appearing in proceedings before the immigration courts, the Board of Immigration Appeals, or the Office of the Chief Administrative Hearing Officer (OCAHO). In coordination with the Department's Justice Management Division (JMD) and its information technology (IT) personnel, EOIR is making the EOIR Guest Wi-Fi available to facilitate equal access to information technology resources for respondents, their attorneys and accredited representatives as that provided to government attorneys. This access is especially critical where EOIR facilities are located in remote locations where other forms of communication resources such as cellular connectivity are limited. This network will also be available to members of the public or the media who appear in EOIR immigration proceedings. These potential users of the EOIR Guest Wi-Fi system will be able to use their Wi-Fi enabled personal electronic devices to make wireless calls if their devices have this technology, access the public internet and through that access their EOIR eRegistry or eInfo accounts or other accessible internet websites. Based on DOJ requirements, users may access the EOIR Guest Wi-Fi system in 4-hour increments during regular EOIR business hours at each facility between the start and end of business no earlier than 6 a.m. and no later than 8 p.m. each business day. Access to the EOIR Guest Wi-Fi system is currently restricted at detention facilities and, if made available at these detention facilities, it will be only available through an access-controlled password that will be generated and maintained by EOIR personnel.

Access to the EOIR Guest Wi-Fi system in the non-detained EOIR facilities requires non-governmental and non-DOJ users to provide the Media Access Control (MAC) address for their personal electronic devices and consent to/accept the DOJ Terms, Conditions of Service, and Use Policy (DOJ Terms of Use). The DOJ Terms of Use inform the user that their MAC address is collected, retained, and that his or her usage is subject to monitoring by DOJ or other authorized government personnel. Users are reminded that by agreeing to the DOJ Terms of Use, they understand that they have no reasonable expectation of privacy regarding any communications or data transiting, stored on or traveling to or from this information system. At any time, the government may for any lawful government purpose monitor, intercept, and search and seize any communication or data transiting or stored on this information system. Any communications or data transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose. Additionally, upon detection of misuse, malware or a virus, access may be immediately terminated and the device will be temporarily blocked. If potentially unlawful activity is detected, information may be released to federal law enforcement authorities and/or judicial authorities. The MAC address information is retained by EOIR's Office of Information Technology (OIT) personnel, including its contractors, and is readily accessible for 30 days online and then moved to EOIR's enterprise back up storage servers for six months (near-line), after which time the information is remotely stored on tape (offline) and is securely erased and destroyed at the end of seven years of offline storage. The online and near-line storage media is overwritten after the information is transferred offline to taped media. Registered users may access the EOIR Guest Wi-Fi system in non-detained facilities in 4-hour increments during regular business hours as stated above unless restricted by the adjudicating official during the course of proceedings or if usage is in violation of EOIR's Electronic Device Usage Policy. Because the system collects the MAC address of an individual's electronic device and the MAC address is linked to an individual or a small group, EOIR is issuing this Privacy Impact Assessment (PIA).

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

(a) The purpose that the records and/or system are designed to serve;
The EOIR Guest Wi-Fi provides wireless network endpoint communications within and between all non-detained EOIR sites. The EOIR Guest Wi-Fi system will be located at the non-detained Immigration Courts and EOIR Headquarters locations to provide individualized Wi-Fi access to EOIR/DHS employees, contractors, respondents (individuals in immigration proceedings), their attorneys or representatives of record, and members of the public appearing in proceedings before the immigration courts, the Board of Immigration Appeals (BIA), or the Office of the Chief Administrative Hearing Officer (OCAHO). These potential users of the EOIR Guest Wi-Fi system will be able to use their personal Wi-Fi enabled electronic devices to access the public internet, make wireless calls if their devices have this technology, and access their EOIR eRegistry or eInfo accounts or other accessible internet websites.

(b) the way the system operates to achieve the purpose(s);
The EOIR Guest Wi-Fi system provides wireless network endpoint communications within and between all non-detained EOIR sites. The system meets Federal Government requirements for securing this type of system. The system uses various security protocols described below at (g) to provide a centralized communications platform for the Authentication, Authorization, and Accounting (AAA)

management of computer data on the EOIR computer network. The individual users connect to EOIR's Guest Wi-Fi system through the use of their personal wireless device's Media Access Control (MAC) address as an identifier once the users accept the DOJ Terms of Use. Once the connection is made at the non-detained EOIR facility, the user is able to access the internet or other wireless enabled functionality, such as wireless calling, in 4-hour time increments.

(c) the type of information collected, maintained, used, or disseminated by the system;
To obtain access to the Wi-Fi connection, guest users' personal device's MAC address is automatically collected because it is required for allocation of a temporary Internet Protocol (IP) address. The MAC address is required to connect the user's personal wireless device to the EOIR Guest Wi-Fi network. This MAC address data is retained online by EOIR for a thirty-day period in order to enable user access to the wireless network during this period and in the event of malware detection. Specifically, if malware is detected, the MAC address information may be used by EOIR's OIT to locate the infected device. By triangulating Wi-Fi access points, either EOIR personnel or Federal Protective Service (FPS) personnel in that EOIR facility would identify the location of the device with the malware and then, in person, identify the specific user with the malware-infected device. Such personnel would notify the user that his or her electronic device has been compromised, as required by DOJ security policy. Additionally, when malware is detected, the MAC address would be used to immediately terminate access to the Wi-Fi system and temporarily block the device. To comply with DOJ computer records retention policy, after the initial thirty-day online storage, the data is moved to six-months of near line storage in readily accessible storage servers and moved to off line remote taped storage for a seven-year period before it is erased and the tapes securely destroyed.

(d) who has access to information in the system;
EOIR OIT government personnel and contractors, who operate under Network Services and System Security and Integrity Staff, have access to this information. If a malware is detected, local Immigration Court or EOIR or FPS personnel may receive this information to assist in notifying the guest user that his or her wireless device is compromised. In the event a potential compromise is detected, DOJ, EOIR or FPS personnel may take additional action to stop access to the system, block the device, and if necessary, share information with federal law enforcement authorities to investigate and take other steps. Users access the wireless guest network system via their personal Wi-Fi enabled electronic devices.

(e) how information in the system is retrieved by the user;
Once the guest user accepts the DOJ Terms of Use, then he or she receive Wi-Fi connectivity and a message notifying him or her of this connectivity. After which, his or her device displays an active Wi-Fi connection icon.

(f) how information is transmitted to and from the system;
All EOIR guest user data is encrypted, and logically separated from the EOIR internal network, from the point where the user data enters the EOIR WiFi Network system until the data leaves the system. User data information is transmitted in encrypted form. If a guest user's personal device is connected to an HTTPS (secure Hyper Text Transport Protocol) website, the data that is sent to/from the guest user device and the HTTPS site is encrypted.

(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
The EOIR Guest Wi-Fi system connects to the EOIR network system, which is part of the DOJ JCON/eWorld General Support System.

(h) whether it is a general support system, major application, or other type of system:
The EOIR Guest Wi-Fi system is a “child” application—that is, it is a subsidiary part of the larger DOJ JCON/eWorld General Support System.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver’s license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

General personal data					
Name		Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender		Telephone number		Military service	
Age		Email address		Physical characteristics	
Race/ethnicity		Education		Mother’s maiden name	
Other general personal data (specify): Media Access Control (MAC) address of the electronic personal device used for Wi-Fi access.					

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify): Media Access Control (MAC) address of the electronic personal device used for Wi-Fi access.					

Distinguishing features/Biometrics - None

Distinguishing features/Biometrics - None					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID		Date/time of access	X	ID files accessed	
IP address	X	Queries run	X	Contents of files	
Other system/audit data (specify): Media Access Control (MAC) address of the electronic personal device used for access. The EOIR Guest Wi-Fi system can automatically track date/time of access. Pursuant to DOJ requirements, Wi-Fi access can be for no longer than 4-hour renewable increments and only during business hours from 6 a.m. to 8 p.m. at each EOIR facility. Queries can be run by EOIR for generic usage analytical statistics, such as number of people accessing the network at any particular EOIR facility and hours of high or low usage. Additionally, EOIR Guest Wi-Fi system usage may be subject to monitoring/logging by the DOJ Justice Management Division (JMD). All traffic is also subject to filtering by JMD. Under the DOJ Terms of Use, users have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, and search and seize any communication or data transiting or stored on this information system. Any communications or data transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose.					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		Email			
Other (specify): Through the users' electronic device (MAC device address) and the log on page to the EOIR Guest Wi-Fi system.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal		Foreign			
Other (specify): EOIR employees and contractors, other DOJ component employees or contractors, and other federal employees or contractors (e.g., DHS and Federal Protective Service personnel) may also utilize the EOIR Guest WiFi network when in EOIR facilities.					

Non-government sources

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers					
Other (specify): Members of the public (including respondents and their family members), public media, and private sector (attorneys and accredited representatives, current law students or law graduates with a sponsor, or reputable individuals) may all be EOIR Guest Wi-Fi system users and as such, must provide the requested information, such as the automatic collection of the MAC address following the user's consent to the DOJ Terms of Use to access the Wi-Fi connection.					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please 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. Please describe the choices that the component 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.)

To minimize risks to privacy, the EOIR Guest Wi-Fi system collects minimal PII from guest users. Only the guest user's Wi-Fi enabled personal device MAC address is collected. The MAC address is required to provide a temporary IP address for connectivity between the EOIR Guest Wi-Fi system and the wireless enabled personal device to the internet. At the end of a four-hour period, access to EOIR's Wi-Fi network is terminated unless the user re-submits an access request, at which time a new 4-hour access time frame is triggered. This limited information is retained on U.S. government equipment that is maintained in a secure setting. Also, to minimize risks and comply with DOJ security policy, EOIR has minimized the retention period for the MAC address to 30-days for online retention in EOIR systems. The device's MAC address is maintained online in order to enable user access to the wireless network and, in the event of malware detection, the MAC address will be used by EOIR personnel to notify the user, as described at Section 1(c) above, that the user's electronic device has been compromised and will be used to immediately terminate the user's access and block the device. The thirty-day online retention period facilitates the ability of EOIR to recognize and prevent the reconnection of malware compromised personal devices to the EOIR Guest Wi-Fi system. The information is then moved to near-line and subsequently to offline taped storage for seven years before it can be securely erased and destroyed under the DOJ computer systems records retention schedule.

The agency carefully considered both IT security requirements and the need to reduce the collection and retention of PII to the absolute bare minimum within this security context.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or

disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): To provide access to the EOIR Guest Wi-Fi network, while at the same time protecting the security of EOIR's information technology system.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The EOIR Guest Wi-Fi will provide equal access to information technology resources for respondents, their attorneys, and accredited representatives as that provided to government attorneys. This access is especially critical where EOIR facilities are located in remote locations where other forms of communication resources such as cellular connectivity are limited. The guest user's personal device MAC address is required to assign a temporary IP address to the device that links the internet to the guest user's device. Guest usage is not tracked or monitored, except for monitoring, logging or filtering for IT security and related purposes. This may include for connectivity and generic usage statistical analytical purposes, and as described in the DOJ Terms of Use and discussed at Section 2.2 above, for monitoring/logging by authorized DOJ or other federal agency personnel to detect any compromise to EOIR Guest Wi-Fi system. If malware is detected, the MAC address may enable the IT Security staff to notify the user that his or her personal electronic device has been compromised, and immediately terminate access and temporarily block the device.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	8 U.S.C. § 1229a; 8 U.S.C. §§ 1324a-c; and Federal Information Security Modernization Act of 2014, 44 U.S.C. § 101 note.
X	Executive Order	Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure & Technology (May 11, 2017).

X	Federal Regulation	8 C.F.R. Chapter V, Subparts A and B, et seq.; 28 CFR Part 68 and 8 CFR § 1003.0.
	Memorandum of Understanding/agreement	
X	Other (summarize and provide copy of relevant portion)	DOJ ORDER 0904, CyberSecurity Program (September 15, 2016), provides the governance framework for uniform policy; implements appropriate privacy protections for DOJ information and information system security; confirms authorities; and assigns responsibilities for protecting information and information systems that store, process, or transmit DOJ electronic information from cyber intrusions. *See* also DOJ Order 2740.1A, Use and Monitoring of DOJ Computers and Computer Systems, revised under DOJ Memorandum 2018-02, Revised Sept. 11, 2018.

3.4 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.)

The guest user's personal Wi-Fi enabled device MAC address is retained online for no more than thirty-days. Wi-Fi access can be for no longer than 4-hour renewable increments and only during business hours from 6 a.m. to 8 p.m. at each EOIR facility. At the end of a 4-hour period, access to EOIR's Wi-Fi network is terminated unless the user re-submits an access request, at which time another 4-hour access time frame is triggered. To comply with DOJ computer records retention policy, after the initial thirty-day online storage, the data is moved to six-months of near line storage, and then moved to off line to taped storage for a seven-year period before it is securely erased and destroyed. This collection falls under the record requirements of the National Archives and Records Administration (NARA) at General Records Schedule 3.2 item 030.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component 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.)

Any collection of PII may pose some risk to privacy through hacking, phishing, or an unexpected breach of the computer system. However, by minimizing this collection of PII to only the MAC address and a thirty-day online retention period, the threats to privacy are significantly reduced. Wireless Guest access is encrypted, segregated, and protected from the wireless access point to the anchor controllers and this process is segregated and isolated from all other network devices. The network is subject to continuous monitoring to prevent outages and security violations. User data information is encrypted via HTTPS and SSL protocols via the internet. Access to this information by EOIR OIT or DOJ JMD IT personnel is controlled by 'need-to-know' requirements, annual training on computer security and the proper handling of PII information is a mandatory requirement for all DOJ and EOIR employees and contractors. Upon completion of annual training all DOJ and EOIR employees and contractors must also sign mandatory Rules of IT Behavior.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components	X			
Federal entities	X			Federal Protective Service may be informed that an issue has been detected with a user's device and may work with EOIR personnel to identify the location of the device and, in person, notify the user of the infected device. DOJ JMD receives all MAC address files and analytical data from EOIR. If unlawful activity is detected, JMD may choose to release this information to other federal law enforcement authorities, including the FBI, the DOJ Computer Crimes and Intellectual Property Division, or DHS. Information may be provided to a court should a search warrant be required.
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures, etc.)

At any time, the government may for any lawful government purpose monitor, intercept, and search and seize any communication or data transiting or stored on this information system. Any communications or data transiting, stored on, or traveling to or from this information system may be disclosed or used for any lawful government purpose. Additionally, generic usage statistics may be collected for analytical purposes. Analytical purposes may include the number of guest users at a particular EOIR facility and the general hours of usage. Usage is subject to monitoring/logging by the DOJ Justice Management Division (JMD). All traffic is also subject to filtering by JMD as described above in sections 2.1 and 2.2. Only EOIR OIT or DOJ JMD IT personnel with a need-to-know may access this information to perform their duties. Also, annual training on computer security and the proper handling of PII information is a mandatory requirement for all DOJ and EOIR employees and contractors. Information will be shared with either an EOIR non-IT employee or Federal Protective Service Officer only in the event that DOJ or EOIR OIT Security personnel detect a security threat relating to a guest user's device and, as a courtesy, the device user needs to be notified of the security threat posed by his or her electronic device. There is no other information sharing affiliated with this collection of information.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information 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 7.	
X	Yes, notice is provided by other means.	Specify how: DOJ Terms of Use is provided at the time the EOIR Guest Wi-Fi Network System user takes affirmative steps to activate the EOIR-Guest Wi-Fi connection on his or her personal device and log on to use the EOIR Guest Wi-Fi system. Among other things, the DOJ Terms of Use includes notice to the user that the user is accessing the EOIR wireless network and that malicious use by any/all computers or devices that connect to the network is prohibited. The guest user is notified that any attempts to install or use anything that

		modifies, disrupts, or interferes in anyway with service is prohibited and that EOIR is not responsible for, nor assumes any liability, for content issues relating to thirdparty websites or spam, malware infections, or viruses that may be on these third party sites. Warning about consequences of misuse are provided. The user is then provided the ability to accept or decline these terms of service. Acceptance results in connectivity in 4-hour increments to the EOIR Guest Wi-Fi network system.
□	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Users can decide that they are unwilling to agree to the DOJ Terms of Use, plus the collection of their device's MAC address, and choose not to access or use the EOIR Wireless Network System.
□	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

□	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Once the user has consented to the terms and conditions for accessing the EOIR Guest Wi-Fi network, information is used only to maintain system security and to notify the user of the potential security defect/hazard posed by his or her electronic device.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

At the time users enable their personal devices to seek access to the EOIR Guest Wi-Fi network, they will be provided clear notice of the DOJ Terms of Use and the opportunity to consent prior to submitting their personal device's MAC device address in order to obtain EOIR Guest Wi-Fi network access. If users decide not to accept DOJ Terms of Use and the collection and online retention of their device's MAC address, then they may not obtain access to the EOIR Guest Wi-Fi network. Additionally, a notice will be posted in the public areas about the EOIR Guest Wi-Fi Network System and access requirements. EOIR also posts separate notice of its policy regarding the use of electronic devices on EOIR premises.

Section 6: Information Security

6.1 Indicate all that apply.

<table>
<tr><td>X</td><td colspan="2">The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: April 20, 2018.
If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:</td></tr>
<tr><td>X</td><td colspan="2">A security risk assessment has been conducted.</td></tr>
<tr><td>X</td><td colspan="2">Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The appropriate security controls are implemented and assessed in the DOJ Cyber Security Assessment Management (CSAM) tool.</td></tr>
<tr><td>X</td><td colspan="2">Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: EOIR uses network management systems and approved user authentication lists to ensure "need-to-know" access. The system is continuously monitored to evaluate system security.</td></tr>
<tr><td>X</td><td colspan="2">Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: EOIR implements "need-to-know" access controls and requires annual computer security and privacy training.</td></tr>
<tr><td>X</td><td colspan="2">Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.</td></tr>
<tr><td>X</td><td colspan="2">Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.</td></tr>
<tr><td>X</td><td colspan="2">The following training is required for authorized users to access or receive information in the system:</td></tr>
<tr><td></td><td>X</td><td>General information security training</td></tr>
<tr><td></td><td>X</td><td>Training specific to the system for authorized users within the Department.</td></tr>
<tr><td></td><td>X</td><td>Training specific to the system for authorized users outside of the component.</td></tr>
<tr><td></td><td>X</td><td>Other (specify): There will be a Quick Reference Guide for WiFi Network guest users.</td></tr>
</table>

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

User data information is unencrypted until it reaches the EOIR WiFi Network system.Thereafter, all EOIR guest user data is encrypted, and logically separated from the EOIR internal network, until such data leaves the system. If a guest user's personal device is connected to an HTTPS (secure Hyper Text Transport Protocol) website, the data that is sent to/from the guest user device and the HTTPS site is encrypted throughout the entire process.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. - Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: DOJ–002, Department of Justice (DOJ) Computer Systems Activity and Access Records, 64 FR 73585-73586 (Dec. 30, 1999), as amended. Available at https://www.govinfo.gov/content/pkg/FR-1999-12-30/pdf/99-33838.pdf.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information about any EOIR Guest Wi-Fi System user's usage may be retrieved from online storage in the event adverse activity is detected within a thirty-day period from where it is stored on the wireless management system maintained on EOIR's JMD computers by reference to the user's stored electronic device's Media Access Control (MAC) address. Beyond thirty days retrieval of information based on the MAC address from near line or taped storage is also possible.