DTC Standard Operating Procedures for the VA: Pega Center of Excellence (COE)

Revision History

Version	Date	Name	Comment
1.0	9/8/2023	Amanda Ross	

Table of Contents

Purpose

The Pega Center of Excellence (CoE) SOP is designed to provide a high-level overview of the different functions performed by the Digital Transformation Center (DTC) at the Department of Veterans Affairs (VA) for the Pega Center of Excellence (CoE).

Intended Audience

The primary audience for this document is customers responsible for developing Pega modules that provide business capabilities to the VA.

The secondary audience for this document is members of the DTC team to have a working knowledge of the processes described in this plan.

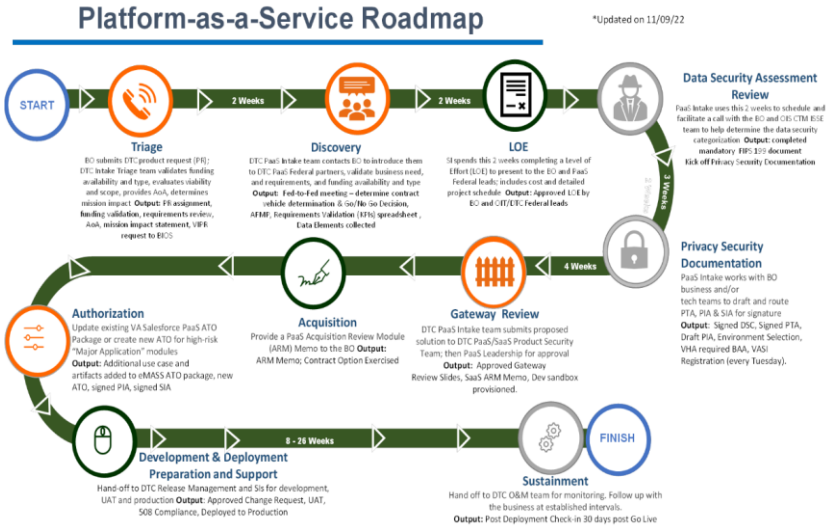
Roles and Responsibilities

Role	Responsibilities
Business Owner (BO)	• The BO initiates engagement with DTC when they submit a product request (PR). They have authority of the use case, product requirements, Vendor selection, etc. to ensure the PR and the acquired product successfully move through the DTC process in conjunction with DTC staff providing guidance. • Participate in completing required security documentation • Verify requirements have been met to move to production
Pega COE Team	• Participate in DTC product lifecycle • Provide support for development, release and sustainment • Ensure a seamless onboarding to Pega within the VA
DTC Intake Team	• Schedules and hold initial call with business owner to determine basic information regarding the request, verify funding and route to appropriate DTC discovery pipeline.
ISSE Team	• Provides Data Security Categorization (DSC).
Product Stream Lead (PSL)	• Serve as the BO main POC. Schedule discovery calls and gather necessary documents (data dictionary, DSC/ Memorandum of

Commented [HWM(GI(1]: Do they have any part of security documentation?

Role	Responsibilities
	Understanding (MOU)) and guide the customer through the process of discovery.
System Owner (SO)	• Ensure adherence to access control policy by key Office of Information Technology (OIT) staff. • Provide oversight for personnel with significant responsibility to information systems. • Update procedures as needed to ensure it meets OIT mission requirements and complies with Federal Laws, Policies, Procedures, and Guidelines. • Ensure all procedures herein are properly complied with.
License Management	• Provides license management support. • Creates license Level of Effort (LOE). • Manages licenses in sustainment.

DTC COE Roadmap



DTC Intake

1. Submit Intake Request

VA User submits intake request through Digital VA Marketplace: DigitalVA Marketplace

2. DTC Triage

DTC Triage team schedules initial meeting to validates funding availability and type, evaluates viability and scope, provides Analysis of Alternatives (AoA) (if applicable), and determines mission impact.

Output: PR assignment, funding validation, requirements review, AoA, mission impact statement, VA IT Process Request (VIPR) request to Business Integration and Outcomes Service (BIOS)

3. Discovery Call

Once Triage phase is complete, DTC Discovery team will schedule a Discovery call to:

- Introduce them to DTC Platform as a Service (PaaS) Federal partners.
- Validate business need & requirements.
- Determine funding availability and type.
- Give an overview of the full process for onboarding with Pega.

System Integrators (SIs) should present to DTC Pega COE a high-level technical design document so that use case and security considerations can be validated and conducts a sizing exercise.

Output: Fed-to-Fed meeting – determine contract vehicle determination & Go/No Go Decision, Acquisition Financial Management Plan (AFMP),

Requirements Validation (Key Performance Indicators (KPIs)) spreadsheet, Data Elements collected.

4. Level of Effort (LOE)

SI spends these 2 weeks completing a LOE to present to the BO and PaaS Federal leads; includes cost and detailed project schedule. DTC License Management team provides license cost to business owner.

Output: Approved LOE by BO and OIT/DTC Federal leads.

5. Data Security Assessment

PaaS Intake uses these 2 weeks to schedule and facilitate a call with the BO and Office of Information Security (OIS) CTM Information System Security Engineering (ISSE) team to help determine the data security categorization. During the call, the business owner should be prepared to speak to the use case and data elements that will be used.

Commented [HWM(GI(2]: Can't find this for the life of me

Output: completed mandatory Federal Information Processing Standards (FIPS) 199 document and kick off Privacy Security Documentation.

6. Privacy Security Documentation

PaaS Intake works with BO business and/or tech teams to draft and route Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA) & Security Impact Assessment (SIA) for signature.

Output: Signed DSC, Signed PTA, Draft PIA, Environment Selection, Veterans Health Administration (VHA) required BAA*, VA Systems Inventory (VASI) Registration (every Tuesday).

Commented [HWM(GI(3]: Don't know this one

The Business Associate Agreement (BAA) is mandated by the Health Insurance Portability & Accountability Act and is required if the system provides a service, function, or activity to the Veterans Health Administration (VHA) or on behalf of the VHA and is associated with Protected Health Information (PHI). If the Major Application does not have a BAA that covers the PHI, then the Minor Application will have to complete a BAA. The VHA Data Portal provides additional information: BAA

7. Gateway Review

DTC PaaS Intake team submits proposed solution to DTC PaaS/Software as a Service (SaaS) Product Security Team, then PaaS Leadership for approval.

Output: Approved Gateway, Review Slides, SaaS Acquisition Review Module (ARM) Memo, Dev sandbox provisioned.

8. Acquisition

DTC Provides a PaaS ARM Memo to the BO. BO engages in contracting activities with local budgeting POC. DTC Federal Lead is engaged for support if needed.

Output: ARM Memo; Contract Option Exercised.

9. Authorization

Update existing VA Salesforce PaaS ATO Package or create new Authority to Operate (ATO) for high-risk "Major Application" modules.

Output: Additional use case and artifacts added to eMASS ATO package, new ATO, signed PIA, signed SIA.

10. Development, Deployment Preparation & Support

Hand-off to DTC Pega COE Release/Platform team and SIs for development, User Acceptance Testing (UAT) and production. SIs will conduct a series of security and technical gate review meetings with DTC throughout development and deployment of integrations/Application Programming Interfaces (APIs).

Output: Approved Change Request, UAT, 508 Compliance, Deployed to Production.

11. Sustainment

Hand off to DTC Platform and Sustainment for monitoring. Follow up with the business at established intervals.

Output: Post Deployment Check-in 30 days post Go Live.

License Management

The Pega licensing model includes a streamlined approach for license procurement. At the VA, there is one type of license that will be purchased regardless of user type.

License Type	Access Included	Types of Procurement Accepted	Color Of Money
Platform Licenses	• Pega SaaS Case Management Bundle for Business End Users • Pega Government Platform (PGP) Core Bundle and Pega Foundation for Healthcare. • 12-month Pega Cloud for Government Subscription for Pega Cloud for Government Pega SaaS Application built on PGP	• 2237 • BTT Strip • ARM (Non OIT Only) • IPRs *No Purchase cards can be used	Pega licenses can be purchased with non-IT funds

Commented [HWM(GI(5]: Don't know this one

Commented [HWM(GI(6]: In progress review?

Commented [HWM(GI(4]: Don't know this one

VA Business owners should take the following items into consideration when determining how many licenses to procure:

- There are no separate licenses for developers.
- The business team should procure the number of licenses required for end users prior to development work beginning. Developers will be assigned to those licenses.
- The Pega VA licensing model is based on Full Time Employee (FTE) usage with each USER being defined as a person who uses the Software in a particular month:

USER TYPE	DEFINITON	FTE WEIGHT
Sporadic User	A person that uses the Software during less than 10 hourly periods in a calendar month.	0.1 FTE
Occasional User	A person that uses the Software during between 10 and 50 hourly periods in a calendar month.	0.5 FTE
Regular User	Any person other than a Sporadic User or Occasional User that uses the Software in a calendar month, or that has the privilege to modify rules or processes	1 FTE

- Users may be allocated within the total licensed User count between Regular, Occasional and Sporadic Users monthly using the following conversion between the User types. This approach allows VA to deploy their licenses in any combination of user types if the total FTE count is not exceeded. VA can adjust this combination as needed as long as they do not deploy users in excess of the total FTE license count. EXAMPLE: If 50 licenses are purchased and there are a group of 100 users that are deemed "sporadic" or "occasional" users, those 50 licenses could cover the 100 users.

Have Additional Pega Licensing Questions? Please Contact:

Delwin.johnson2@va.gov OR kenton.ngo@va.gov

Account Management

Within the VA Pega Platform there are several types of user accounts. The table below outlines the various types and their purpose.

Table 1: User Account Management

Account Types	Purpose
Pega COE Admin	This is the highest level of access to the Pega Gov cloud platform. This level gives access to the base platform level access. Only Pega COE Developers will have access to this level.
Pega COE Author	This access level is dedicated to COE Developers to develop and manage Enterprise/Platform level components.
Application Author	Application Author is granted to SI and Citizen Developer (CD) who are configuring any applications or components. Editing capabilities will be limited to that application only. Cross application access is NOT allowed.
Manager/Supervisor	Manager/Supervisor access level is defined at the application level that's specific to the application functionality. Cross application access is NOT allowed.
User Read/Write	This access level is granted to the application users that are requiring to creating a case and performing a task on the workflow. Cross application access is NOT allowed.
User Read only.	This access level is granted to the application users that is only required to view a case or run reports. Cross application access is NOT allowed.

1. Establishing Security Groups

During the Application design and implementation process different user personas will be defined. The SI or the CD will request the DTC Pega COE to create the necessary security groups in Active Directory (AD) for the users to be added once the application goes live.

2. Establishing Accounts

A specific process needs to be followed to establish an account for each user within the system. The following steps must complete before a new account is established.

The user completes a User Permissions Request Form in the DTC Help Desk App, which includes the following:

1. Verification that user is current on signed Rules of Behavior, Cyber Training, and Privacy Training
2. Federation ID
3. Email Address
4. Manager
5. Does the user require color-blind palettes on charts?
6. Any specific requirements or permissions

Note: These items require the direct written approval of the Application Approver in an email or chatter post in addition to their approval of the case request.

Once a user has completed the account request, the system owner for the application must approve. The VA Helpdesk team will then review the request and verify that the appropriate approval has been received. The user will then be created and/or added to the appropriate security group(s) based on job requirements and enforcing the least privilege concept. In the event a user requires Elevated Permissions, it must be justified and approved by the system owner/Information Security Officer (ISO) or their designated organizational official. The following section outlines the requirements for an Elevated Permissions User.

3. Elevated Account Management

The following requirements for Elevated Permissions are requested and stored by the DTC Electronic Permission Access System (EPAS) Team.

1. Background Investigation Dates – requested from and provided by B3 Facility Security Officer (FSO); received and stored by the DTC EPAS in VA Teams.

2. Completed course certificate for Talent Management System (TMS) #1357076 Information Security Role-Based Training for System Administrator – requested from and provided by user; received and stored by the DTC EPAS in VA Teams.
3. User's Supervisor approval for requested Elevated Permissions profile; received and stored by the DTC EPAS in VA Teams.
4. COR review and approval of EPAS form (MyVA Elevated Privileges) – reviewed, approved, and stored in the VA EPAS system.
5. The Pega System Owner is provided a weekly report of new Elevated Permission Users – provided by the DTC EPAS Team.

4. Elevated Account Maintenance

Once one year has passed from submission, the DTC EPAS team completes the supervisor and steps again and submits a new EPAS.

5. Modifying Accounts

If a user is requesting a modification to their account, they must submit an access request (via the VA User Account Request form) along with valid justification to the designated approval authority. Once the approving authority approves the request, the System/Module Administrator is notified, and the modification is made to the account.

6. Disabling Accounts

Common user accounts are Locked and disabled after 45 days of inactivity automatically by the Pega platform.

7. Deleting Accounts

Should an account need to be removed due to termination or reassignment of responsibilities, the account will be disabled at the same time (or just before) the employee is notified of their dismissal or upon receipt of resignation and the VA FIM offboarding process is inherited. The user will no longer be able to access VA Pega when their access to the VA Network and Single Sign On (SSO) are disabled. The user will be set to Inactive in VA Pega with specific security measures put in place, including the removal of permission sets, groups, queues, etc. which provide application access following 45 days of inactivity.

Commented [HWM(GI(7]: Don't know this one

If a user account should need to be re-activated, the user MUST request a user account via the normal new user channels and appropriate access will be given.

8. Project/Department Transfers

When a user is transferred to a different department or project within the VA Pega environment, the current Project Manager is responsible for notifying the Application Administrators. This process is designed to ensure that privilege creep does not occur. Audits of User Deactivation, Reactivated Users, and migration of Users (not logged in for 180 Days) to the Minimum Access Profile take place on a Daily or Weekly basis.

9. Auditing Accounts

The VA Pega Platform will utilize the Pega audit capabilities to audit the creation, modification, disabling, and termination actions of users and system/service accounts. All changes that are performed on accounts within The VA Pega Platform are tracked in the VA Pega Platform module Test "Dummy" Users

Application Development Teams are responsible for the creation of any test "dummy" users in DEV, SIT and INT. If test users are needed in REG, the appropriate setup instructions should be provided in the Deployment Plan for the DTC Release Team. Test "dummy" users are not permitted in environments past REG as those are full copy or Production environments which contain Protected Health Information / Personally Identifiable Information (PHI/PII), and individual access must be managed/monitored.

Current audit Standard Operating Procedures include the following reports reviewed weekly, unless otherwise needed:

1. Report of "Users Deactivated Last Night"
2. Report of "Users Reactivated within the Lats Week".
3. Report of "Users Deactivated Over 90 Days Ago"

Environment Management

All Pega environments within the VA, including sandboxes are managed by the DTC Pega COE Team.

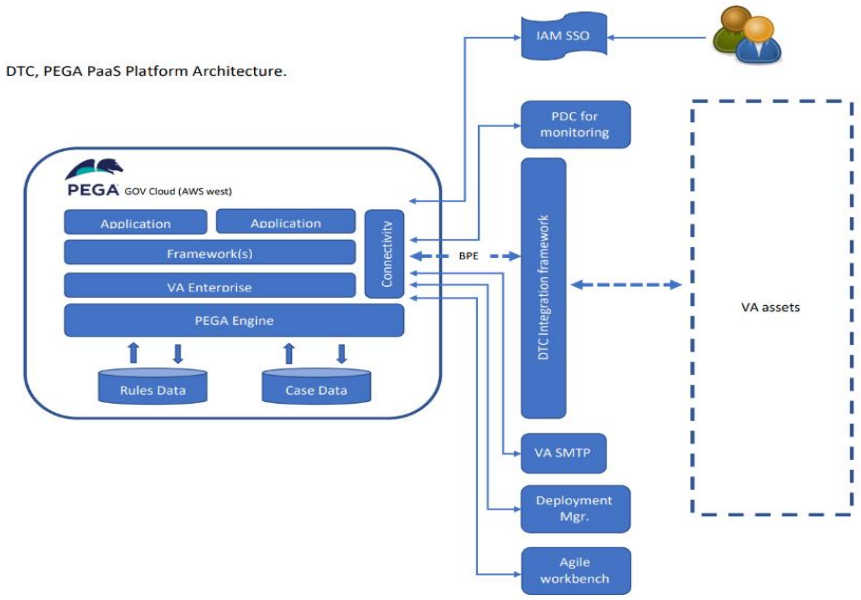
Any enterprise level components, features, functionality required by SI/CD will follow DTC's standard sprint cycle. Enterprise reusability falls to the DTC team; prioritization and Service Level Agreements (SLA's) are determined based team bandwidth

1. Environment Types

Environment Type	Purpose	Sandbox Type	Deployment Responsibility
Development	Available to SI/CD for development work	Developer Sandbox	DTC
Testing	Available for SI/CD to complete system and regression testing	NA	DTC
Staging	Available for SI/CD/Business team to complete UAT	NA	DTC
Production	Live environment	NA	DTC
Platform Support Environments (Agile Studio, Diagnostic Cloud, Release Manager)	Contain platform support toolkits that are used to support the first four environments	used by DTC	N/A
Agile Studio	Available to SI/CD to manage sprints and agile processes	NA	DTC

2. Architecture Diagram

DTC, PEGA PaaS Platform Architecture.



Development Support

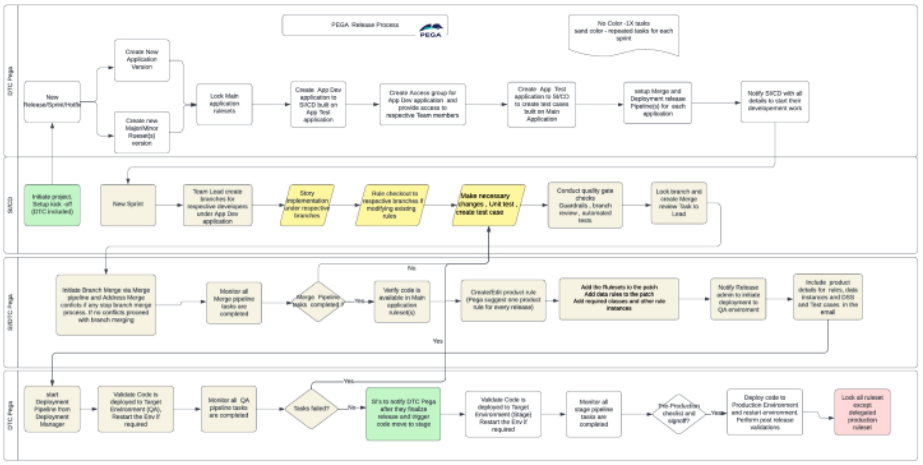
Once a request has received gateway review (step 7 in the DTC intake process), access to the development environment is provided. While the system integrator or citizen developer is working through development and testing of their solution, the DTC Pega COE team will be readily available for guidance and support to include design, architectural review and release management. the DTC team will also Conduct quality audits on the design, architecture, and code periodically. The DTC will provide additional support for the CDs in training, application design and implementations including assistance with integrations and complex process flows and activities. The DTC Pega COE team offers weekly office hours for drop-in support and Q&A.

For system integrators or citizen developers who desire additional training about the Pega platform, Pega offers online self-paced courses at: Pega Academy Home | Pega Academy.

For a deeper understanding and complete list of Pega COE development resources, including coding standards, please visit the Pega COE confluence site.

Release/Deployment Management

The DTC Pega COE provides release management support for all modules being developed. SI/CD can expect the following path for module releases:



Deployment tasks created by the project teams are executed by the DTC Release Team to migrate code to the consolidated Testing, Staging, and Production environments.

SI/CD should have and be prepared to provide the following documentation as part of the release process:

Resource	Purpose	Responsible Party
Deployment Checklist	Outlines requirements that must be met to move to production	DTC COE Team will Provide
Results of System and Regression Testing	ALL module functionality supported in a release must be completely tested prior to release. This includes functional testing of new capabilities to ensure that changes do not negatively impact existing functionality.	SI/CD to Provide to COE Team
User Stories	To ensure validation of end user requirements	SI/CD to Provide to COE Team
Evidence of UAT Testing	UAT testing ensures the end user expectations are met and module is ready for production	SI/CD to Provide to COE Team
Module Playbook	This ensures DTC COEs understanding of the modules functionality in order to provide adequate sustainment.	SI/CD to Provide to COE Team

The tasks involved in the deployment/release process are described in detail below:

1. Once development is completed, SI/CD should request for release to DTC COE team through email.

2. SI/CD will provide evidence of completed deployment checklist tasks to COE team for review. COE team will review and verify requirements have been met.

Minimum Requirements:

- 70% development team test cases coverage (will be executed on the platform) **Any % of test cases not executed through platform automation must be accounted for with manual test cases**
- 85% guardrail score
- 0% technical debt

3. Once it has been verified that deployment requirements are met, DTC COE Team will merge into trunk for development, ensure rule sets are locked and create package for migration. The package will then be migrated to upper environments from development to testing for system testing.

4. Once in test environment, SI/CD should complete system and regression testing. SI/CD should be prepared to share the results of testing to include user stories. Once testing is complete, the business team should notify the DTC COE Team via email. If additional development is needed to address concerns from testing, this must be completed in the development environment, as no code changes are permitted in the upper environment. Upon completion of the additional development, SI/CD should revert to step 1 for review by the DTC COE Team.

5. Upon email receipt of the email verifying testing is complete, DTC COE Team will migrate package to staging. SI/CD should organize and complete UAT testing. Upon completion of UAT Testing, the business team should notify the DTC COE Team via email with attached evidence of UAT Testing.

6. Upon email receipt of completion of UAT testing, DTC COE Team will schedule release and migrate the package to production. This can be done anytime but without any downtime or impact to end users unless the module is a major release (EX. database changes or library update). However, Business Owners should be prepared be available for smoke testing approximately one hour prior to release, to ensure all functionality is working appropriately. The DTC COE team will schedule release based on availability of required parties.

Commented [RAH(GI8]: Smoke Testing? Business users get online for 45mins to test quickly to ensure its working correctly; this would be scheduled/coordinated by COE team and should align with release time

7. Once in sustainment, DTC COE Team will remove all SI/CD and business owners from development, testing & staging environments.

1. Dark Releases for New Modules

DTC supports and recommends dark releases to Production prior to going live in Production for larger or more complex modules.

What Does This Mean for Integrator teams?

The module and its users are considered "dark," meaning that they are not actively creating records, data, etc. in Production. All workflow rules, process builder scripts, community, integrations, and other configurations are not visible to an active user and no real data is being created.

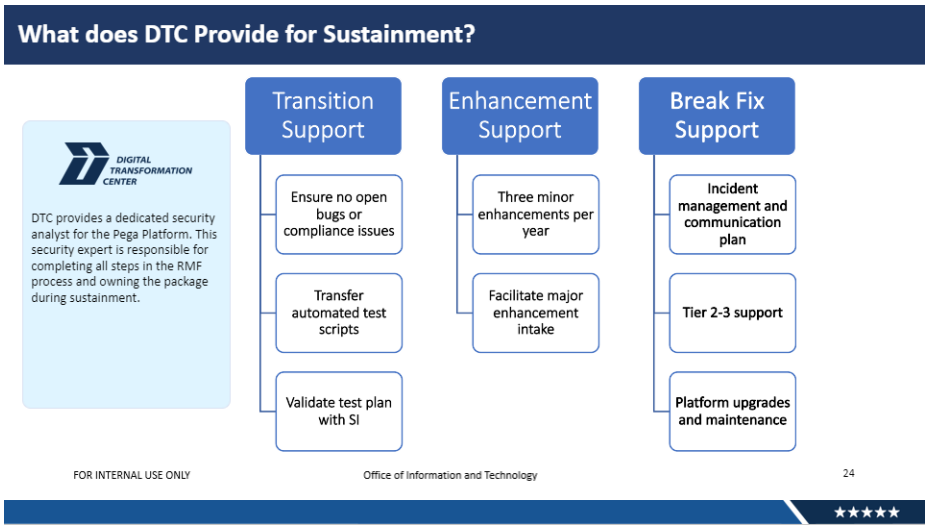
By pushing these configurations early and regularly, the current state of the project is integrated with existing configurations, has an interim sign off from the customer, and has met DTC standards. The resulting benefit is that this process gives the project great milestone accomplishments. In addition, the development teams save time because the sandboxes are refreshed, and the configurations do not have to be manually pushed to the sandboxes each time they are adjusted.

This same concept can be applied and utilized via feature toggles for existing applications. This can increase stability for the application in production and allow teams to control their own migration windows based on external integrations that do not occur on the same cadence as the DTC release schedule.

For a deeper understanding and complete list of Pega COE release resources, please visit the Pega COE confluence site.

Sustainment Support

The DTC Pega COE team provides the following support for modules in sustainment.



For all support requests after the solution has gone live, Business Owners and Customer Teams are directed to submit a ticket through the DTC Customer Success Center.

Support Options	Business Hours
Open a Ticket with the Customer Success Center	Monday - Friday: 8:00 AM - 9:00 PM EST Excludes Federal Holidays

Support Options	Business Hours
Customer Service Line (CSL): (202) 921-0911, option 2	Monday - Friday: 8:00 AM - 9:00 PM EST Excludes Federal Holidays

For a deeper understanding and complete list of Pega COE release resources, please visit the Pega COE confluence site.