Criminal Division

Administrative Privacy Impact Assessment
for the
Gambling Device Registration System

Issued by:

Raymond Hulser
Criminal Division, Senior Component Official for Privacy

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

Date approved: 4-26-2018

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The United States Department of Justice (DOJ), Criminal Division (CRM), Office of Enforcement Operations (OEO), facilitates the legal obligation placed upon the Attorney General to maintain registration records for persons or entities engaging in certain activities involving gambling devices,[1] in accordance with the Gambling Devices Act of 1962,[2] and the Johnson Act, as amended.[3] The Gambling Device Registration System (GRS) collects and maintains the registration information submitted by persons or entities engaged in the business of manufacturing, repairing, reconditioning, buying, selling, leasing, using, or making available for use by others gambling devices before any such device enters interstate or foreign commerce.

CRM conducted this Administrative Privacy Impact Assessment[4] to assess and mitigate the risks to the information in identifiable form (IIF) collected in this system, which includes but is not limited to, an individual's name, business address, business phone number, and business e-mail.

Section 1: The Type and Purpose of the System and Information Collected and Stored within the System:

1.1 What is the purpose for which the records and/or system were designed to serve the agency?

The Gambling Devices Act of 1962 requires any person or entity engaged in activities involving gambling devices, their subassemblies, or constituent parts, to register annually with the Attorney General. Registration is required when the activities affect interstate or foreign commerce and involve manufacturing, repairing, reconditioning, buying, selling, leasing, using, or making a gambling device available for use by others. The Attorney General has delegated this function to CRM OEO.[5]

---

[1] Under the Gambling Devices Act of 1962, the term "gambling device" means:

(1) any so-called "slot machine" or any other machine or mechanical device an essential part of which is a drum or reel with insignia thereon, and (A) which when operated may deliver, as the result of the application of an element of chance, any money or property, or (B) by the operation of which a person may become entitled to receive, as the result of the application of an element of chance, any money or property;

(2) any other machine or mechanical device (including, but not limited to, roulette wheels and similar devices) designed and manufactured primarily for use in connection with gambling, and (A) which when operated may deliver, as the result of the application of an element of chance, any money or property, or (B) by the operation of which a person may become entitled to receive, as the result of the application of an element of chance, any money or property; or

(3) any subassembly or essential part intended to be used in connection with any such machine or mechanical device, but which is not attached to any such machine or mechanical device as a constituent part.

15 U.S.C § 1171(a) (2012).

[2] *Id.* §§ 1171–78.

[3] *Id.* § 1175 *et seq.*

[4] The DOJ Administrative PIA is designed primarily for those systems used for administrative purposes and contains fewer questions than the traditional DOJ PIA template. The contents of the Administrative PIA template, however, document all requirements set forth by Section 208(b)(2) of the E-Government Act of 2002, 44 U.S.C. § 3501 note, and OMB policy.

[5] 28 C.F.R. § 0.55(h) (2017).

GRS automates the collection and preservation of these registrations. Pursuant to statutory authorities, OEO has collected and preserved this information for many decades. As such, GRS does not constitute a new type or collection purpose. Instead, GRS provides an enhancement to the administration and efficiency of the program.

GRS is a web-based database system that: 1) serves as the public interface for registrants to submit or renew gambling device registrations; 2) allows OEO to validate the information against previous submissions; and 3) serves as the official record of the registration on behalf of the Attorney General. GRS is an application in the Custom Database Applications System (CDAS or IT System) and resides on CRM's unclassified network (JCON-IIA).

1.2 What information in identifiable form (IIF) is made available or is to be collected, maintained, used or disseminated by the system (e.g., identifying numbers, general personal data, work-related data, distinguishing features/biometrics, system admin and user data)?

GRS collects IIF required for compliance with the Gambling Devices Act of 1962 and other federal statutes that regulate gambling devices, including:

- Registrant's name;
- Any trade name under which the registrant does business;
- Name and title of officer(s) or owner(s) of the business, company, organization, or tribe;
- Address of the registrant's place of business - or home address, if not engaged in business;
- Address where required gambling device may be viewed; and
- Each gambling activity the registrant intends to engage in during the calendar year.

GRS collects IIF to effectuate necessary communications with the registrant or for historical record-keeping purposes, including:

- Name of the individual or agent completing the form;
- Previous registrant numbers, if previously registered;
- Registrant phone number; and
- Registrant e-mail address(es).

GRS also creates IIF, including:

- DOJ Records Number (DJ#), which is assigned by the database and also serves as a registrant number;
- Effective date of the registration; and
- Official DOJ letter confirming the date of the registration.

Finally, GRS collects and maintains audit log information from system users to monitor and account for system access and user activity.

1.3 About whom (e.g., government employees, members of the public, individuals associated with investigations) and from whom is the IIF collected (e.g., directly from individual about whom the information pertains, government or non-government sources)?

GRS collects and maintains information on the owners, agents, or corporate officers who register that they are engaged in:

(1) manufacturing gambling devices, if the activities of such business in any way affect interstate or foreign commerce;
(2) repairing, reconditioning, buying, selling, leasing, using, or making available for use by others any gambling device, if in such business he or she sells, ships, or delivers any such device knowing that it will be introduced into interstate or foreign commerce; or
(3) repairing, reconditioning, buying, selling, leasing, using, or making available for use by others any gambling device, if in such business he or she buys or receives any such device knowing that it has been transported in interstate or foreign commerce.

This information is collected directly from the registrant. GRS collects and maintains audit log information on the actions of the DOJ employees with access to GRS.

Section 2: The Uses and Sharing of Information Collected and Stored within the System:

2.1 What are all the Department's intended uses of the IIF collected (e.g., criminal law enforcement, intelligence matters, civil enforcement, administrative matters, public affairs, or human resources)?

OEO's primary use for this information is to facilitate the registration requirements of the Gambling Devices Act of 1962 and other federal statutes that regulate gambling devices. Other components of the DOJ may use this information to investigate and/or prosecute individuals that sell, deliver, or ship in intrastate, interstate, or foreign commerce or own, possess, or have in his or her custody any gambling device that is not marked and numbered as required by the Gambling Devices Act of 1962. The information collected and maintained in GRS may be used for other criminal and civil law enforcement purposes, including, enforcement of federal, state, local or tribal gaming laws.

GRS audit log information is used for tracking user access and computer activity to support the audit requirements of DOJ IT systems and protect DOJ information and IT systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Audit log information is used by IT system and security personnel, or persons authorized to assist these personnel, for the purpose of planning and managing IT system services and to otherwise perform their official duties.

2.2 Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the intended uses described above and to further the component's and/or the Department's mission. Indicate legal authorities, policies, or agreements that authorize collection of the information in the system.

The information collected is the minimum amount necessary to satisfy statutory requirements and the least intrusive for the system management. The collection of the name of the owner/agent, type of activity involved, and business and records addresses meet the requirements of the Gambling Devices Act of 1962 and the Johnson Act. Collection of the mailing address, e-mail, and phone number enables communication between OEO and the registrant and automation of the registration process. Additionally, they serve as a means of verifying the authenticity of information requests or changes from the registrant. The assigned registrant number allows for continuity of successive years' registrations, as well as the eventual archiving of the record.

2.3 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 or necessary.

GRS has a built in retention and disposal process. GRS categorizes a record as closed when the registrant ceases to re-register for three years. Records are maintained in GRS for seven years after they are closed. An annual automated process identifies records that have met this criteria in order to effect notification to the Records Management Unit, after which they are purged from the system. Maintenance and disposition is defined under National Archives and Records Administration schedule N1-060-08-012.

2.4 With whom does the component intend to share the information in the system (e.g., within the component, other Department components, foreign/federal/state/local authorities, public, etc.) and how will the information be shared (e.g., case-by-case basis, bulk transfer, or direct access)?

Information from GRS is shared on a case-by-case basis only. It may be shared within DOJ to those that have a need for the information in the performance of their duties.

GRS information can be shared with federal, state, local, and tribal law enforcement or gaming authorities pursuant to their official duties.

Information pertaining to a specific record in GRS can also be shared with the submitting registrant or their agent, as listed in the system.

To the extent that the registration information is a record maintained in a system of records, DOJ may disclose records only in a manner consistent with the Privacy Act of 1974,[6] or the Freedom of Information Act, as amended.[7]

2.5 Are there any potential threats to privacy that exist in light of the information collected or shared? 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.

Privacy Risk: Unauthorized access or misuse of information
Mitigation: DOJ employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. Employee access to this system is limited based on a need-to-know and further delimited by restrictions which limit users to the minimum access needed. Once those criteria are met and management approval is received, access is granted. This IT system makes use of a Personal Identity Verification (PIV) card and pin number for user authentication. It also has been evaluated and authorized to operate according to the risk management framework required by the Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113–283; December 18, 2014). An audit log is maintained and clearly visible on the screen when the user is logged into the system.

Additionally, DOJ employees complete annual training regarding handling of IIF as part of their Cyber Security and Awareness Training (CSAT).

The IT system assessment is documented in the DOJ the Cyber Security Assessment and Management (CSAM) assessment tool and maintained as part of the DOJ ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. There is no outside access to this system; access is restricted to the few DOJ employees who administer the program.

In completing the online form, registrants are asked to e-mail the completed registration form to the Department as an Extensible Markup Language (XML) file. The uploading of information from an XML file allows for direct entry from the registrants while negating the need to create a public interface or user accounts.

The approved DOJ employees act as a gatekeeper for all information leaving the system.

Privacy Risk: Over-collection
Mitigation: The careful minimization of information collection was considered in the design of this database. The system solicits and collects the minimum amount of required information through structured data fields to help limit the possibility of over collection. OEO requests the

[6] 5 U.S.C. § 552a (2012)
[7] *Id.* § 552.

least intrusive data reasonable to satisfy the requirements of the statute and administer GRS. Additionally, the information collected is specifically designed to relate to the registrant's business information instead of personal information, where possible.

Privacy Risk: Erroneous Information
Mitigation: Information is entered directly by the registrant to minimize the possibility of error. Upon receipt, GRS validates the data fields as an initial measure to ensure accuracy. GRS then scans the database for closely matching records and packages. Pursuant to the training provided to system users, an employee conducts a second review of the data for accuracy and manually searches GRS for similar or corresponding records. An approved registration generates an automated notice that is e-mailed back to the registrant, providing confirmation and an additional level of review.

Privacy Risk: Misidentification
Mitigation: Misidentification could occur during two processes: 1) the annual re-registration process; and 2) during retrieval of a record for correction by the registrant or for a law enforcement or gaming authority.

During the initial step of the re-registration process, the system generates an e-mail, which is sent to the e-mail address provided by the registrant in the previous year's registration. The registrant is instructed to review the form, make necessary changes, and submit the form again. Re-registrations that are determined to contain information that is identical to the previous year's submission are automatically approved by GRS. Re-registrations with any variances go through the process described above, under "erroneous information."

The correct identification of a retrieved record is confirmed when the employee reviews the registrant number and other verifying information.

Section 3: The Security of the Information Collected and Stored within the System:

3.1 What controls has the component put into place to ensure that the information is handled, retained, and disposed appropriately (e.g., access/security controls, monitoring/testing/evaluation, auditing, privacy training, automatic purging of information, MOUs)?

With any system involving employee action, training is a vital component in the proper handling, maintenance, and disposal of records. All DOJ employees are required to complete mandatory CSAT training, as well as read and agree to comply with DOJ Information Technology Rules of Behavior. This occurs during their orientation upon entering into service with DOJ and annually thereafter. Additionally, OEO provides one-on-one training for employees granted access to GRS, and maintains a Standard Operating Procedure for the system.

GRS operates on the CDAS IT system, which implements access monitoring, privacy and records controls standardized by the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems, as defined in NIST Special Publication 800-53.

3.2 Has a Certification and Accreditation been completed for this system? If yes, please provide the date; if one is underway, provide a status or completed expected completion date.

Yes. CRM uses CSAM to manage information IT system assessments and the CDAS Authorization to Operate (ATO). ATOs are granted after a Certification and Accreditation (C&A) has been completed. GRS is currently operating under the CDAS ATO signed on October 25, 2017.

3.3 Has the security risk assessment been completed for this system? If yes, please provide the date.

Yes. The security risk assessment is performed as part of the CSAM process (see Section 3.2, above). All CRM IT Systems are subject to the Continuous Diagnostics and Monitoring (CDM) system, which includes constant vulnerability assessment.

3.4 Do contractors have access to the system, and if yes, can you confirm that there are (a) provisions in their contract binding them under the Privacy Act; and (b) information security provisions in their contracts required by DOJ policy?

Whether the contract is executed by the Justice Management Division or the Criminal Division, all contracts have provisions requiring contractors to comply with the Privacy Act and information security provisions in their contract, as required by DOJ policy.

Section 4: Notice, Consent, and Redress:

4.1 Will individuals be notified if their information is collected, maintained, or disseminated by the system (e.g., system of records notice, Privacy Act 552a(e)(3) notice)? Please specify.

The DOJ Gambling Device Registration webpage was created to centralize information regarding the gambling device registration process.[8] Registration requests are completed via the "Request for Registration Under the Gambling Devices Act of 1962" form (OMB No. 1123-0010

[8] https://www.justice.gov/criminal-oeo/gambling-device-registration.

(7/31/2017)), available at the Gambling Device Registration webpage.[9] To accompany the Request for Registration form, OEO created "Frequently Asked Questions"[10] and "Tips on Completing a Registration Request,"[11] whitepapers that provide further information to the public on the uses of this information, how to make changes, and which portions are public information.

4.2 Do individuals have the opportunity to decline to provide information? Please specify.

No. Registration is mandatory for all persons subject to the registration requirements of the Gambling Devices Act and the Johnson Act. The registrant would assume the risk of criminal or civil penalties by federal, state, local, tribal, or gaming authorities should he or she fail to register. Persons who fail to register, in full or in part, when engaged in activities that require such registration can face federal fines of up to $5,000 and imprisonment of up to two years.[12]

4.3 Do individuals have the opportunity to consent to particular uses of the information? Please specify.

No. The IIF collected is used for the purposes required by statute or necessary for the effective operation of GRS. The routine uses of this information are described in the System of Records Notice. An individual need not decline to provide consent for these uses.

Section 5: Privacy Act:

5.1 Is a system of records being created under the Privacy Act, 5 U.S.C. § 552a? If yes, indicate the existing system of records notice or whether one is being developed.

While GRS is currently covered by the existing Criminal Division System of Records Notice JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24155 (May 25, 2017), as a discretionary matter, the Criminal Division is in the process of publishing a new SORN in order to provide increased transparency about GRS and the gambling device registration records.

[9] https://www.justice.gov/sites/default/files/pages/attachments/2016/05/09/gdr-form-v2.0.8.pdf.
[10] https://www.justice.gov/criminal-oeo/file/623891/download.
[11] https://www.justice.gov/criminal-oeo/file/623896/download.
[12] *See* 15 U.S.C. § 1176 (2012) (outlining the penalties for violating certain provisions of the Gambling Devices Act).

5.2 Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved (e.g., name or other personal identifier.)

Information in this system is retrieved by a registrant/agent name, business name, registrant number or address.