U.S. Department of Justice

Privacy Impact Assessment
for
Giglio Information Systems

Issued by:

Erika Brown Lee, Chief Privacy and Civil Liberties Officer

Date approved: March 2, 2015

(September 2012 DOJ PIA Form)

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).

Introduction

The purpose of *Giglio* information file systems ("files" or "systems") is to enable prosecuting offices to comply with their constitutional obligation to disclose potential impeachment information to defense counsel in federal criminal prosecutions. *Giglio* is the name of a United States Supreme Court precedent that imposes certain obligations on prosecutors to disclose potential impeachment information on federal law enforcement agency witnesses or affiants.[1] This privacy impact assessment (PIA) is being conducted to reflect updates to the Department of Justice's ("Department" or "DOJ") *Giglio* policy. This PIA covers multiple individual *Giglio* information systems that are used by Department of Justice prosecuting offices and investigative agencies. This PIA also provides notice of the Department's maintenance of such information to Government employees as well as to defense counsel and members of the public. It is through this PIA process and other internal policies that the Department has considered the need to ensure that trials are fair, while protecting the legitimate privacy interests of Government employees.

Prosecuting Offices

Although most of the *Giglio* systems are located within the various United States Attorneys' Offices (USAOs), DOJ also has specialized litigation components with independent prosecutorial authorities that maintain *Giglio* systems. These components include the Criminal Division, National Security Division, Civil Rights Division, Antitrust Division, Environmental and Natural Resources Division, Tax Division, and Civil Division. The systems are designed to enable prosecuting offices to consistently and appropriately handle potential impeachment information relating to a federal, state, or

[1] *Giglio v. United States*, 405 U.S. 150 (1972).

local law enforcement witness who may testify in many different cases in federal court over a period of time. It is important to note that not all witnesses or affiants who testify on behalf of DOJ have a *Giglio* file. Even when a *Giglio* file is created, only potential impeachment information which is material to the defense is maintained.[2]

Investigative Agencies

DOJ investigative agencies also maintain their own *Giglio* systems. The DOJ investigative agencies that have the authority to maintain their own *Giglio* information include the Federal Bureau of Investigation, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, Office of the Inspector General, and Office of Professional Responsibility. In addition, other federal agencies having law enforcement agents may be deemed an investigative agency for purposes of *Giglio* requirements (e.g., the Department of Treasury, Internal Revenue Service, agents may be a necessary witness or affiant in a DOJ criminal prosecution in a tax case).[3] These investigative agencies disclose to the prosecuting offices potential impeachment information of witnesses or affiants.

---

[2] Potential impeachment information relating to agency employees may include, but is not limited to, the categories listed below:

a) any finding of misconduct that reflects upon the truthfulness or possible bias of the employee, including a finding of lack of candor during a criminal, civil, or administrative inquiry or proceeding;
b) any past or pending criminal charge brought against the employee;
c) any allegation of misconduct bearing upon truthfulness, bias, or integrity that is the subject of a pending investigation;
d) any prior findings by a judge that an agency employee has testified untruthfully, made a knowing false statement in writing, engaged in an unlawful search or seizure, illegally obtained a confession, or engaged in other misconduct;
e) any misconduct finding or pending misconduct allegation that either casts a substantial doubt upon the accuracy of any witness—including witness testimony—that the prosecutor intends to rely on to prove an element of any crime charged, or that might have a significant bearing on the admissibility of prosecution evidence. Accordingly, agencies and employees should disclose findings or allegations that relate to substantive violations concerning
    i. failure to follow legal or agency requirements for the collection and handling of evidence, obtaining statements, recording communications, and obtaining consents to search or to record communications;
    ii. failure to comply with agency procedures for supervising the activities of a cooperating person (C.I., C.S., CHS, etc.);
    iii. failure to follow mandatory protocols with regard to the forensic analysis of evidence;
(f) information that may be used to suggest that the agency employee is biased for or against a defendant (*See U.S. v. Abel*, 469 U.S. 45, 52 (1984)). The Supreme Court has stated, "[b]ias is a term used in the 'common law of evidence' to describe the relationship between a party and a witness which might lead the witness to slant, unconsciously or otherwise, his testimony in favor of or against a party. Bias may be induced by a witness' like, dislike, or fear of a party, or by the witness's self -interest."; and
(g) information that reflects that the agency employee's ability to perceive and recall truth is impaired.

[3] In early 1997, the Secretary of the Treasury issued the 1996 version of the *Giglio* policy for all Treasury investigative agencies, and that policy remains in effect for all Treasury investigative agencies.

Giglio Policy and Process

Section 9-5.100 of the Department's United States Attorneys' Manual (USAM 9-5.100)[4] outlines procedures for DOJ to organize certain potential impeachment information regarding federal, state, and local law enforcement witnesses and affiants in a system of records searchable by the name of the law enforcement witness/affiant. In 2014, the Deputy Attorney General expanded the scope of this policy in order for DOJ prosecuting offices and investigative agencies to consistently and more easily comply with their constitutional duty to disclose potential impeachment information to defense counsel in criminal cases. Specifically, the Deputy Attorney General amended USAM 9-5.100 to update the policy concerning potential impeachment information for law enforcement witnesses in several important respects, including the candid conversation between a prosecutor and an agency employee; the definition of impeachment information; record-keeping; information that must be provided to agencies; the transfer of *Giglio*-related information between prosecuting offices; and the notification of a prosecuting office of *Giglio* issues when an agency employee is transferred to a new district. The primary source of the impeachment information collected and maintained in the DOJ *Giglio* system of records is the law enforcement witness or affiant herself or himself, or the DOJ investigative agency that employs the witness or affiant.

The purpose of each prosecuting office's *Giglio* information system is not to duplicate what is kept in agency files, but rather to permit prosecuting offices to maintain a more organized, logical, and comprehensive filing system, searchable by the witness's or affiant's name, that allows prosecutors to more efficiently and effectively access and analyze relevant impeachment information about specific witnesses or affiants in order to make consistent decisions about the appropriate handling of the same potential impeachment information in different cases over time.

Types of *Giglio* files

There are various types of *Giglio* files that are collected, maintained, used, or disseminated by the system. These files include potential witness impeachment information, such as records of disciplinary actions. For example, a file could contain specific instances of conduct that may attack the credibility of the witness, including reputation for truthfulness or veracity. This record could include prior court testimony or other statements made while under oath. Other types of *Giglio* information include prior inconsistent statements, reports reflecting witness variations, and other known conditions that could affect the witness's bias, such as animosity toward a defendant, relationship with the victim, or known but uncharged criminal conduct. *Giglio* systems may also track requests and responses for *Giglio* reviews. Tracking systems provide an effective record-keeping functionality and permit the Department to keep track of access and dissemination.

---

[4] The USAM can be located at: http://www.justice.gov/usao/eousa/foia_reading_room/usam/.

System Access

Access to *Giglio* systems is limited to prosecutors who have a case-related or need to know basis. The *Giglio* Requesting Official within each prosecuting office will make a request to the appropriate official within an investigative agency for information.[5] The *Giglio* Requesting Official will then search the files obtained from the investigative agency to determine if it contains any impeachable information. In the absence of this system, the impeachment information, and the analysis of it, would remain in the individual criminal case file in which the witness or affiant previously testified, or a general subject matter file that was not indexed by the witness's name. The former practice made it difficult, if not impossible, to routinely retrieve this information for analysis and review when the same witness or affiant subsequently testified in a different case.

Each prosecuting office is permitted to maintain its own *Giglio* system that is to be directly accessed only by a few senior management personnel within that office. Potential impeachment information on federal law enforcement witnesses and affiants is compiled by prosecuting offices according to the procedures outlined in USAM 9-5.100. Typically, the process involves an inquiry and a request for impeachment information from the prosecutor directly to the individual witness or affiant, and also to the General Counsel's office or manager/supervisor at the agency that employees that witness or affiant. Prosecutors follow similar procedures with regard to witnesses and affiants employed by federal law enforcement agencies not explicitly covered by USAM 9-5.100 and state and local law enforcement agencies.

Giglio systems are used as a support system and are not major applications. Information contained in a *Giglio* system file will be retrieved by selected and authorized employees by using their computer username and password. Currently, it is anticipated that *Giglio* information files will be hosted on the Department's Justice Consolidated Office Network (JCON) system or SharePoint site. SharePoint is a technology that integrates intranet, content management and document management processes. Information retrieved from the system may be sent via email to individual prosecutors both within and outside of the prosecuting office on a case-related need-to-know basis.

Section 2: Information in the System

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

Giglio systems will contain potential impeachment information received from the prospective witness, affiant, agency counsel, or other sources. The potential impeachment information that can be collected, maintained, or disseminated can be comprised of internal investigation materials, prior

[5] Each of the Department of Justice prosecuting offices designates one or more senior official(s) to serve as the point(s) of contact concerning impeachment information. These individuals are known as Requesting Officials.

testimony, written statements, human resources records, complaints from the public, police reports, and/or other disciplinary records.

Identifying numbers					
Social Security	x	Alien Registration		Financial account	
Taxpayer ID		Driver's license	x	Financial transaction	
Employee ID	x	Passport		Patient ID	x
File/case ID	x	Credit card			
Other identifying numbers (specify): Given the broad scope of potential records gathered for *Giglio* purposes, it is possible that the above-checked identifying numbers could be collected, maintained, or disseminated. When considering providing discovery beyond that required by the discovery obligations, prosecuting agencies should always consider any appropriate countervailing concerns, including protecting the privacy interests of witnesses.					

General personal data					
Name	x	Date of birth	x	Religion	
Maiden name	x	Place of birth	x	Financial info	
Alias		Home address	x	Medical information	x
Gender	x	Telephone number	x	Military service	x
Age	x	Email address	x	Physical characteristics	x
Race/ethnicity	x	Education	x	Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation	x	Telephone number	x	Salary	x
Job title	x	Email address	x	Work history	x
Work address	x	Business associates	x		
Other work-related data (specify): Data relating to agency internal investigations (either pending or completed) of employee misconduct, including violations of agency rules and regulations, will be included. Similarly, negative credibility references or findings based on the witness/affiant's prior statements under oath will be included.					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	

Distinguishing features/Biometrics
Other distinguishing features/biometrics (specify): N/A

System admin/audit data					
User ID	x	Date/time of access	x	ID files accessed	x
IP address		Queries run		Contents of files	
Other system/audit data (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	x	Hard copy: mail/fax	x	Online	x
Telephone	x	Email	x		
Other (specify):					

Government sources					
Within the Component	x	Other DOJ components	x	Other federal entities	x
State, local, tribal	x	Foreign			
Other (specify): The majority of impeachment information will come either directly from the witness or affiant himself/herself, from the General Counsel's Office, or manager/supervisor at the agency that employs that witness or affiant. In limited circumstances, impeachment information from state, local, or tribal agencies could be included in the *Giglio* system.					

Non-government sources					
Members of the public	x	Public media, internet	x	Private sector	
Commercial data brokers					
Other (specify): Some information may be gathered from publicly available sources such as the internet, electronic court records, or other sources that are available to any member of the public with computer access (e.g., derogatory news coverage or court decisions that have been critical of an employee's actions, etc.).					

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.)

Due to the especially sensitive nature of the information maintained in this system, a potential threat to privacy that exists in light of the information collected is unauthorized access and unauthorized dissemination of *Giglio* information. With respect to the security of information, it is the Department's policy that access to the data be limited to senior management officials in the prosecuting and investigative offices, and that each prosecuting office with a *Giglio* file system develop its own internal plan to preserve the security and confidentiality of potential impeachment information through proper storage and restricted access. All users must be cleared and vetted by senior management in order to view *Giglio* records. The potential threat to privacy is mitigated by the fact that only a limited number of designated individuals have access to the shared folder. If an internal SharePoint System is used, access is limited to a discrete group of designated individuals, as referenced in Section 1 of this PIA. Also, an internal SharePoint system will track the individuals who access and use the system. All DOJ system users are subject to monitoring and auditing of computer activity.

There is a potential privacy risk that sensitive information will not be adequately protected by prosecuting agencies. This privacy risk is mitigated by authorizing only those Department personnel that have the requisite need to know the information contained in the *Giglio* file. Criminal prosecutors have an affirmative constitutional obligation to disclose to defense counsel in criminal trials material impeachment information about government witnesses or affiants. Department policies also limit the collection of *Giglio* information to enumerated types of potential impeachment information, thereby limiting the impact of creating a negative dossier about potential witnesses or affiants.

An additional threat to privacy is misuse of the information contained in the *Giglio* information file. This threat to privacy is mitigated by DOJ IT security policy. All Department personnel with access to Department networks, and all individuals at contractor facilities working on Department information systems (or providing services) must receive annual Information Technology (IT) security awareness training. This course identifies potential risks and vulnerabilities associated with DOJ-owned information systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on information systems. There is a specific module dedicated to privacy awareness, which includes information on certain federal information privacy laws and requirements, such as the Privacy Act and considerations for the proper handling of personally identifiable information (PII). All users of DOJ-owned systems must also sign a Rules of Behavior agreement, confirming that they have completed the course, and that they abide by the requirements reviewed in the course, in order to use a DOJ-owned IT system. In addition, Requesting Officials ensure that the information in their office's *Giglio* information system is securely maintained and is accessible only upon a request to a *Giglio* Requesting Official or other senior management entrusted with such responsibility.

Another potential threat to privacy is the use of inaccurate information that could potentially harm the reputation of the witness or affiant. This threat is mitigated by the Department's requirement for prosecuting offices to work with investigative agencies to verify that the information is accurate before use. Thus, once impeachment information is entered into the system, prosecutors must request an update from the investigative agency. This practice ensures that the data will remain current and accurate. The investigating agency is responsible for advising the prosecuting office whether any allegation is unsubstantiated, not credible, or resulted in the employee's exoneration. Furthermore, the

law enforcement agent has the opportunity to discuss with the prosecuting office any additional facts that are relevant or helpful to explain the impeachment information. Thus, this privacy risk is mitigated by the fact that *Giglio* information is part of a continuing dialog between the law enforcement officer and the prosecuting office.

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			
x	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		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
x	For litigation		
x	Other (specify): Specifically, the information is being collected to enable prosecutors and investigative offices to effectively fulfill their constitutional obligation to provide impeachment information regarding government law enforcement witnesses and affiants to defendants and their counsel in federal criminal litigation.		

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 U.S. Constitution, case law, and other rules or regulations impose on prosecutors an obligation to disclose to the defendant material impeachment information concerning government witnesses, including law enforcement witnesses or affiants, in criminal cases. If a prosecuting office fails to provide certain impeachment information, that prosecutor could face disciplinary action and dismissal of a criminal prosecution by the court. In sum, the prosecuting offices and investigative agencies will use the *Giglio* information to fulfill their legal and policy obligations.

There are several reasons why the information that is collected, maintained, or disseminated is necessary to further the Department's mission. It is necessary to index *Giglio* information systems by the name of the law enforcement witness. This maintenance will accomplish the efficient and accurate tracking of potential impeachment information relating to law enforcement witnesses. As disclosure questions arise in future cases with regard to the same witness, *Giglio* Requesting Officials can access past analysis and actions, share that information with the current case prosecutor as needed, and give comprehensive legal advice about how the information should be handled in the current case (e.g., whether disclosure is to be provided to the court or defense counsel). The methodical use of *Giglio*

information will further the Department's mission to facilitate a fair and just result in each case, which is the Department's goal in pursuing a criminal prosecution. Thus, providing broad and early discovery often promotes the truth-seeking mission of the Department and fosters a speedy resolution of many cases.

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	28 U.S.C. §§ 516 and 547
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
x	Other (summarize and provide copy of relevant portion)	(1) USAM 9-5.100 (2) *U.S. v. Giglio*, 405 U.S. 150 (1972) (3) Memorandum from the Deputy Attorney General, Amendment of Section 9-5.100 of the United States Attorneys' Manual (The "*Giglio* Policy") (5/12/2014)

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 retention period for *Giglio* systems are strictly regulated by the USAM 9-5.100. Upon being notified that an agency employee has retired, transferred to an office in another judicial district, or been reassigned to a position in which the employee will neither be an affiant nor witness, and subsequent to the resolution of any litigation pending in the prosecuting office in which the agency employee was involved, the Requesting Official shall remove from the prosecuting office's system any record that can be accessed by the identity of the employee. The information must be removed at the conclusion of the direct and collateral appeals, if any, of the case in which the witness or affiant participated, or within one year of the agency employee's retirement, transfer, or reassignment, whichever is later.

Records are retained and destroyed in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration (NARA). Retention periods vary depending on the type of the record. The General Records Schedule (GRS) for *Giglio* files is GRS 20.

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.)

With respect to quality control and reliability of information, prosecuting offices must request an update from the investigative agency. This ensures that the data will remain current and accurate. With respect to the security of information, policy requires that access to the data be limited to those individuals with a need to know the information in order to perform their job. Typically these individuals will be senior prosecuting management officials and trusted senior administrative support personnel. In addition, each office with a *Giglio* system of records must develop its own internal plan to preserve the security and confidentiality of potential impeachment information through proper storage and restricted access.[6] Also, as noted above, the information will be purged from the system at the conclusion of direct and collateral appeals, if any, of the case in which the witness or affiant participated, or within one year of the agency employee's retirement, transfer, or reassignment, whichever is later.

Another privacy control mandates that each Department office with a *Giglio* system of records independently develop a plan to preserve the security and confidentiality of the potential impeachment information in the system.[7] Note that in rare cases the information could be shared with persons outside the Department of Justice, but only in connection with a criminal case to which the United States is a party, or where otherwise authorized by law. Individual prosecuting offices and investigative agencies have periodic *Giglio* training as new employees come on-board or updates in law and/or policy occur.

The witness/affiant, the agency that employs that person, and the prosecutor all have a strong interest in ensuring that the information is accurate and kept secure. Furthermore, Department employees must be aware of the rules guiding affirmative disclosures of information. Rules of professional conduct in most jurisdictions also impose ethical obligations on prosecutors regarding discovery in criminal cases. Each prosecuting office is required to develop individual *Giglio* plans to make certain that information contained within the *Giglio* information files will not be disclosed to persons outside the Department except in a criminal case to which the United States is a party, and where otherwise authorized by law, regulation or court order. Privacy risks are mitigated by the fact that disciplinary action can be taken against any individual using information inappropriately. Therefore, there are significant repercussions associated with misuse of information or wrongful disclosure of information contained in *Giglio* files.

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.

[6] *See* USAM 9-5.100, paragraph 7(b).
[7] *See* USAM 9-5.100, paragraph 12(b).

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			
State, local, tribal gov't entities	X			
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			*Giglio* information may be disclosed to the court or defense counsel in a federal criminal prosecution.

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.)

The Department recognizes the sensitivity of the impeachment information contained in each *Giglio* information system. As a result DOJ imposes strict information sharing and access controls on each office that maintains *Giglio* information. USAM 9-5.100 specifically requires each office that compiles a *Giglio* system to ensure that the information is securely maintained and is accessible only upon a request to a *Giglio* Requesting Official or other senior management entrusted with responsibility. The information shall only be disclosed to requesting individuals within that office on a case-related, need to know basis.[8] Before the information can be disclosed, the prosecutor must show that there is a case-related need. Once the requisite need is established, the *Giglio* Requesting Official must seek an update of the status of the information from an agency official.[9] For cross-jurisdictional criminal cases, *Giglio* information may also be disclosed to prosecutors in another office if the witness/affiant testifies in another jurisdiction. System administrators may have an occasional need to

[8] *See* USAM 9-5.100, paragraph 7(b).
[9] *See* USAM 9-5.100, paragraph 7(c).

access the information files. A similar duty to update the information exists in this circumstance.[10] These procedures work together to ensure the appropriate use 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.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. DOJ/017, *Giglio* Information Files, 80 Fed. Reg. 16025 (Mar. 4, 2015).	
X	Yes, notice is provided by other means.	Specify how: Prosecutors and investigative components are expected to inform the witness/affiant about the proceeding should tell the witness/affiant when potential impeachment information has been disclosed either to the defense or to the court. Similarly, prosecutors have an obligation under the policy to inform the employing agency about what use they will make of the potential impeachment information.[11]
	No, notice is not provided.	Specify why not:

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

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Individuals cannot decline to serve as witnesses or affiants; and testifying, or being an affiant, in a criminal case is part of the basic duties of law enforcement employees.

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:

[10] *See* USAM 9-5.100, paragraph 10(b).
[11] *See* USAM 9-5.100, paragraph 8.

X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: As a general matter, law enforcement officers are required to testify as part of their job duties. If they decide not to consent to use of the information, they may not be able to perform as law enforcement officers. Law enforcement officers have both an obligation and an opportunity to engage in vigorous discussions with the prosecutors about the method of disclosure, including asking the court for a protective order or other methods of protecting the information from further disclosure.

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.

Clear and conspicuous notice of the collection and dissemination of information in the *Giglio* system of records will be provided in the System of Records Notice (SORN), published in the Federal Register. This notice mitigates the risk that the individual will not know that the information is being collected. In addition to the SORN, law enforcement officers are also made aware and are expected to assist in the disclosure of the information to prosecutors, the court, and the defense. One part of a law enforcement officer's responsibility is to testify in court, as needed. As a result, law enforcement officers are made aware that their credibility could be impugned by opposing counsel for conduct, both on and off duty.

Individuals are also notified verbally by prosecuting offices. Prosecutors must discuss *Giglio* information with law enforcement officers prior to providing a sworn statement or testimony in any investigation or case. Legally, prosecuting and investigative offices are constitutionally required to acquire, maintain, and disclose for law enforcement purposes, records obtained from federal and state agencies' personnel records relating to impeachment information that is material to the defense. As noted above, individual law enforcement witnesses and affiants have an affirmative obligation to inform the prosecutor of any conduct that may be potential impeachment information prior to providing a sworn statement or testimony, even in the absence of a specific request. Typically, Special Agents in Charge (SACs) and other supervisory law enforcement officials must take all necessary actions to ensure that its employees are aware of potential impeachment issues affecting personnel. In short, law enforcement officers are on notice that providing impeachment information for disclosure is one important part of the criminal prosecution process.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: 6/28/2012, Justice Consolidated Office Network (JCON).[12] If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:		
X	A security risk assessment has been conducted.		
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Certification of system against National Institute of Science and Technology Publication (NIST) 800-53 security controls, valid authority to operate (ATO). Risk rating of system is "moderate," Federal Information Standards Publication-199.		
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Continuous monitoring is provided by Intrusion Detection/Prevention System and Security Information and Events Management System by EOUSA SOC (Security Operations Center). In addition to the continuous on-line monitoring and audit trail capability, there are capabilities to alert personnel of any unusual or inappropriate activity.		
X	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: All accesses to the JCON system are monitored against failed attempts and require HSPD-12 PIV card authentication logons. The PIV card provides an additional layer of user authentication. Additionally the EOUSA SOC monitors 24x7x365 intrusion attempts and improper usage.		
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.		
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.		
X	The following training is required for authorized users to access or receive information in the system:		
	X	General information security training	
	X	Training specific to the system for authorized users within the Department.	
		Training specific to the system for authorized users outside of the component.	
		Other (specify): All Department users must take Computer Security Awareness Training (CSAT).	

[12] This PIA covers multiple systems, so the answers to Section 6 may cover most, but not all of the *Giglio* information systems.

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

The Department employs a variety of security controls which are designed to protect the privacy of law enforcement officers from unauthorized access and disclosure. General access to Department of Justice workspaces, as well as access to data, is carefully controlled. All users of the *Giglio* information systems must undergo a suitability check as part of their employment at the Department of Justice and before access is granted to Department IT systems. DOJ employees at every prosecuting office and investigative agency must certify that they understand the rules associated with protecting PII before they are granted access to information. The vast majority of *Giglio* systems are maintained on the USAO's internal version of the Justice Consolidated Network (JCON) systems and those security controls are listed above. In limited circumstances, *Giglio* information can be uploaded into SharePoint database, for tracking manageability. If there are future technical changes to any *Giglio* system that would impact privacy, the Department can provide an update to this PIA if and when necessary.

With respect to physical controls, Department office spaces are protected by locked doors and video surveillance. Further, Department offices are patrolled by Federal Protective Services or other private security guards. DOJ computers are subject to monitoring, and all employees are subject to disciplinary action for violating the rules of behavior. All DOJ employees must utilize authentication information, including username and password, in order to gain access to network drives and SharePoint sites. With respect to actual access to *Giglio* information, role-based access is granted by network administrators to the *Giglio* folder contained on the JCON network or SharePoint site. Only those individuals with access privileges are permitted access to the system or SharePoint site. These robust auditing and access measures mitigate the risk of unauthorized access and use.

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-017, *Giglio* Information Files, 80 Fed. Reg. 16025 (Mar. 4, 2015). This System of Records Notice replaces JUSTICE/USA-018, 65 FR 75308.
	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.

The information in the system about United States citizens and/or lawfully admitted permanent resident aliens will be retrieved by witness or affiant name, case name, or other personal identifier. In most cases, the information will be retrieved by the name of the witness or affiant.