Architecture, Security and Compliance

April 24, 2024

REVENUE COLLECTIONS MANAGEMENT
BUREAU OF THE FISCAL SERVICE

This version of Pay.gov Architecture, Security, and Compliance supersedes all previous versions.

Revision History

Date	Author	Description
April 17, 2017	Walter Rowinsky FRB Cleveland	Initıal version.
July 17. 2017	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 7.1 (no changes).
October 16, 2017	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.2 (added new section 5.7; updated section 5).
January 15, 2018	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.3 (updated section 5.7).
April 16, 2018	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.3 (replaced references to Vantiv with Worldpay).
December 30, 2019	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.11 (deleted section 5.7 ReCAPTCHA).
March 30, 2020	Walter Rowinsky FRB Cleveland	Updated section 7.3.1.
April 26, c021	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.16 (added new section 6.6 and 7).
October 10, 2022	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 8.0 (added new sections 5.6 and 5.7).
April 24, 2024	Walter Rowinsky FRB Cleveland	Updated section 5.5 (web service ciphers).

Table of Contents

1 Introduction

This document provides a description of Pay.gov's architecture, security implementation and industry and statutory compliance.

1.1 Related Documents

Detailed documents describing Pay.gov services and functions can be found at https://qa.pay.gov/agencydocs/. These documents are intended for agency users and technicians.

Agencies should also request the Agency Guide to Fraud Management.

Information about Pay.gov's Public (customer) user interface is available in the online help at https://pay.gov/public.

2 Pay.gov Architecture

2.1 Background

Launched in October 2000, Pay.gov is a secure government-wide collection portal that provides a suite of complementary electronic non-interactive and interactive services that enable agencies to collect payments and related information from their customers and to manage agency collections activities.

Pay.gov's services meet the U.S. Department of the Treasury Bureau of the Fiscal Service commitment to electronic collections processing using Internet technologies. They satisfy demands from agencies and consumers for electronic alternatives by providing the ability to electronically submit transaction information, make payments, and submit queries, twenty-four hours a day.

Both agencies and their customers have secure access to Pay.gov from any computer or mobile device with Internet access.

3 Architecture

Pay.gov's primary, fully redundant and replicated contingency, and test environments are hosted in the Treasury Web Application Infrastructure (TWAI), a highly secure environment provided by the Federal Reserve Information Technology (FRIT) to support several enterprise-wide Treasury applications. The TWAI is physically located at three Federal Reserve Banks.

The TWAI is built using a zone structure, with firewalls and routers separating each zone, and complies with the Federal Information Processing Standard (FIPS) 140-2.

Pay.gov's Quality Assurance environment is available for agencies to test their interface to Pay.gov, and if hosted by Pay.gov, their forms or bills. All connectivity to and from the TWAI is supported by TWAI system administrators. Pay.gov is supported by technicians at the Federal Reserve Bank of Cleveland and system administrators at TWAI.

All communications between Pay.gov and agencies is conducted through dedicated lines, virtual private networks, or hardware hardware-based (on Pay.gov's side) TLS version 1.2 encryption and uses industry-standard technology, such as XML and Web Services Definition Language files.

All data identified as sensitive stored within Pay.gov is encrypted.

3.1 Business Recovery and Contingency

The U.S. Treasury maintains fully redundant servers within Pay.gov's primary operations center and a fully redundant set of servers within their contingency site. Pay.gov's contingency plan and business impact assessment meet all Bureau of the Fiscal Service baseline security requirements.

In the event of a Treasury-declared catastrophe, Pay.gov should be fully operational at its contingency site within one hour after Treasury's decision to move to the contingency site. If Pay.gov is forced to failover, agency applications will not have to make any changes to connect to Pay.gov at the contingency site.

The Treasury conducts a thorough failover exercise for Pay.gov to its contingency site at least once a year.

3.2 Capacity Planning

Pay.gov regularly submits capacity projection updates to the TWAI.

Performance and load testing is conducted regularly using volume projections submitted by new and existing agencies. Agency submission of accurate projected volume increases is critical to capacity and performance planning.

3.3 System and Application Performance

Pay.gov system infrastructure and application availability statistics are found on Pay.gov's Agency website, Frequently Asked Questions link: https://qa.pay.gov/agencydocs/html/faqs.html.

4 Regulatory and Industry Compliance

4.1 Federal Information Security Management Act (FISMA)

Pay.gov meets FISMA Security Assessment and Authorization (SA&A) requirements for business recovery, application and environmental security, and business risk assessment and mitigation.

Pay.gov is certified annually by the U.S. Treasury and external assessors , based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). Certification and risk assessment includes environmental and application penetration testing.

Pay.gov's NIST FIPS 199 risk impact level rating is moderate.

Visit http://csrc.nist.gov/groups/SMA/fisma/ for more information on FISMA and the NIST RMF.

4.2 Government Paperwork Elimination Act (GPEA)

Pay.gov helps federal agencies meet the directives outlined in the Government Paperwork Elimination Act, primarily by reducing the number of paper transactions and utilizing electronic transaction processing over the Internet.

4.3 Privacy

A Privacy Impact Assessment (PIA) for Pay.gov is available from the Bureau of the Fiscal Service at https://www.fiscal.treasury.gov/fsreports/rpt/fspia/paygov_pia.pdf.

4.4 Payment Card Industry Data Security Standard (PCI DSS) Compliance

Pay.gov has been added to Visa's Global List of Payment Card Industry Data Security Standard (PCI DSS) Validated Service Providers. The Attestation of Compliance document is available on the Pay.gov documentation web site at https://qa.pay.gov/agencydocs/html/references.html.

However, agencies should note that they also have a responsibility to validate their compliance with the PCI DSS. Agencies should contact Worldpay, the card acquiring processor, or the Bureau of the Fiscal Service for more information.

4.5 Section 508 Accessibility

Pay.gov is committed to making electronic and information technology accessible to people with disabilities in accordance with Section 508 of the Rehabilitation Act of 1973 (codified at 29 U.S.C. § 791 *et seq*) and related laws and regulations (for more information, see http://www.section508.gov). Pay.gov conducts regular accessibility testing of its Public, Agency and eBilling Online user interfaces.

Pay.gov's web sites are best viewed at 1024 x 768 resolution using the current version of most common Web browsers. For accessibility, the user interfaces have

been designed to function best when using the latest version of the JAWS for Windows screen reader in conjunction with the current version of Microsoft Internet Explorer or another major browser.

Freedom Scientific, the makers of JAWS, recommends that users avoid using the Microsoft EDGE browser at this time.

5 Security

5.1 Encryption

All communication between Pay.gov, agencies and their customers is securely encrypted following Treasury guidelines.

Identified sensitive data stored within Pay.gov is encrypted, both within the application and at rest.

5.2

5.3 HTTPS

Pay.gov supports HTTPS: HTTP/1.1 over TLS 1.2 (Transport Layer Security).

5.4 HSTS

Pay.gov supports HTTP Strict Transport Security (HSTS) for agency – Pay.gov communication.

The HSTS web security policy mechanism helps protect websites against protocol downgrade attacks and cookie hijacking. It requires that web browser and other user agents use only secure HTTPS connections when communicating with Pay.gov.

5.5 Transport Layer Security (TLS)

TLS 1.2 is the only protocol enabled for both inbound and outbound agency – Pay.gov communication. This requirement applies to both the QA agency test environment and Pay.gov's production environment.

TLS is a cryptographic protocol that provides security for all communications between client web browsers, applications, and servers.

TLS 1.2 must be supported by the following communications:

- Web browsers communicating with Pay.gov.
- OCI Interactive
- Hosted Collection Pages
- All Trusted Collection Services (TCS)
- eBilling Web Services (ebilling and access code services).
- eBilling Online Web Service
- Billing Agreement Web Service
- ACH Credit Web Service

For Pay.gov Web Services, only the following ciphers are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

Pay.gov does not support any Secure Sockets Layer (SSL) cryptographic protocol.

5.6 Certificate-based Authentication

For some services Pay.gov requires the use of security certificates issued by the U.S. Treasury's certificate authority (TOCA) to identify and authenticate agency application servers and to communicate with Pay.gov.

Pay.gov services requiring certificate-based authentication include:

- all Trusted Collection Services
- Hosted Collection Pages
- eBilling Services
- Billing Online Web Service
- ACH Credit Web Service
- Billing Agreement Web Service
- OCI-Interactive

5.7 SHA-256

Data is protected using SHA-256, which converts data into fixed-length, virtually irreversible hash values. This secure format is unreadable unless the recipient has a key.

5.8 Collections API Authentication

All Collections API requests are HTTPS POSTs in JSON format. Each must include an HTTP header named authorization that includes the Authorization, Credential, Signed Header, and Signature.

The authorization/authentication information is provided on request by Pay.gov for each of your Collections API applications.

See the *Collections API Technical Reference* for details about requesting credentials and including authentication information in transaction HTML headers.

5.9 Plastic Card Security

Pay.gov services support both plastic card security codes (CVV2) and the address verification service (AVS).

Your agency determines what action Pay.gov takes based on the response received for either security feature.

5.9.1 Plastic Card Security Codes

A security code is the three or four digit code printed on the back of a plastic card and used to verify that the purchaser has the credit card in hand when making a purchase on the internet or over the telephone. (Examples: CSS, CVV2, CVC.).

The card issuing bank does not make an authorization decision based on the security code response. However, your agency has the option to pre-configure, by application, Pay.gov actions based on the security code response.

5.9.2 Address Verification Service (AVS)

The customer's ZIP code on file with the card issuing bank is confirmed as part of the transaction verification. The AVS response code returned can be forwarded on to the agency and is viewable in Pay.gov Transaction Search results.

Your agency has the option to pre-configure your Pay.gov cash flows as to how Pay.gov will automatically act on your behalf in regard to the AVS or CVV2 code returned by a plastic card issuer. For example, automatically failing an approved transaction if the AVS code indicates the supplied billing address does not match the billing address on file with the card issuer.

Please consult with your Pay.gov Agency Implementation liaison or Pay.gov's fraud team when enabling AVS checks to ensure that the optimal configuration for your agency is selected.

Unless your cash flow is otherwise pre-configured, Pay.gov will not fail a transaction based on the AVS results. However, at the time your Pay.gov cash flow is created you have the option to specify that Pay.gov act differently in response to AVS results. You can also change that configuration option at a later date by contacting your Pay.gov Agency Implementation liaison.

6 Access Control

Your agency can control access to your cash flow applications on Pay.gov's public website and to the functions on Pay.gov's agency websites.

In addition to the summary information in the following sections, see the *Agency Guide to Access Control* at https://qa.pay.gov/agencydocs/ for details.

6.1 Agency Security Contacts

Access control begins with your agency security contacts. These are individuals at your agency who work with Pay.gov's Application Security function to specify what Pay.gov areas and functions your agency users and some customers are allowed to use.

During the initial setup of your Pay.gov cash flow(s) you must designate at least two security contacts, one primary and one secondary, in the Agency Configuration Template (ACT). Additional secondary security contacts may be designated.

In general, your agency security contacts submit an Access Requests Worksheet (ARW) to create, modify, or delete:

- agency users, their roles, and permissions
- roles for customers accessing an agency's private forms

Your agency security contacts also request and administer security certificates for the Pay.gov services that require them.

6.2 Roles

Roles are sets of permissions that control what a customer or agency user can access, what functions they can perform and what information they can view.

User roles are requested to be assigned specifically to each cash flow application. An agency security contact creates a list of cash flow applications in an ARW, lists users and selects the cashflow applications and roles to be assigned to each user.

Multiple applications and roles with various permissions can be assigned to a single user.

6.3 Controlling Agency User Access

Pay.gov requires that all agency users must:

- have a Pay.gov account (created at your agency's request)
- be assigned one or more roles with permissions to access one or more of your cash flows and perform specific functions on Pay.gov
- associate their account with their PIV/CAC card/credentials
- sign in to Pay.gov with their PIV/CAC card/credentials before being able to perform any function

Your agency security contacts request creation of agency user accounts and the assignment of roles to your agency cash flows. Pay.gov creates the user account,

assigns the roles and provides a temporary password, which the agency users must change when they first log in.

6.4 Controlling Customer Access

Customers can only access Pay.gov's public website. They do not need a Pay.gov account or role to perform most transactions. All customers visiting the public website can create any publicly available transaction and payment, search for publicly available transaction forms, search for agencies.

However, customer access can be expanded or restricted through:

- Enrollment
- Private agency cash flows available to only customers granted access
- Hiding gov cash flows so only customers given their URLs can access them
- Assigning roles for functions such as splitting creating a transaction from making its payment

6.4.1 Self-Enrollment

Customers can create an account on the public website by clicking the Sign in button and then clicking the Create an Account button. The first step is to create an ID.me or Login.gov sign in and then enter their information on Pay.gov.

6.4.2 Enrollment by Agency

In some cases, your agency may request the creation of Pay.gov accounts for customers. For example, this may be required if a customer needs to access a cash flow not publicly available (private forms/cash flows). The customer is still required to associate the account with ID.me or Login.gov.

6.4.3 Private Forms/Cash Flows

During configuration, your agency can designate that the Pay.gov online form used to create a transaction is Private (available only to designated customers). Your Pay.gov security contacts would then need to enroll those customers. The customers would then have access to the cash flow when they log in to Pay.gov.

6.4.4 Hiding Public Forms/Cash Flows

You can control customer access to a form/cash flow by requesting it be hidden on Pay.gov. Hidden forms are not listed and are not included in search results. Customers can access them only if your agency provides them the form's/cash flow's web address (URL).

6.5 eBill Access

All customer access to eBills is restricted. They must enter an access code (provided by Pay.gov) and answer a security question. If they add the ebill to their Pay.gov account they only need to do this once and then the ebill is always available in their account.

If the customer does not add the ebill to their account they must enter the access code and answer the security question each time they want view the bill.

See the *eBilling Web Services Technical Reference* and the *Agency Guide to eBilling Online* for more information.

6.6 Dual Authentication

Signing in to Public or the Agency Collections website is a two step process.

Customers sign in to the public site with their ID.me or Login.gov email address and password, then they receive a security code which must be entered before they can access Pay.gov

6.6.1 Option to Remember Device and Browser

Customers and Agency users have the option to have their device remembered when they sign in. If they choose this option they will not need to enter a security code each time they sign in from that device and browser.

However, if they sign in from a different device or browser they will again be required to enter a security code.

7 Field Validation

Real-time validation is enabled for form and payment page fields in order to ensure no malicious content is entered, and all required fields are completed.

8 Support Services

8.1 Agency and Customer Support

The Federal Reserve Bank of Cleveland provides customer support to agencies and their customers. Agency users and customers can talk directly with a customer support representative during business hours, leave messages after hours, or send email asking for assistance at any time.

Messages received off-business hours are reviewed by on-call staff and responded to as soon as practical and reasonable. Customer support staff do not monitor emails received during off-business hours.

eMail received during business hours is responded to periodically during the day. eMail received after business hours is replied to by close of the next business day.

> ***Important!*** Never use emails to report critical issues or urgent problems. Phone Customer Support at the number below.

8.2 Technical Support

Agencies requesting technical support should contact Pay.gov Customer Support, which will refer them to Technical Support as appropriate.

Technicians are on-site and/or on-call 24 hours a day, seven days a week. Application monitoring occurs frequently with early warning alerts generated to notify technicians of potential problem situations.

8.3 Contact Information

8.3.1 Bureau of the Fiscal Service

To obtain further information about how Pay.gov can help with your collections process, or to inquire about other Pay.gov services, please contact your Bureau of the Fiscal Service liaison.

8.3.2 Pay.gov Customer Support

Hours: 8:00 am to 7:00 pm Eastern Time
Monday through Friday, closed bank holidays

Phone: (800) 624-1373

Email Address: pay.gov.clev@clev.frb.org

8.3.3 Pay.gov Agency Implementation

For information about your collections application setup contact your Pay.gov Agency Implementation liaison.

8.3.4 Pay.gov Fraud Team

For Pay.gov fraud-related support or guidance contact the Pay.gov Fraud Team at clev.egov.fraud.team@clev.frb.org

8.3.5 CIR

The Collections Information Repository holds information about your agency's collection transactions and ensures the monies are credited correctly. Your reconcilement processes use reports and information available from the CIR.

For questions or additional information regarding Collections Information Repository (CIR) reports or schedules, contact CIR at CIR.customersupport@clev.frb.rg