Administrative Questions

Question: What is the Commonwealth Application Certification and Accreditation (CA)^2 process?

Answer: The (CA)^2 process is an assessment tool that measures a proposed E-Government initiative's compliance with OA/Office for Information Technology (OA/OIT) ITB policies, procedures, and standards. The (CA)^2 process also identifies the inherent risks associated with an existing or proposed E-Government initiative. The assessment process consists of policy compliance assessments and risk assessments, which include source code analysis, host-based intrusion scans, and web application risk assessments.

Question: Who has to complete the (CA)^2 process?

Answer: All agencies, departments, boards, commissions and councils under the Governor's jurisdiction who are creating a new web facing application or who are in the process of making significant changes to an existing web application's security architecture.

Note: This also applies to any organization or entity that uses the Commonwealth's Enterprise Sever Farm (ESF) to host their web facing application.

Question: I was told that their can only be two (CA)^2 Points of Contact per agency. Is this true?

Answer: In accordance with ITB-SEC005 - ***Commonwealth Application Certification and Accreditation***, agencies are supposed to appoint a primary and secondary point of contact to complete the (CA)^2 assessment process and to act as the liaison between the agency, OA/OIT/OIS, and the (CA)^2 Review Board.

In larger agencies, the Agency CIO may appoint more than two points of contact but they have to be aware that these users can see and edit all of the applications within the (CA)^2 application. If you have a business need to complete a request, we recommend that you contact your Agency CIO to see if you can have access to the application or who your (CA)^2 Points of Contact are so they can submit your application on your behalf.

Question: What is a conditional approval and a conditional accreditation?

Answer: During the process, there may be times when an application has issues that will keep it moving from one part of the process to the next. For example, the agency may have an application that has been written in a language that cannot be scanned with the common application scanners.

To move the application forward in the $(CA)^2$ process, the agency may request that the application receive a conditional approval for the certification phase pending the outcome of the web vulnerability scan. If there are no issues during the vulnerability scan, then the application would be allowed to move forward and it will be accredited.

Web applications that go through the process and have risks that cannot be remediated will be required to have a risk mitigation plan. The risk mitigation plan will identify the risks associated with the Web application and identify how the agency plans to mitigating these risks. This plan will be attached to the $(CA)^2$ submission and the reviewed by the CTO to determine if the application can go into production with a conditional accreditation.

User Questions

Question: How can I complete the $(CA)^2$ process?

Answer: OA/OIT created a web application that assists agencies with completing the process. The application can be accessed by going out the $(CA)^2$ website located at: https://www.sqca.state.pa.us

Question: How does a user acquire access to the application?

Answer: Users should first contact their Agency CIO to see if the agency currently has a $(CA)^2$ Point of Contact. If there are no existing $(CA)^2$ Points of Contact, then they should send an email to ra-CA2@state.pa.us requesting access to the application and they should carbon copy (CC) their Agency CIO

Question: I accessed the site but I cannot log onto the application. What should do?

Answer: You should send an email to ra-CA2@state.pa.us requesting access to the application or to request assistance with accessing the application.

Question: Why can I see other agency requests?

Answer: The application is role based and is designed so that there is a primary and secondary Point of Contact that can access all of the agency web applications to make edits, revisions, and to recertify it. This also allows agencies to continue to process applications even if the submitter is out of the office for an extended leave, takes a position in another agency, or separates from the Commonwealth (retirement, private sector employment, etc.).

Note: It is important for agencies to try to limit the number of users who can access the application.

Application Specific Questions

Question: What types of applications need to go through the (CA)^2 process?

Answer: Initially, the only applications that have to go through the process are web facing applications and portal applications that have data covered under the Pennsylvania Breach of Personal Information Notification Act. Eventually, all web applications will need to go through the process but this won't happen until the Office of Administration, Office for Information Technology establishes standards for source code and web vulnerability scanning tools.

Question: Are enterprise portal applications required to go through the process?

Answer: Agencies using the Enterprise Portal's Studio Server or BEA Publisher to collect personal information that is defined in the Breach of Personal Information Notification Act have to complete the (CA)^2 process? Enterprise portal applications that only post static information or do not collect breach act information do not have to go through the (CA)^2 process.

Question: If a web application is developed and owned by a company that is PCI PA-DSS compliant does it still need to be scanned as well?

Answer: Yes all web facing applications need to complete the process regardless of who developed them.

Question: Our application is a custom off the shelf (COTS) application. Do we need to complete the process?

Answer: Yes COTS applications need to go through the process. Please note, that you may not be able to complete the source code scanning process because the application may be written in a proprietary language which is not supported by the common source code scanning tools. In these instances, the agency should either ask the vendor to complete the scans or request a conditional approval.

Question: Is it ok for my application vendor to complete the source code and web vulnerability scans for us?

Answer: Yes it is ok for you vendor to complete the scans and provide you with the reports to enter into the system as long as there are no critical issues discovered during the scan. In cases were there are critical issues, the Commonwealth will require the vendor to remediate them before allowing the application into production.

Question: Can my vendor have access to the (CA)^2 application to submit our web application for review?

Answer: The (CA)^2 application is restricted to Commonwealth personnel. This is due to the fact that all agency applications are accessible to the agency users and this may allow contractor access to confidential information that cannot be released to non-Commonwealth personnel (application flaws, risk mitigation plans, etc.).

Question: My application has been rejected several times and my CIO would like me to meet with the (CA)^2 Review Board to see how we can proceed. How do I do this?

Answer: Simply make this request in your comments field and submit the application. The (CA)^2 Administrator will read it and then make arrangements with you and the (CA)^2 Review Board.