

Date of Approval: **October 01, 2020**

PIA ID Number: **5461**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Get My Payment, GMP

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Get My Payment, GMP 4b

What is the approval date of the most recent PCLIA?

4/14/2020

Changes that occurred to require this update:

Significant System Management Changes

Were there other system changes not listed above?

Yes

What were those changes?

First Change User will be able to view the status of multiple Economic Impact Payments (EIP) on one screen Second Change Users that have a no payment date and no bank account information on file will have the ability to request a debit card (or provide bank routing information from original scope) If the users opt for a debit card, no additional shared secret based authentication will be required (for bank account information, the second set of authentication will still be required) Third Change The status will indicate if the user opted for and/or were paid by debit card.

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Small Business and Self Employed (SB/SE)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

Get My Payment, (GMP) application allows taxpayers receiving a stimulus payment to check the status of their payment. After authenticating using shared secret (SSN and address), the system will provide the status of the payment and or the date of delivery. The GMP application will request refund information from Customer Account Data Engine (CADE2). GMP will be storing Taxpayer extract information from CADE2. The system uses shared secret credentials to authenticate the taxpayer. The shared secret credentials are matched against the data from the CADE2 Extract and matched users will be able to see their Stimulus Status. If the payment has not been issued already, then users will have an option to enter their bank account information to receive the payment as direct deposit into their account or opt to receive the payment as a debit card.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

Another compelling reason for collecting the SSN

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

This application does truncate the Social Security Number (all digits are masked). The application cannot mitigate the use of Social Security numbers until an alternate identifier has been adopted by the IRS to identify taxpayers.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record.

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Date of Birth

Financial Account Numbers

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Status of the refund and or the date of delivery

Cite the authority for collecting SBU/PII (including SSN if relevant)

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The SSN is collected from the taxpayer to assist in the authentication, prior to providing them with payment status information. After entering their SSN and address, the system will provide the status of the payment and or the date of delivery. The system uses shared secret credentials to authenticate the taxpayer. The shared secret credentials are matched against the data from the CADE2 Extract and matched users will be able to see their Payment Status. If the payment has not been issued, users can choose to either opt for a debit card, or enter the bank account information (account number, routing number and account type) to receive the payment as direct deposit.

How is the SBU/PII verified for accuracy, timeliness and completion?

The validation process will verify the accuracy and completeness of the information in accordance with the business rules. The Get My Payment (GMP) system will store the PII that is coming from the CADE2 Extract to provide the payment status, the extracts will be sent daily to GMP. GMP, upon additional shared secret validation will be collecting banking information for certain taxpayers and providing the extract of these to the Individual Master File (IMF).

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: CADE 2
Current PCLIA: Yes
Approval Date: 10/30/2019
SA&A: Yes
ATO/IATO Date: 2/12/2020

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: CADE 2
Transmission Method: HTTPS
ISA/MOU No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: SECURITY AUDIT & ANALYSIS SYSTEM (SAAS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 6/11/2020

System Name: Individual Master File
Current PCLIA: Yes
Approval Date: 10/3/2019
SA&A: Yes
ATO/IATO Date: 11/26/2019

Identify the authority:

Coronavirus Aid, Relief, and Economic Security (CARES) Act.

For what purpose?

For taxpayers with a payment status of "need more information", the system collects their banking information and sends it to IMF as a periodic extract.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Yes

When was the e-RA completed?

4/9/2020

What was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity
Confidence based on Single Factor Identity Validation

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number. Using Get My Payment (GMP) is voluntary, and the retrieval of tax information will be tracked. A privacy notice will be placed on the entry page of the tool.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

This system is used solely at the discretion of the user to retrieve their stimulus, individuals are not required to use the application.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

The taxpayer has due process by calling or visiting the IRS.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

System Administrators: Read Write

IRS Contractor Employees

Contractor Developers: Read Only

How is access to SBU/PII determined and by whom?

Access to the data by taxpayers is determined by the taxpayer entering valid shared secrets for the purpose of authentication. Once they enter shared secrets and their data matches up with the CADE 2 information to ensure that the information is correct, they are eligible to use the system. IRS System Administrators are provided access to the servers thru the Online 5081 system. This requires the supervisor to authorize the access to the server or servers.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

GMP is a non-recordkeeping system. It is a system that allows taxpayers receiving a stimulus to determine when it will be received. GMP authenticates taxpayer identification and extracts taxpayer data from CADE2 and IDRS to provide economic stimulus information. GMP, itself, maintains no persistent tax return data in a GMP specific database. Data received through authentication is stored on the session and will not be retained for any period of time in GMP. Official copies of tax return records are appropriately scheduled, and disposition authorities are published in IRS Document 12990, Records Control Schedule (RCS) 29 for Tax Administration - Wage and Investment Records. GMP audit data is captured by the Security Audit and Analysis System (SAAS) and maintained for seven years under RCS 19.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

4/13/2020

Describe the system's audit trail.

The audit trail being sent to Security Audit and Analysis System (SAAS) identifies the GMP application, the tax filer type, the SSN, and the date time stamp. The Auditable events are Authenticating (successful or unsuccessful) and whether the taxpayer has too many invalid attempts at authentication and is locked out.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

DocIT repository

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

Yes

Please describe the outstanding issues:

Plan of Action and Milestones are currently being tracked for addition to the Integrated Customer Communication Environment (ICCE) System Security Plan (SSP) and Information System Contingency Plan (ISCP).

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

An End of Test Report is produced after each testing cycle and is stored in the Integrated Customer Communications Environment 's DocIT repository.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

No