pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Commonwealth Application Certification and Accreditation

ITP Number	***Effective Date***
ITP-SEC005	April 30, 2009
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
ra-oaitb@pa.gov	Annual

This Information Technology Policy (ITP) establishes policy for the Commonwealth Application Certification and Accreditation $(CA)^2$ process.

1. Purpose

On January 15, 2000, Act No. 69 of 1999 (73 P.S. § 2260.101, *et. Seq.*), known as the Electronic Transactions Act (ETA or Act), became effective. The ETA provides for the validity of electronic signatures and electronic transactions by providing legal recognition to contracts, signatures, and records made electronically. The Act also provides direction relating to:

- Uniform electronic transactions
- The creation and retention of electronic records
- The use of information technology (IT) security procedures
- The use of electronic signatures for identification and transaction validation.

In addition to these mandates, Chapter 5 of the Act, relating to governmental agencies, sets forth the rules for the acceptance and use of electronic transactions by governmental agencies. Chapter 5 of the Act also directs all executive agencies to comply with standards established by the Office of Administration (OA), the agency responsible for creating IT policies, procedures, and standards that promote consistency and interoperability between governmental agencies.

The OA created Management Directive (MD) 210.12, *Electronic Commerce Initiatives and Security*. This MD identifies the OA as the governing body responsible for ensuring that Commonwealth agencies under the Governor's jurisdiction are complying with the security requirements identified in the Act.

MD 210.12 also requires the OA to issue Information Technology Policies (ITPs) to provide agencies with technical guidance and security procedures relating to using, sending, receiving, and storing electronic records and electronic signatures. In addition to the ITPs, MD 210.12 requires agencies to complete a security assessment prior to participating in or initiating an electronic transaction involving the use, transmission, or storage of electronic records or electronic signatures. This assessment, the Commonwealth Application Certification and Accreditation $(CA)^2$ process, is the subject of this ITP.

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) IT policies, procedures, and standards. The $(CA)^2$ process also identifies the inherent risks associated with an existing or proposed E-Government initiative.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

ITP-SEC005 sets forth the policies and procedures that agencies and OA/OIT/Enterprise Information Security Office (OA/OIT/EISO) are to adhere to when assessing internet facing web applications for potential vulnerabilities. For the purpose of this ITP, an internet facing web application is defined as an application that uses the Internet provide citizens, Commonwealth employees, and business partners with access to agency-specific data or services and that resides on a Commonwealth Web server.

Examples of Web applications include forms, login pages, dynamic content, and discussion boards.

This ITP enables OA/OIT/EISO to complete $(CA)^2$ assessments on:

- Internet facing Web applications hosted on the Commonwealth's network(s).
- Web application frameworks that have not been vetted through the $(CA)^2$ process. For more information about a Web application framework's accreditation status, please contact OA/OIT Service and Solutions to see if the framework has been accredited.
- Internet, Intranet, Extranet Web applications or Web application frameworks that process "Breach Act Data," "Sensitive Security Information," or may pose undue risk to the Commonwealth's IT infrastructure.
- Hardware and virtual devices that host Web applications, Web services, databases, etc.

This policy shall not apply to vendor hosted Web applications as long as the following conditions are met:

- The Web application and its components are hosted by the vendor. This includes components that support the application such as Web services, databases, etc.

- The terms and conditions of the contract place the responsibility for network and application security on the vendor. This includes host scanning, network vulnerability testing, Web application vulnerability scanning, PCI scanning, etc.

- The terms and conditions of the contract include a Non-Disclosure Agreement or similar language that protects the Commonwealth's data.

3. Objective

To establish policy for the Commonwealth Application Certification and Accreditation $(CA)^2$ process.

4. Policy

Agencies that are developing Web applications are required to submit $(CA)^2$ requests to OA/OIT for review. This review consists of policy compliance assessments and risk assessments, which include source code analysis, host-based intrusion scans, and Web application risk assessments.

The $(CA)^2$ process is incorporated into the Commonwealth's System Development Life Cycle (SDLC) process and starts with a policy compliance assessment which occurs at the end of requirements gathering phase and ends with a Web application vulnerability assessment including scanning for common vulnerabilities listed by industry authoritative sources such as the current OWASP Top 10 Vulnerabilities Project (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project), while the application is in staging. Applications that successfully go through the process will be deemed accredited and will receive a seal from OA/OIT showing the application's accreditation status.

A Web applications that goes through the process and has risks that cannot be remediated will be deemed as an "at risk application" and 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 mitigate these risks. This plan will be attached to the $(CA)^2$ submission and the reviewed by the OA/OIT/EISO to determine if the application can go into production with a conditional accreditation.

In addition to new applications, accredited Web applications are to undergo a reaccreditation process every three years in order to maintain the security accreditation and any changes to an accredited application's or pre-existing

application's security architecture will void its accreditation status. In order to regain $(CA)^2$ accreditation, agencies will be required to submit a new or updated $(CA)^2$ request.

In addition to the security requirements established by the OA/OIT ITPs, there may also be agency-specific security requirements that are not captured by OA/OIT policy, procedures, and standards. These requirements may be specific to the agency or Agency Business Owner and may have their genesis in such as federal or state laws or regulations, executive orders, or management directives.

- Since these requirements are agency- or business-owner specific, it is the responsibility of the agencies to ensure:

- All required security controls mandated by law, agency policy, or business owner requirements are incorporated into the agency's Web application's security architecture.

- All appropriate security requirements are addressed in agency acquisitions of information systems and information system services.

- All financial applications that use credit cards are compliant with Payment Card Industry Data Security Standards (PCI-DSS). These standards include:

    - Building and Maintaining Secure Networks – This includes installing and maintaining a firewall configuration to protect cardholder data; and not using vendor-supplied defaults for system passwords and other security parameters.

    - Protecting Cardholder Data – This includes protecting stored cardholder data and encrypting transmission of cardholder data across open/public networks.

    - Maintaining a Vulnerability Management Program – This includes using and regularly updating anti-virus software or programs. In addition to antivirus, e-commerce applications are to develop a process to ensure that security is built into the application and systems.

    - Implementing Strong Access Control Measures – This includes restricting access to cardholder data by business need-to-know basis, and assigning a unique ID to each person with computer access. This also includes restricting physical access to cardholder data.

    - Regular Monitoring and Testing Networks – This includes tracking and monitoring all access to network resources and cardholder data, and regularly testing security systems and processes.

    - Maintaining an Information Security Policy – Agencies are to maintain a policy that addresses information security for employees and contractors.

Non-accredited applications and conditionally approved applications will be deemed as an "at risk application." For the purpose of this policy, an "at risk application" is an application that:

- Is in production but has not undergone/completed the $(CA)^2$ assessment process.

- Has initiated the $(CA)^2$ process but receives a conditional approval due to business constraints or issues that cannot be remediated at the time the application needed to be put into production.

Applications that have started the $(CA)^2$ process but have not been updated within one year of the initial submission date will be automatically removed from the $(CA)^2$ system. This is being done to remove applications that are not ready to begin the assessment process, have been placed on hold, have been cancelled and were not removed from the system.

Note: Submitters can avoid having applications removed from the $(CA)^2$ system by going into the system and submitting a update/status report in the system's comments field or by contacting the $(CA)^2$ Administrator.

5. Responsibilities

OA/OIT Chief Technology Officer (CTO) – The CTO reports to the Deputy Secretary for Information Technology and is responsible for the day-to-day operations of Commonwealth's IT infrastructure. As part of these duties, the CTO is to ensure that all Web applications being placed onto Commonwealth networks are secure and that potential vulnerabilities are either remediated or that a risk mitigation plan is in place before allowing Web applications to be put into production. In order to do this, the CTO will empower the Commonwealth Information Security Officer (CISO) to complete the $(CA)^2$ process on Web applications being hosted on Commonwealth networks.

CISO – The CISO reports to the CTO and is responsible for protecting the Commonwealth's IT infrastructure from internal and external cyber security threats. This responsibility includes managing the OA/OIT/EISO which is responsible for completing the $(CA)^2$ process on existing and prospective Web applications.

In addition to managing the OA/OIT/EISO, the CISO will be responsible for putting together a board of technical experts and security advisors who will review $(CA)^2$ requests to determine if they present security threats to the Commonwealth's IT infrastructure. This board will be comprised of:

- $(CA)^2$ Administrator – The $(CA)^2$ Administrator is responsible for the administration of the $(CA)^2$ process. In addition to this, the $(CA)^2$ Administrator is responsible for:

- Day-to-Day Operations – The (CA)^2 Administrator is responsible for addressing agency questions, comments or concerns, troubleshooting issues, and updating the (CA)^2 system to address changes in OA/OIT ITPs or security threats.

- (CA)^2 System Administration – (CA)^2 Administrator will ensure enter and update user accounts in the (CA)^2 system.

- (CA)^2 Review Board - The (CA)^2 Administrator will act as the (CA)^2 Review Board coordinator and schedule meetings between the (CA)^2 Review Board, (CA)^2 Points of Contact (POC), and agency personnel.

- (CA)^2 Reviewers – The CISO will be responsible working with OA/OIT Bureau Directors to appoint representatives from their respective bureaus to participate on the (CA)^2 Review Board. The (CA)^2 reviewers will assist OA/OIT/EISO in evaluating (CA)^2 submissions and represent OA/OIT in instances where clarification is needed or agencies request technical assistance.

- (CA)^2 POC – Agencies are responsible for appointing representatives to act as the liaison between the agency, OA/OIT/EISO, and the (CA)^2 Review Board. In addition to this, (CA)^2 POC is responsible for:

  - Submitting Web Applications – The (CA)^2 POC is responsible for entering agency Web application information into the (CA)^2 system.

  - Updating Web Application Information – If there are changes to an application's security architecture, the (CA)^2 POC will be responsible resubmitting the application through the (CA)^2 process. Changes to an application's security architecture that are not documented in the (CA)^2 system will cause the application to become non-accredited.

  - Triennial Reaccreditation – The (CA)^2 POC is responsible for ensuring that all Web applications due to be reaccredited are resubmitted through the (CA)^2 process before the application's expiration date.

Note: Failure to submit an application before the expiration date will cause the application to become unaccredited and the agency will assume the risk of allowing the application to continue to operate in this condition.

  - Contacting the OA/OIT/EISO – The (CA)^2 POC will be responsible for contacting the OA/OIT/EISO to add/delete (CA)^2 users, request assistance with security scans, and to request meeting with the (CA)^2 Review Board.

OA/OIT/EISO - OA/OIT/EISO is headed by the CISO and is responsible for conducting security assessments on Web applications and Web sites to make sure they comply with the requirements identified within the ETA, MD 210.12, and the ITPs. In addition to security assessments, OA/OIT/EISO will ensure that the $(CA)^2$ process is updated on an ongoing basis to ensure that it takes into account the latest cyber security threats to Web applications and Web sites. OA/OIT/EISO is also responsible for:

- Source Code Application Scans – In accordance with the $(CA)^2$ process, Web applications have to undergo a source code analysis to ensure that there are no application coding flaws that could be exploited by hackers and crackers to circumvent the application and network security protocols. As part the process, OA/OIT/EISO will review source code scan reports to make sure those applications don't have coding vulnerabilities.

Note: Upon request, OA/OIT/EISO will assist agencies in completing source code scans.

- Host-Based Intrusion Scans – All Web applications hosted on agency Web servers will have to provide OA/OIT/EISO with a copy of a current intrusion scan report that shows that the host is secure and the most recent patches are in place.

- Web Application Scans – While deployed in staging, Web applications are to undergo a Web application scan to show that the application security protocols are in place and functioning correctly. This report would be attached to the $(CA)^2$ submission and reviewed by OA/OIT/EISO to make sure there are no issues.

- Payment Card Industry Data Security Standard (PCI-DSS) – OA/OIT/EISO will assess Web applications that process credit cards to see if they comply with PCI- DSS and OA/OIT policies, procedures, and standards.

Agencies – Agencies developing or procuring Web applications have to complete the $(CA)^2$ process. In addition to completing the $(CA)^2$ process, agencies are responsible for:

- Appointing $(CA)^2$ POC – As part of the assessment process, agencies will 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/EISO, and the $(CA)^2$ review. For more information about the $(CA)^2$ POC roles and responsibilities, reference the section entitled *$(CA)^2$ Review Board, $(CA)^2$ Points of Contact (POC)*.

- Triennial Reaccreditation – Web applications are accredited for only three years. After three years, applications have to undergo the reaccreditation process which means that agencies are to update the application information

and complete the $(CA)^2$ risk assessment process.

- Compliance - Agencies will make sure that they comply with the policies, procedures, and standards identified in OA/OIT ITPs.

- Risk Mitigation Plan – Agencies that have applications that have risks that cannot be remediated will be required to submit a risk mitigation plan to OA/OIT/EISO. This plan will identify the risks associated with the Web application and identify how the agency plans to mitigate those risks.

- Conditional Accreditation – Applications receiving conditional approvals will only receive 18 month grace period to remediate the issues documented during the $(CA)^2$ risk assessment process. After this period, agencies will need to resubmit the application for a new risk assessment.

- Agency or Business Owner-Specific Security Requirements – The agency will be responsible for capturing any agency or business owner-specific security requirements not addressed in the OA/OIT ITPs.

Office of the Budget, Comptroller Operations, Bureau of Audits (OB-BOA) – OB-BOA is responsible for evaluating the risk and materiality impact of financial or fiscal- based applications and determining if further examination or assessment is warranted. In addition to this, OB-BOA will:

- $(CA)^2$ Review Board Representative(s) – The Director of OB-BOA is responsible for appointing members from the bureau to participate in the $(CA)^2$ process.

- Accounting and Financial Controls – OB-BOA is responsible for evaluating the soundness, adequacy, and relevance of controls related to accounting and financial applications.

6. Procedures

The $(CA)^2$ process is broken into four phases based on the SDLC process. These phases are entitled: the initiation phase, which occurs immediately after business requirements and prior to the development process; the certification phase, which occurs during the development process; the accreditation phase, which occurs when the application is placed into staging; and the maintenance phase, which occurs after the application is placed into production. The will provide more detail on these phases:

- **Initiation Phase**
  Prior to proceeding to the development phase, agencies will be required to complete a $(CA)^2$ request. In order to do this, the $(CA)^2$ POC will complete a policy validation assessment. This assessment contains questions based on the current OA/OIT ITPs and are meant to measure the proposed

application's compliance with OA/OIT policies, procedures, and standards.

As part of this process, the $(CA)^2$ POC will access the assessment via the $(CA)^2$ system. After accessing the assessment, the $(CA)^2$ POC will answer the questions based upon the information it has in its Web application's requirements document. When completed, the $(CA)^2$ POC will submit the questionnaire to the $(CA)^2$ Review Board who will review the questionnaire to determine if the proposed application:

- Complies with OA/OIT's policies, procedures and standards.
- Properly identifies the data security level.
- Proposes security measures to address potential security risks.

If there are no issues, the $(CA)^2$ Review Board will signoff on the request and $(CA)^2$ POC will receive a message from the $(CA)^2$ system that it can proceed to the certification phase.

If there are issues, the $(CA)^2$ Review Board will put its questions or comments into the $(CA)^2$ assessment and the $(CA)^2$ system will forward them back to the $(CA)^2$ POC which will take the questions and comments back to its development team and address the questions. After the issues have been addressed, the $(CA)^2$ POC will put the agency's response into the $(CA)^2$ system and resubmit its request. This process will continue until the $(CA)^2$ Review Board signs-off on the request.

Note: If further clarification is needed, the $(CA)^2$ POC can contact the $(CA)^2$ Administrator to request a meeting with the $(CA)^2$ Review Board to address any concerns that the agency might have with the $(CA)^2$ Review Board's questions or comments, or to get guidance on how the $(CA)^2$ Review Board would like the agency to address security-related issues.

- **Certification Phase**

  After the $(CA)^2$ Review Board has signed off on the initiation phase, the agency can start the development process. During this process, the agency is to use a source code scanning tool to scan the Web application's source code as it is being written to catch any application coding errors that could lead to potential security vulnerabilities such as cross-site scripting and SQL inject attacks.

  Upon completion of the development process, the agency will need to conduct a final source code scan on the application and submit a final report. The final report needs to show that there are no security vulnerabilities with the application code before the application will be allowed to proceed to the accreditation phase.

  The results of this scan need to be converted to a readable format (e.g., PDF,

MS Word) and attached to the $(CA)^2$ request. OA/OIT/EISO will review the report to ensure that there are no issues that would prevent the application from moving into staging.

Note: Agencies using a third-party vendor to develop the application or deploying a COTS solution will need to contact the vendor and request that it provides them with this report before hosting it on the Commonwealth's network.

If there are no issues, the application is deemed as certified and the application moves onto the accreditation phase. If there are issues, the OA/OIT/EISO will send the report back to the agency with questions/comments and the agency will either remediate the issues or submit a risk mitigation plan, which OA/OIT/EISO will review to determine if the application will proceed as a conditionally accredited Web application.

- **Accreditation Phase**

  After the Web application has been certified, the agency will begin the accreditation process. During this phase, the agency will move the Web application into the staging environment. After the application is ready to be moved into staging, the agency is required to complete the following security assessments:

  - Intrusion Testing – Agencies hosting Web applications will be required to submit a host-based assessment to OA/OIT/EISO prior to hosting Commonwealth applications or data. Scan results are to be in a readable format and are to have both a high-level executive summary and a detailed findings document. OA/OIT/EISO will review the report to ensure that there are no issues that would prevent the application from moving into production.

  - Web Application Vulnerability Assessments and Penetration Testing (Vulnerability Assessment) – Agencies that have procured a COTS solution or who have developed an in-house application have to ensure that it undergoes a vulnerability assessment before putting the application into production. This process enables the agency and OA/OIT/EISO to validate that the security measures that they have identified in the initiation phase are functional and they have mitigated any risks before placing the application into production.

  Upon the completion of these assessments, the $(CA)^2$ POC will access the $(CA)^2$ system and submit the executive summaries from these scans. OA/OIT/EISO will review these summaries to ensure there are no exploitable vulnerabilities.

  The $(CA)^2$ POC will be notified if there are issues and what actions need to be taken to address them. This process will continue until the application is

accredited or the agency submits a risk mitigation plan that addresses how it will mitigate the risks.

OA/OIT/EISO will review the risk mitigation plan, if any, to make sure that it addresses the risks identified by the $(CA)^2$ process. After the OA/OIT/EISO signs off on the risk mitigation plan, the $(CA)^2$ request will be forwarded to the CTO with the recommendation that the$(CA)^2$ application receive a conditional accreditation. If granted, the CTO will notify the $(CA)^2$ Administrator, who will notify the $(CA)^2$ POC to proceed with moving the application into production based on a conditional accreditation, which means that the application's potential risks have been identified and mitigated and the maintenance phase will begin.

If there are no issues, the OA/OIT EISO will approve the application and forward it onto the CTO for final approval. If the request is approved by the CTO or the CTO's designee, the $(CA)^2$ POC will be notified that its application is $(CA)^2$ accredited. The $(CA)^2$ Administrator will then forward the agency a $(CA)^2$ JPEG to affix to the application as proof that it has successfully undergone the $(CA)^2$ process. At this point, the application will move into production and the $(CA)^2$ maintenance phase begins.

- **Maintenance Phase**
  During the maintenance phase, the agency will have to proactively monitor its firewall and intrusion detection logs to make sure that there are no attempts to breach the application or Web site. All attempts are to be reported to OA/OIT/EISO and successful breaches will require the agency to reconfigure its application's or Web site's security architecture to address the problem that caused the breach.

  In addition to proactively monitoring their systems, agencies are to keep abreast of the current cyber security threat environment in order to properly identify potential threats to their applications and Web sites. As part of this process, the agency will have to account for any potential threats that could exploit the application or Web sites architecture. These threats are to be mitigated and the agency will be required to update its $(CA)^2$ submission to reflect these changes.

  Note: All security-related changes or updates to an application have to be entered in the $(CA)^2$ system as an update.

  The final step in the maintenance phase is the reaccreditation process. In order for an application to maintain its accreditation status, agencies will need to repeat the $(CA)^2$ process.

  As part of this process, the $(CA)^2$ POC will receive an e-mail from the $(CA)^2$ system notifying the POC that its accreditation status will expire in 180 days.

These notifications will occur in increments of 180 days, ninety days, sixty days and thirty days, and then after thirty days the $(CA)^2$ system will notify the $(CA)^2$ POC daily until the Web application gets reaccredited or the agency removes it from the $(CA)^2$ system.

In order to reaccredit the application, the $(CA)^2$ POC will have to access the $(CA)^2$ system and update its application form. The POC will confirm that information provided hasn't changed and submit executive summaries for recent source code scans, intrusion tests, and vulnerability assessments into the $(CA)^2$ system.

The $(CA)^2$ Review Board and OA/OIT/EISO will then review this information and reaccredit the application or repeat the processes identified in the previous steps. Once the application is reaccredited, it will return to the maintenance phase until the agency either removes the application from production or reaccredits it.

7. Related ITPs/Other References

- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- MD 210.12 – *Electronic Commerce Initiatives and Security*

8. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

9. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	4/28/2009	Replaces ITB B.5 Security & Digital Certificate Policy and Encryption & Internet/Intranet Browser Standards for e-Government Web Sites & Applications
	12/23/2009	The policy had to be modified to meet new application hosting requirements identified by the Office of General Counsel.
	9/17/2010	Recertification has been changed to every three years
	8/16/2011	The scope was modified to clarify what applications need to go through the process, a new term called "At Risk Application" was added, and a new clause informing agencies that submissions not updated within one year of the initial submission will be automatically be removed from the $(CA)^2$ system.
	4/2/2014	ITP Reformat