RSAC Sandbox

RSAConference2020

HUMAN ELEMENT

SESSION ID: **SBX1-R5**

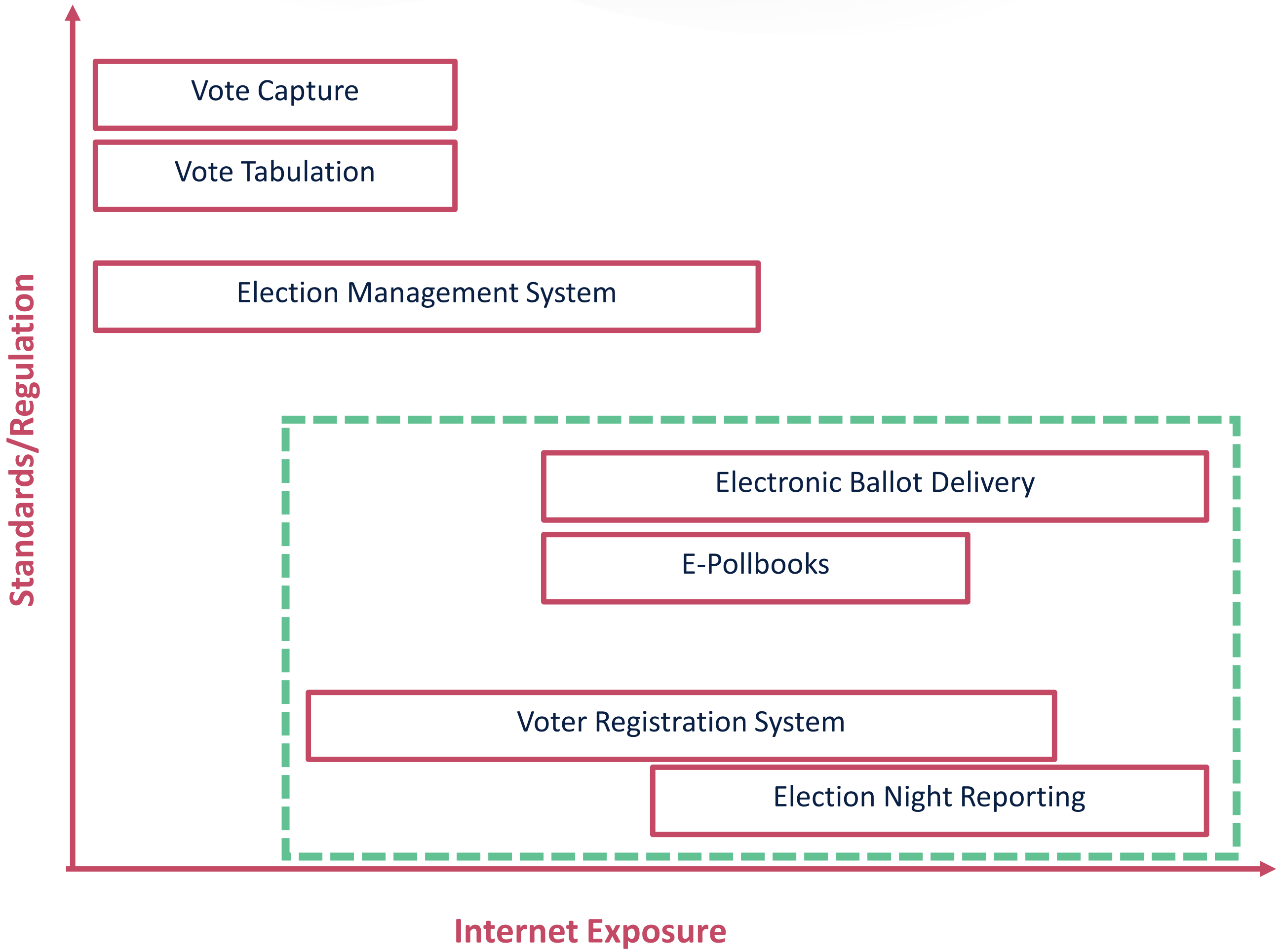
Beyond the Ballot Box: Securing America's Supporting Election Technology

Aaron Wilson

Sr. Director of Election Security
Center for Internet Security
@aa_wilson

Non-Voting Election Technology Best Practices

- Exposure to more threats
- Significant impact on voter confidence
- Very few existing standards



Standards/Regulation

Vote Capture

Vote Tabulation

Election Management System

Electronic Ballot Delivery

E-Pollbooks

Voter Registration System

Election Night Reporting

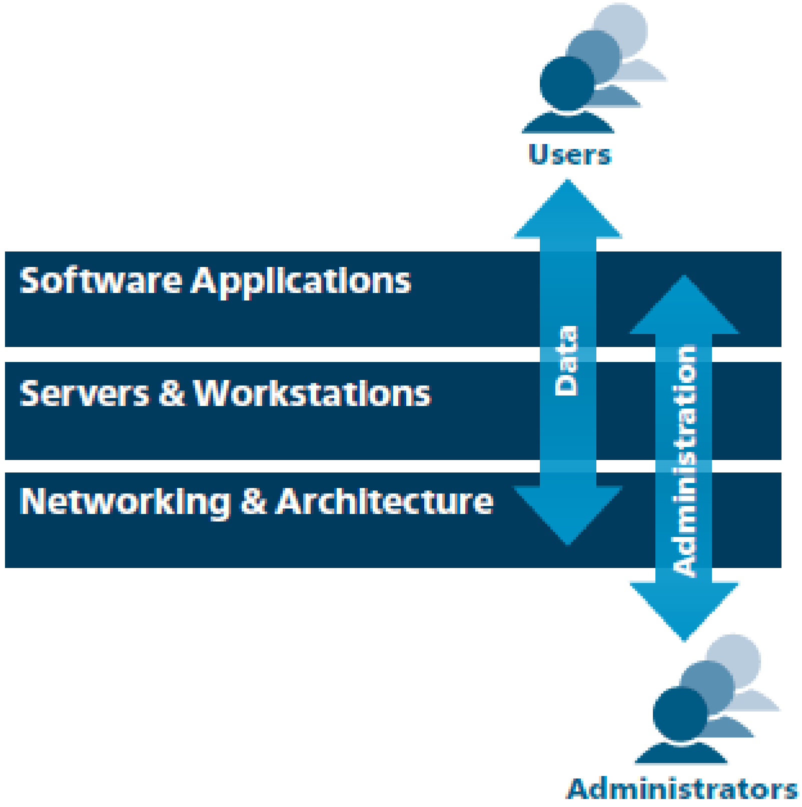
Internet Exposure

Security Best Practices
for Non-Voting
Election Technology

- How to secure internet-connected election services
- 160 best practices tailored for election technology
- Target audience is technology providers
- Developed with the help of election officials and technology providers

Organization and Structure

- Technology Areas



Users

Software Applications

Servers & Workstations

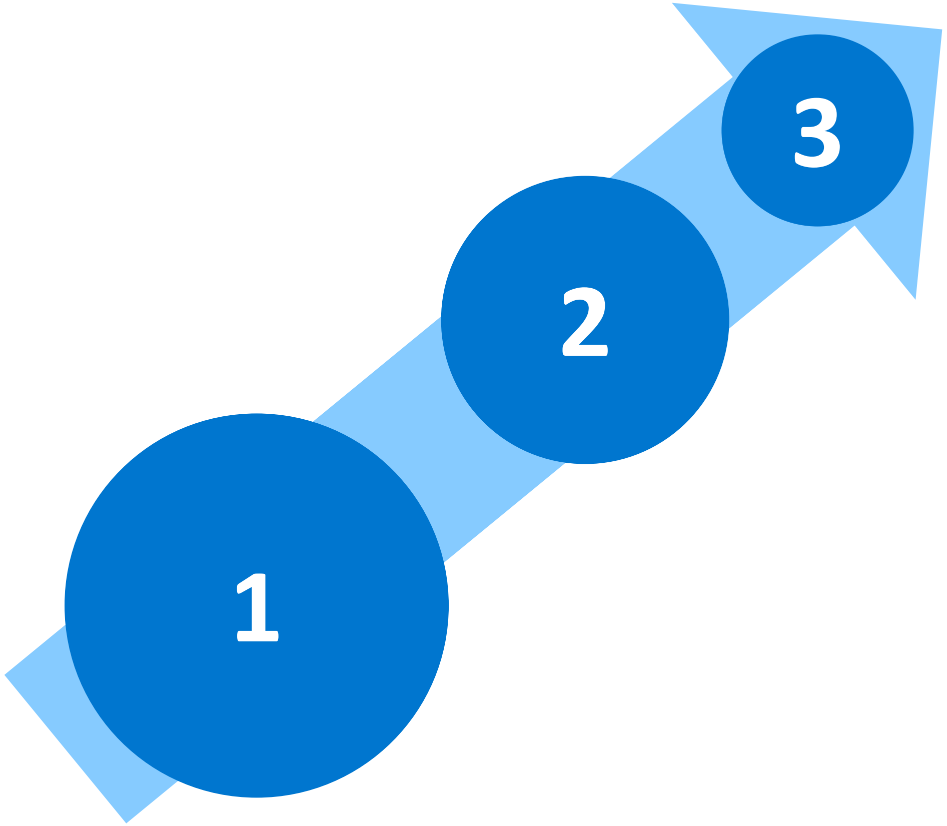
Networking & Architecture

Data

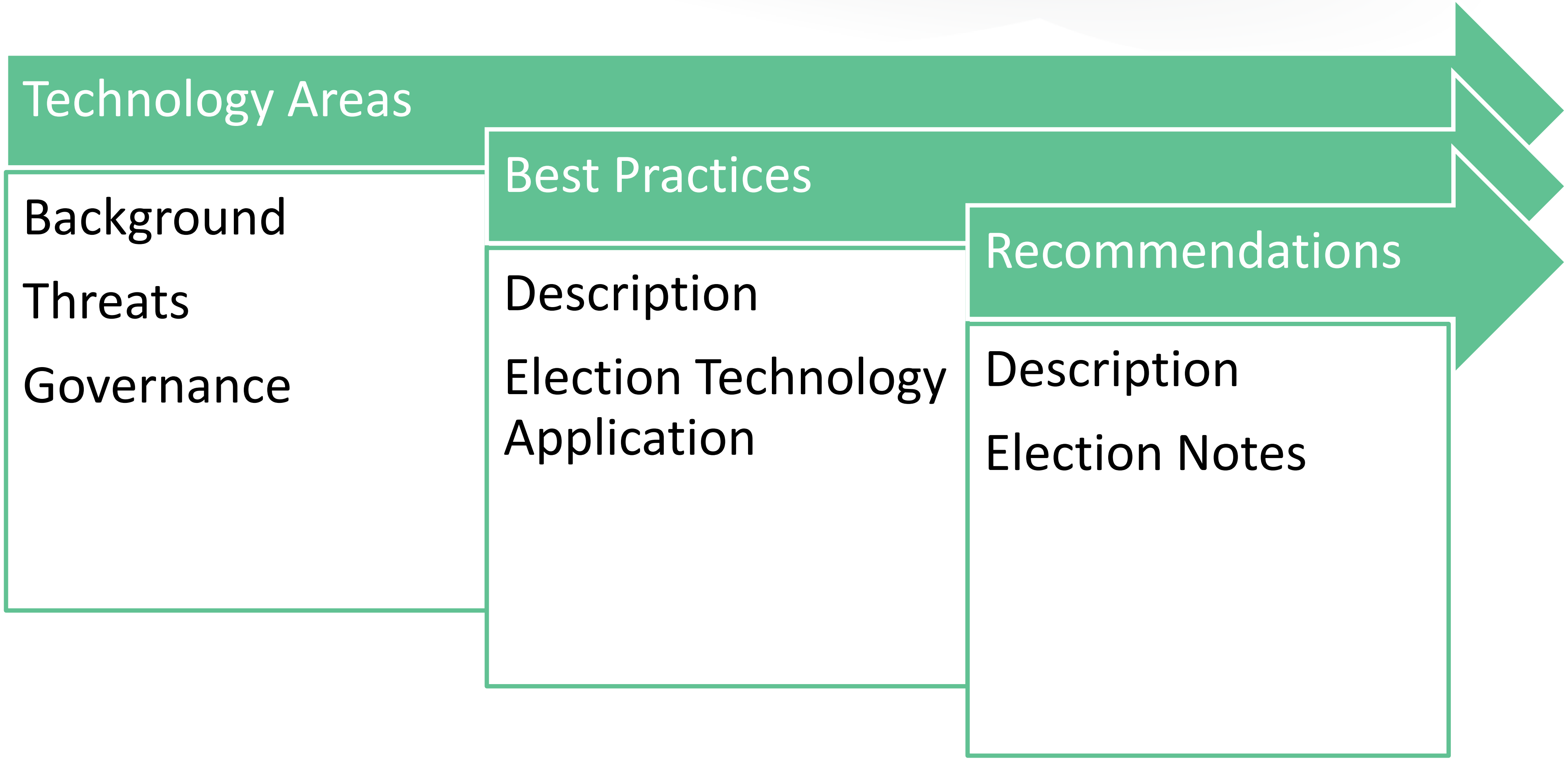
Administration

Administrators

- Profile Levels



Structure



Technology Areas

- Background
- Threats
- Governance

Best Practices

- Description
- Election Technology Application

Recommendations

- Description
- Election Notes

Denial of Service Example

1

1.1.3 Deny Communications with Known Malicious IP Addresses

1.3.4 Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

1.5.1 Establish and Maintain Effective Partnerships With Your Upstream Network Service Provider

1.5.2 Port and Packet Size Filtering

1.5.7 Set Up Out-of-Band Communication for DDoS Response

2

1.5.3 Enable Firewall Logging

1.5.5 Configure Devices to Detect and Alarm on Traffic Anomalies

5.4.2 Assign Job Titles and Duties for Incident Response

3

1.5.4 Configure Perimeter Devices to Prevent Common Types of Attacks

1.5.6 Establish DDoS Mitigation Services With a Third-Party DDoS Mitigation Provider

3.2.12 Deploy Web Application Firewalls

Ransomware Example

1

1.1.4 Deny Communications with Known Malicious IP Addresses

1.1.6 Deploy Network-Based IDS Sensors

1.4.1 Ensure Regular Automated Backups

1.4.2 Perform Complete System Backups

1.4.4 Protect Backups

1.4.5 Ensure All Backups Have at Least One Offline Backup Destination

2.3.1 Utilize Centrally Managed Anti-Malware Software

4.1.1 Maintain an Inventory of Sensitive Information

4.1.2 Remove Sensitive Data or Systems Not Regularly Accessed by the Organization

2

1.4.3 Verify Data on Backup Media

1.1.7 Deploy Network-Based Intrusion Prevention Systems

2.3.3 Enable Operating System Anti-Exploitation Features and Deploy

Anti-Exploit Technologies

2.4.3 Ensure the Use of Dedicated Administrative Accounts

4.2.5 Segment the Network Based on Sensitivity

3

1.1.2 Scan for Unauthorized Connections across Trusted Network Boundaries

1.4.6 Verify Complete System Recovery

2.3.7 Deploy a Host-Based Intrusion Detection System

4.1.4 Monitor and Detect Any Unauthorized Use of Encryption

Unauthorized Data Modification Example

1

1.6.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

2.2.1 Run Automated Vulnerability Scanning Tools

2.2.5 Deploy Automated Software Patch Management Tools

2.4.2 Change Default Passwords

3.1.1 Store and Communicate Data Securely

3.1.2 Use the Latest Best Practices for Identifying and Authenticating Users

3.1.3 Use Best Practices for Securely Handling Input and Output

3.1.4 Deploy Appropriate Access Control Mechanisms

4.2.2 Digitally Sign Sensitive Information in Transit

4.3.1 Follow Secure Configuration Guidance for Cloud Storage

2

1.4.3 Verify Data on Backup Media

2.2.2 Perform Authenticated Vulnerability Scanning

2.5.4 Use Write-Once or Formatted Media

3.2.16 Use Standard Hardening Configuration Templates for Databases

5.1.3 Require Multi-Factor Authentication

3

1.1.9 Deploy Application Layer Filtering Proxy Server

1.4.6 Verify Complete System Recovery

2.5.8 Use USB Write Blocker to Transfer Data into Sensitive Systems

3.2.14 Deploy Web Application Firewalls (WAFs)

4.2.9 Enforce Access Control to Data through Automated Tools

Verifying Election Technology with RABET-V

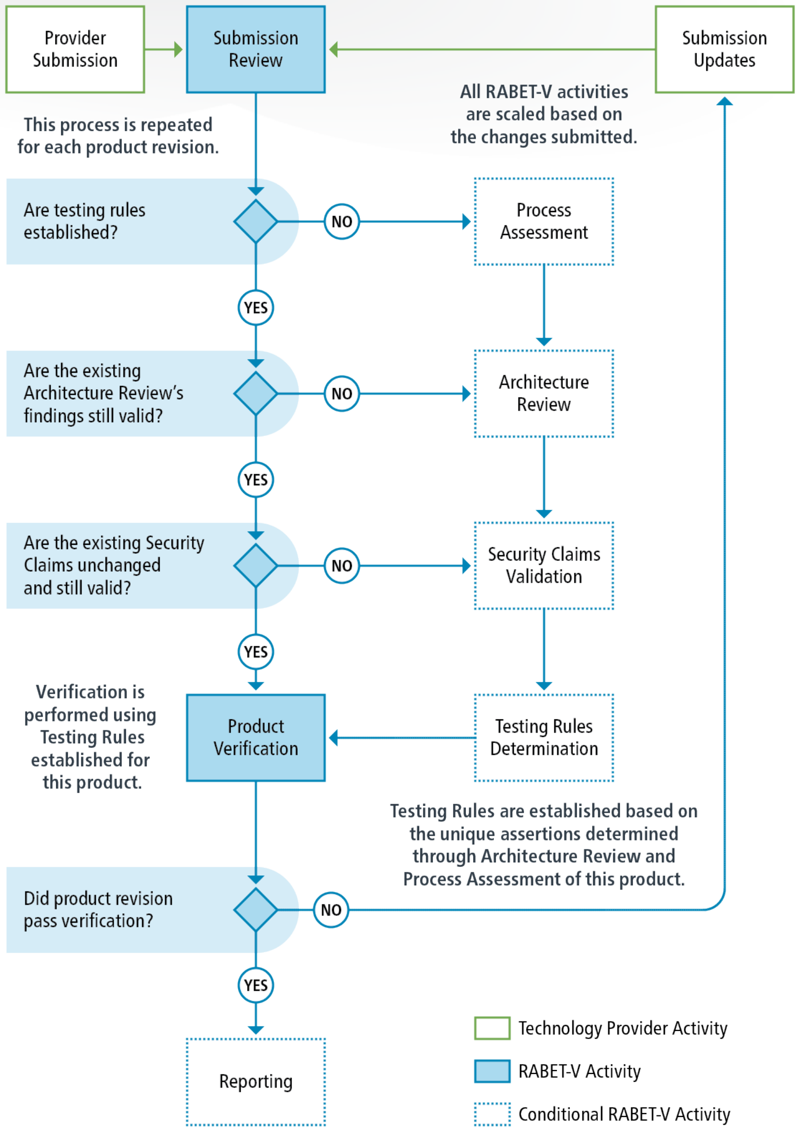
RABET-V: Rapid Architecture-Based Election Technology Verification

What is RABET-V

- RABET-V is an **election technology verification process** that supports **rapid** product changes **by design**
- Informed by our community of election stakeholders
- Uses a risk-based approach to verifying product revisions, where the risk estimate is based heavily on the **product architecture** and the **provider's software development processes**.
- Leverages modern software development, testing, and deployment processes

RABET-V Process Flow

- RABET-V is a total of seven activities, five of which are conditional activities
- Repeated for initial review and subsequent product revisions
- Activities adapt to the risk associated with the product changes



Provider Submission

Submission Review

Submission Updates

This process is repeated for each product revision.

All RABET-V activities are scaled based on the changes submitted.

Are testing rules established?

NO

Process Assessment

YES

Are the existing Architecture Review's findings still valid?

NO

Architecture Review

YES

Are the existing Security Claims unchanged and still valid?

NO

Security Claims Validation

YES

Verification is performed using Testing Rules established for this product.

Product Verification

Testing Rules Determination

Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.

Did product revision pass verification?

NO

YES

Reporting

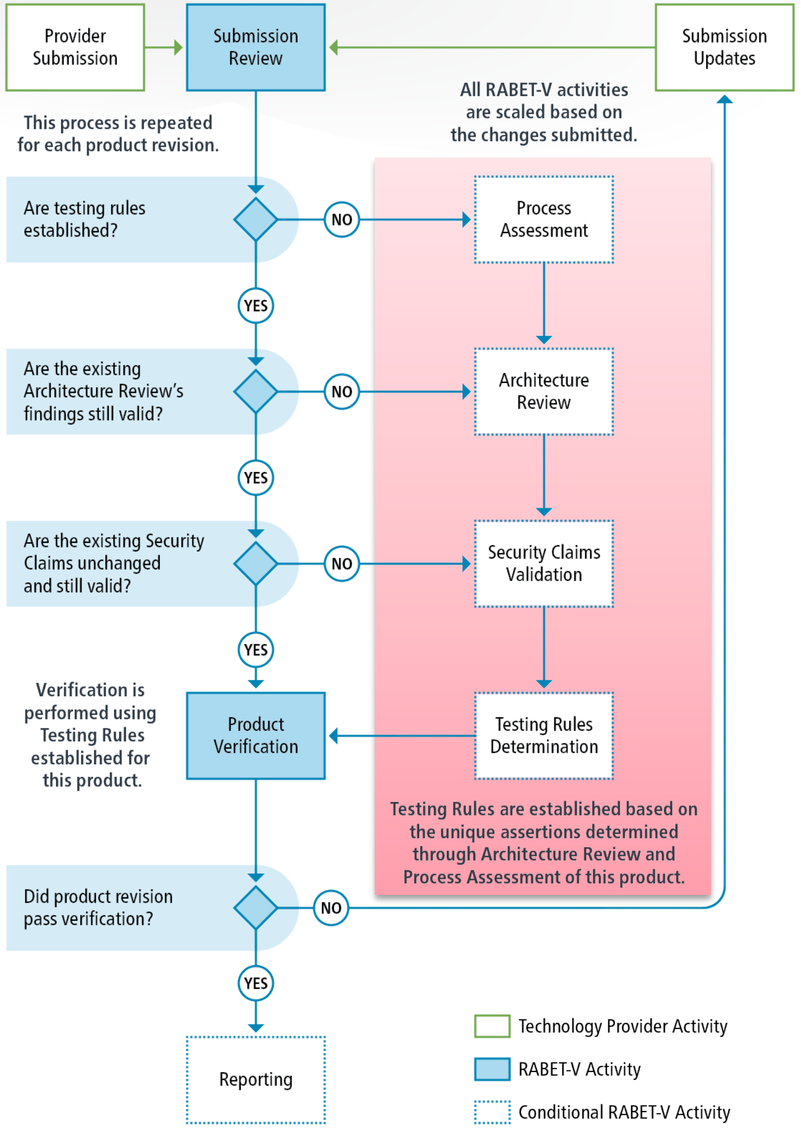
□ Technology Provider Activity

🟦 RABET-V Activity

⬚ Conditional RABET-V Activity

RABET-V Initial Review

- Unique product Testing Rules are determined based on risk
- The **Process Assessment**, **Architecture Review**, and **Security Claims Validation** activities provide assertions about the system's construction which inform the **Testing Rules Determination**
- Testing Rules determine how to test product changes



Provider Submission

Submission Review

Submission Updates

This process is repeated for each product revision.

All RABET-V activities are scaled based on the changes submitted.

Are testing rules established?

NO

YES

Process Assessment

Are the existing Architecture Review's findings still valid?

NO

YES

Architecture Review

Are the existing Security Claims unchanged and still valid?

NO

YES

Security Claims Validation

Verification is performed using Testing Rules established for this product.

Product Verification

Testing Rules Determination

Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.

Did product revision pass verification?

NO

YES

Reporting

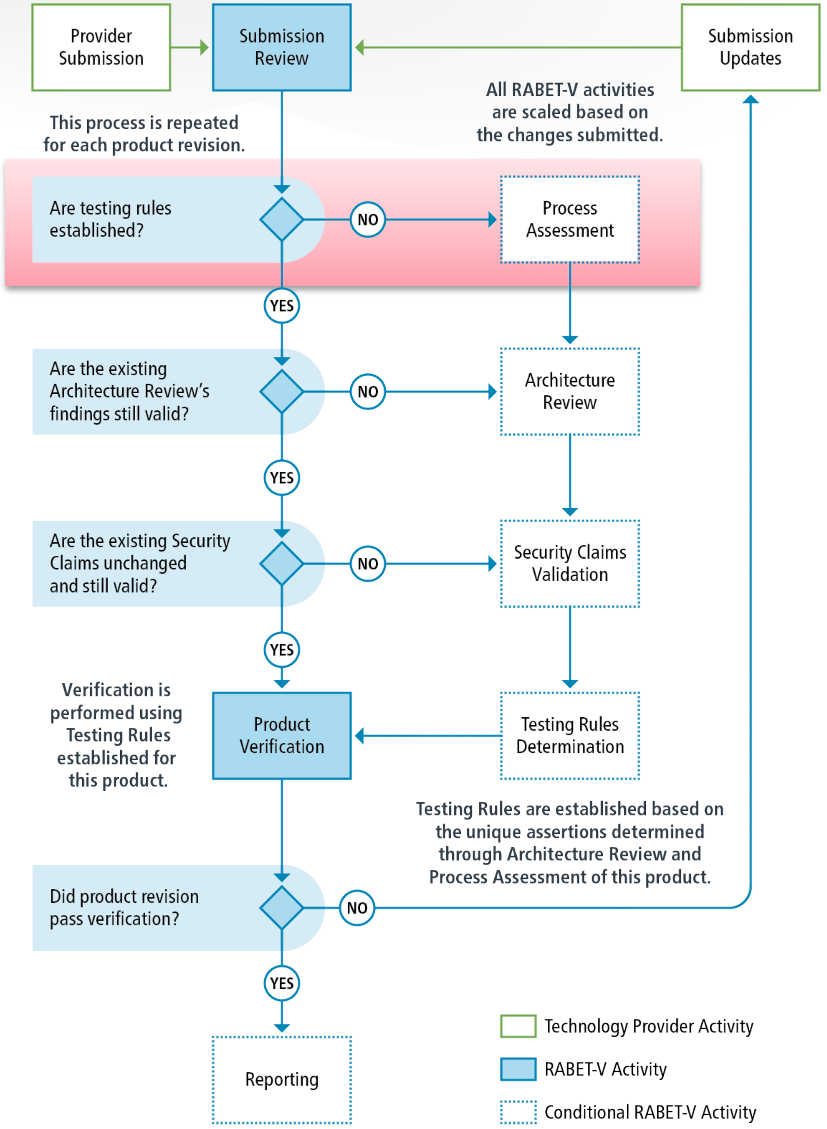
□ Technology Provider Activity

■ RABET-V Activity

⬚ Conditional RABET-V Activity

Process Assessment

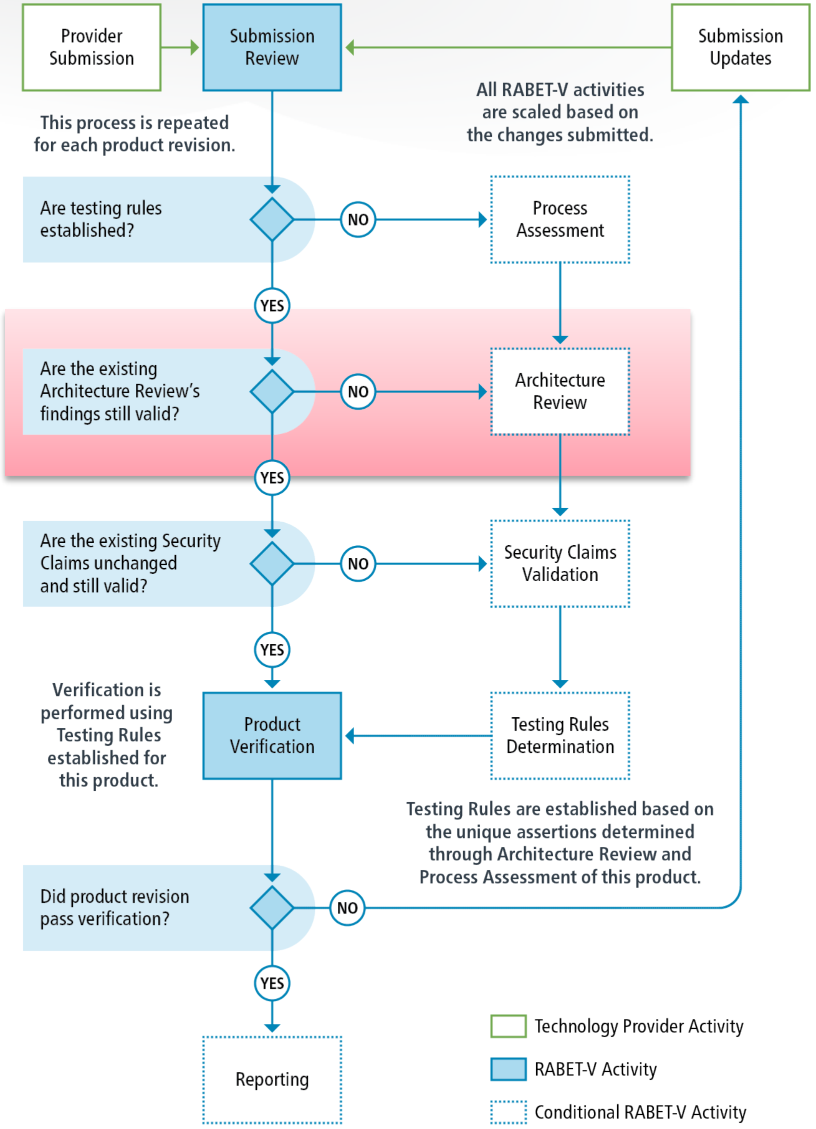
- Focuses on developer's software development lifecycle processes
- Product changes resulting from organizations with more mature processes will be considered lower risk
- More reliable process artifacts make RABET-V testing more streamlined



Provider Submission
Submission Review
Submission Updates
This process is repeated for each product revision.
All RABET-V activities are scaled based on the changes submitted.
Are testing rules established?
NO
Process Assessment
YES
Are the existing Architecture Review's findings still valid?
NO
Architecture Review
YES
Are the existing Security Claims unchanged and still valid?
NO
Security Claims Validation
YES
Verification is performed using Testing Rules established for this product.
Product Verification
Testing Rules Determination
Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.
Did product revision pass verification?
NO
YES
Reporting
Technology Provider Activity
RABET-V Activity
Conditional RABET-V Activity

Architecture Review

- Results in assertions about how the system should be tested
  - System
  - Software
  - Security
  - Data
- Well-architected solutions will result in the maximum amount of assertions and shorter verification cycles



Provider Submission

Submission Review

Submission Updates

This process is repeated for each product revision.

All RABET-V activities are scaled based on the changes submitted.

Are testing rules established?

NO

Process Assessment

YES

Are the existing Architecture Review's findings still valid?

NO

Architecture Review

YES

Are the existing Security Claims unchanged and still valid?

NO

Security Claims Validation

YES

Verification is performed using Testing Rules established for this product.

Product Verification

Testing Rules Determination

Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.

Did product revision pass verification?

NO

YES

Reporting

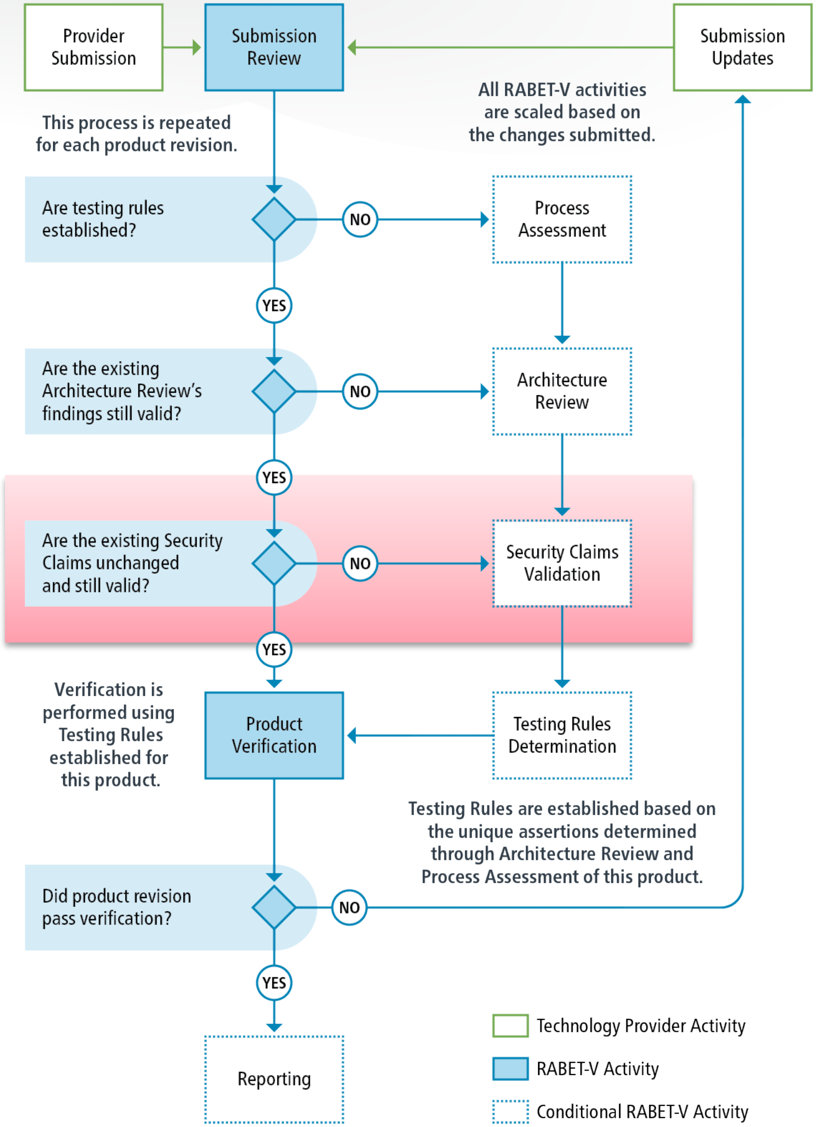
Technology Provider Activity

RABET-V Activity

Conditional RABET-V Activity

Security Claims Validation

- Looks at the claims made by Technology Provider about the product security, i.e.
  - Input Sanitization
  - Error Handling
- Validates claims and key architectural elements supporting the claims
- Validated claims are published at the end of each iteration



Provider Submission

Submission Review

Submission Updates

This process is repeated for each product revision.

All RABET-V activities are scaled based on the changes submitted.

Are testing rules established?

Process Assessment

Are the existing Architecture Review's findings still valid?

Architecture Review

Are the existing Security Claims unchanged and still valid?

Security Claims Validation

Verification is performed using Testing Rules established for this product.

Product Verification

Testing Rules Determination

Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.

Did product revision pass verification?

Reporting

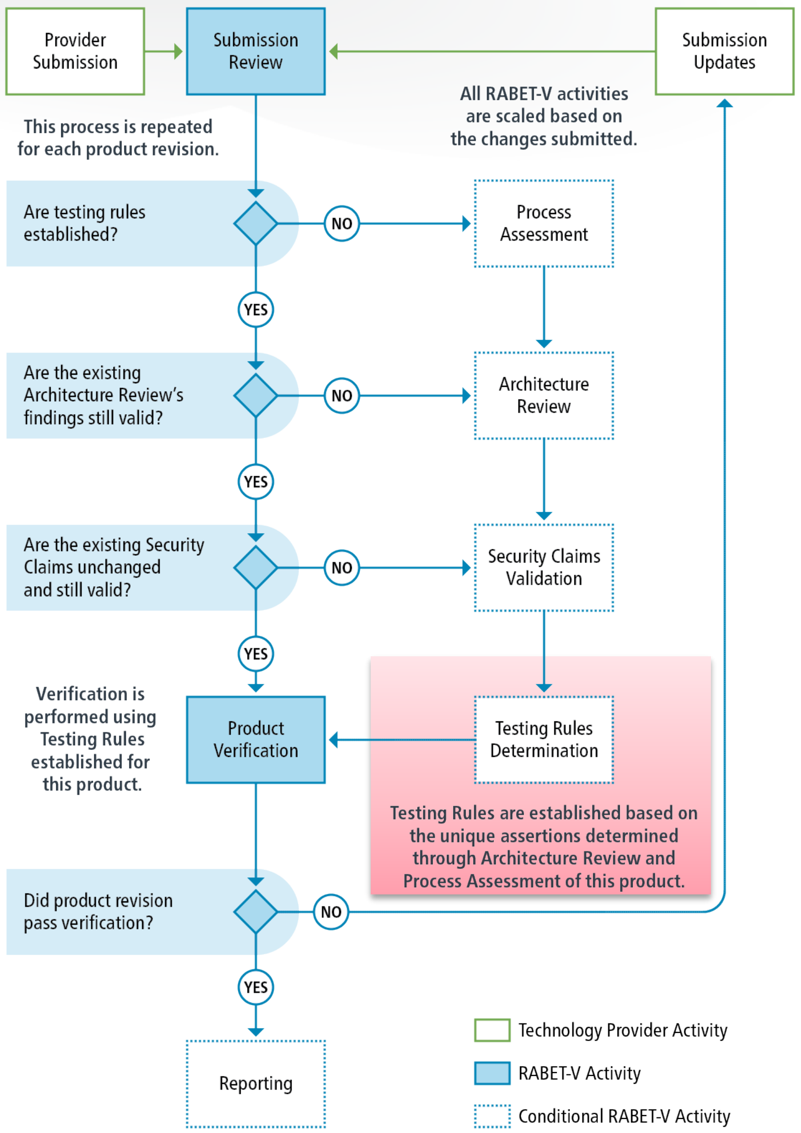
Technology Provider Activity

RABET-V Activity

Conditional RABET-V Activity

Testing Rules Determination

- Builds a set of Testing Rules to achieve the most rapid, flexible, and reliable testing of product revisions possible given the product architecture and provider's processes
- Matches test methods with change types



Provider Submission

Submission Review

Submission Updates

This process is repeated for each product revision.

All RABET-V activities are scaled based on the changes submitted.

Are testing rules established?

NO

Process Assessment

YES

Are the existing Architecture Review's findings still valid?

NO

Architecture Review

YES

Are the existing Security Claims unchanged and still valid?

NO

Security Claims Validation

YES

Verification is performed using Testing Rules established for this product.

Product Verification

Testing Rules Determination

Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.

Did product revision pass verification?

NO

YES

Reporting

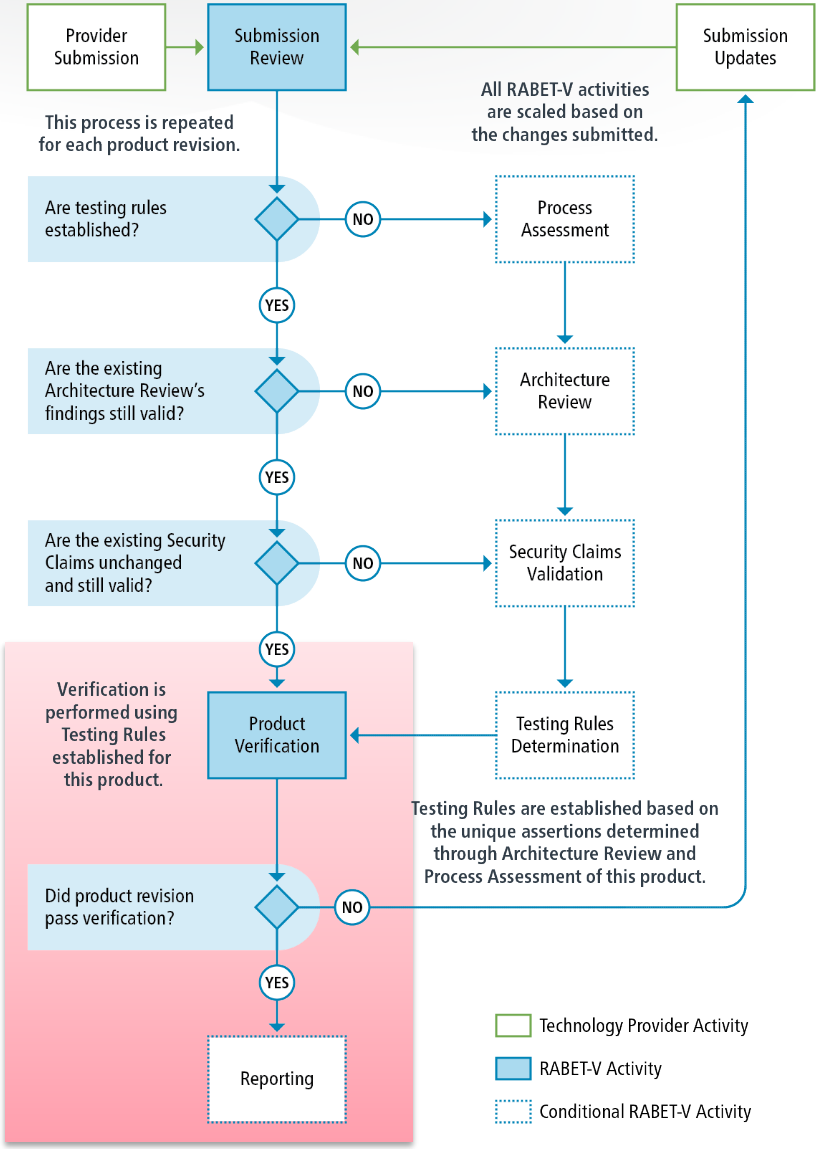
□ Technology Provider Activity

■ RABET-V Activity

⬚ Conditional RABET-V Activity

Product Verification and Reporting

- Test Plan created from Testing Rules
- Test Plan is more streamlined for small, low-risk change sets
- Will leverage product development artifacts when possible
- Reporting on product goals, expected usage, validated security claims, and verified product changes



Provider Submission

Submission Review

Submission Updates

This process is repeated for each product revision.

All RABET-V activities are scaled based on the changes submitted.

Are testing rules established? — NO → Process Assessment; YES ↓

Are the existing Architecture Review's findings still valid? — NO → Architecture Review; YES ↓

Are the existing Security Claims unchanged and still valid? — NO → Security Claims Validation; YES ↓

Testing Rules Determination

Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.

Verification is performed using Testing Rules established for this product.

Product Verification

Did product revision pass verification? — NO → Submission Updates; YES ↓

Reporting

□ Technology Provider Activity

■ RABET-V Activity

⬚ Conditional RABET-V Activity

RABET-V Provides...

- Rapid testing of many product revisions, allowing products to innovate and maintain proper security patches
- Re-verification of product changes at a minimum cost
- Incentives for high-quality, modern system architectures that are more resistant to attacks and more resilient in recovery
- Incentives for technology providers to have robust, risk-mitigating software development processes
- Incentives to update in smaller, more manageable cycles, more accurately reflecting the modern age of software development
- A consistent basis from which approval authorities (namely states) can draw information, resulting in quicker decisions and reduced, amortized overall cost.

RABET-V Pilot Program

- Launched in February 2020
  - Steering Committee – Federal agencies, states election officials, vendors
  - Technical Advisory Committee – industry experts
- Developing our Working Model
- Get the latest information on our project hub:
  - https://github.com/it-dept-cis/RABET-V-Pilot

RABET-V Pilot Program Questions

- What are the time and cost expectations for each activity during the initial and subsequent iterations?
- What is the best way to conduct architecture reviews and are they are risk-informing as we propose?
- What is the best way to conduct process assessments and are they as risk-information as we propose?
- What is the best approach to a long term RABET-V process?

Apply What You've Learned Today

- Next week you should:
  - Learn and adopt the security best practices for non-voting election technology
  - Begin to follow the RABET-V pilot at https://github.com/it-dept-cis/RABET-V-Pilot
- In the first three months following this presentation you should:
  - Understand how to secure your election technology and begin implementing missing controls
- Within six months you should:
  - Review the RABET-V pilot program reports
  - Prepare your product for RABET-V

Thank You

Any questions?