



# High Availability - Overview

Ryan Kelley

# Agenda

---

- High Availability Defined
- Steps Completed
- Next Steps
- Continuity Testing and Your Application



***Higher Volume = Greater Impact***

# High Availability Defined

---

***High Availability provides resiliency within primary data centers & planned downtime.***

Pay.gov is capable to support future growth and innovation and needs to continue to focus on offerings that limit downtime to agency systems and users. 86% of all downtime in the past 3 years has been from planned maintenance events.

**OBJECTIVE - the objective of the recent HA study was to identify/explain the application, infrastructure, and process changes needed to achieve the following goals:**

- **Unavailability of any Pay.gov critical component should not exceed a goal of 15 minutes during any planned outage**
- **Unavailability of any Pay.gov critical component during planned outages should not exceed 45 minutes per month**
- **Maintain data integrity**

# High Availability Defined

## *Pay.gov enables collections via a variety of solutions*

Pay.gov Program Offering	Description	HA Service
Trusted Collections Services (TCS) Single	Web services connection; certificate-based authentication. Agency collects remittance info, submits payment info to Pay.gov for settlement.	Yes
Hosted Collection Pages (HCP)	Agency server to Pay.gov interface. Agency collects remittance info, transfers payer to the Pay.gov collection page to enter payment info.	Yes
Collection Control Panel	Web interface; assigned agency personnel manually process ACH/plastic card (card present) transactions.	No
eBilling/eBilling Online	Agencies pro-actively notify client payment is due, client locates bill and and securely pays it via CCP (eBilling) or XML web services connection with certificate (eBilling Online).	No
Forms Service	Agency collects form data; end user submits payment info; publically available or private.	No
Adapter File	Only available to Education Lending and CBP. Allows secure transmission of transaction data.	No

# Defining High Availability

---

***Pay.gov conducted analysis over a 3 year time period to derive the following outage scenarios:***

## **Planned:**

Pay.gov Code Deployment of Core  
Pay.gov Code Deployment w/DB Schema Change  
Database Version Upgrade  
Weblogic Version Upgrade  
Veritas File System Upgrade  
Planned Continuity Event  
Data Encryption Rekey  
Re-encryption of Data

## **Unplanned:**

Telco Failure  
File System Failure  
Database Max Connections  
OCI Interactive DOS  
Vantiv Authorization Unavailable  
Unplanned Continuity Event  
Redundant System Failures  
Application Failures

# Steps Completed

---

- Oracle DataGuard for active/standby database
- Pay.gov core code modularized
- Pay.gov HA interfaces hosted by an independent server cluster
- All changes requiring an outage reviewed for reduction of time
- All changes requiring an outage are reviewed for possible grouping to reduce overall outage time
- Reduced contingency failover from 2-3 hours to less than 1 hour from point of failover decision

# Next Steps

---

- Use Logical Standby to enable online upgrades of Oracle DB and data schema changes
- Enhance existing stored procedures to minimize SQL calls and be backwards compatible with previous schema
- Actively use non-critical modules of Pay.gov in EROC enabling processing in Dallas and EROC with central DB in Dallas
- Evaluate the use and need of infrastructure Maintenance windows (Sunday 2-6 AM ET)

# Continuity Testing and Your Application

---

- **Full Failover**
  - Used in a continuity of business event / disaster recovery
  - Can impact agency system-to-system interfaces if not properly configured to communicate with alternate DR site
- **Test Failover**
  - Routine testing and validation of Pay.gov system components in DR
  - Completed annually during TWAI continuity drill as well as after each point release of Pay.gov

# Continuity Testing and Your Application

---

- **What is a full failover?**
  - Involves a full shutdown and outage of Pay.gov production site in Dallas, Texas (DOC)
  - Pay.gov will be brought up in East Rutherford, New Jersey (EROC)
  - Agencies will be notified at least 1 month in advance of failover
  - Agencies with system-to-system applications will be expected to pre-validate connections when possible
  - Transparent to agency/public users but potentially can effect agency system-to-system connections

# Continuity Testing and Your Application

---

- What is a test failover?
  - Validate code migration and environment changes related to a release
  - Completed with every Pay.gov major or point release
  - Completed with major infrastructure changes in contingency site (EROC)
  - 3-7 tests per year
  - No outages in production Pay.gov and completely transparent to agency systems

# Continuity Testing and Your Application

---

- Full Failover tentatively planned for 8/27/16
- Failover will last at least 1 week and potentially up to 4 weeks
- Pay.gov will return after failover to Dallas Operations Center
- Agencies will be formally notified at least 1 month in advance of this failover
- Future failovers may become more frequent and will then provide less notice of a failover

# Contact Information

---



**Pay.gov Team:**

[Pay.gov@fiscal.treasury.gov](mailto:Pay.gov@fiscal.treasury.gov)