Addressing the Statewide Challenge of Application Security

Jack Danahy
VP Product/Engineering
NuHarbor Security

Why Me?

30 years in Cybersecurity
12 patents (6 in Application Security)
Founder, 3 Cybersecurity Companies – All acquired

- **Ounce Labs**, acquired by IBM: Industry's first Application Security analytics platform
- Former WW Executive/Application Security and Director/Advanced Security at IBM

Currently Product/Engineering Leader at NuHarbor Security

- Creator – ASCOE initiative

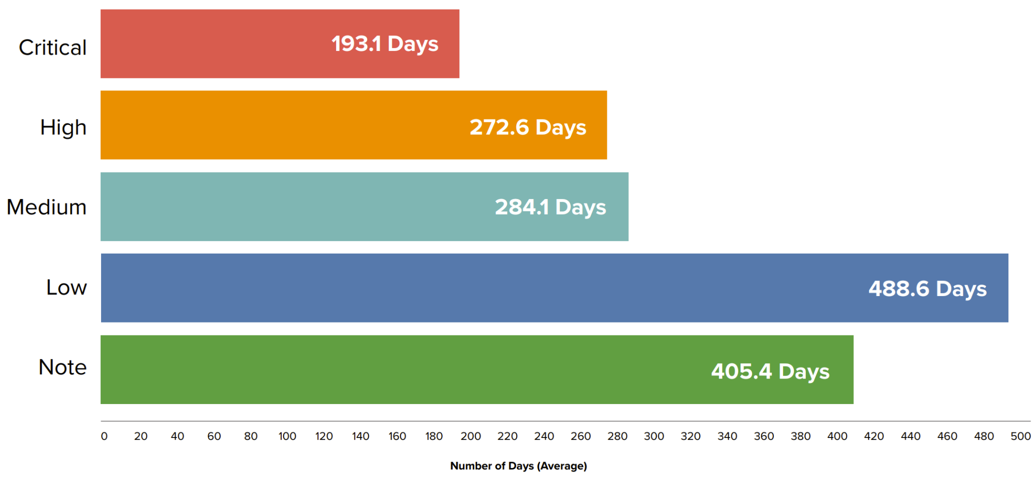
jdanahy@nuharborsecurity.com
(802) 503-0907

Application Security Prioritization

60%

have had production applications exploited by OWASP top-10 vulnerabilities in the past 12 months

Time to Fix Vulnerabilities



Risks

Application security and software supply chain security are increasingly important, as all attack types, from ransomware to credential theft, to APT's, are leveraging both configuration and software vulnerabilities.

Impacts

- Vulnerabilities in third-party software account for 14% of data breaches at an average cost of $4.33M across all industries
- The average cost of a data breach in the public sector is $1.93M
- 82% of public sector applications contain security flaws
- Public sector flaw fix rate is 22%

Statewide Application Security

Critical Considerations

Liability : Applications identified with vulnerabilities that are left unmitigated present a liability to the state and the organization.
Access : Production applications are deployed without source code or configuration information, limiting the capability/quality of security reviews.

Recourse : Production applications, particularly custom software, rarely have contractual terms defining vendor responsibility for vulnerability identification or remediation.

Application Security Program Objectives

1. Reduce statewide exposure to the exploitation of vulnerable software through ongoing identification and remediation of flaws in the software inventory.
2. Decrease cost and frequency of security disruption by incorporating security service levels, visibility and recourse into all software and software service contracts

NuHarbor SECURITY

Application Security is not Absolute

Outcome Expectations

Application Security Decisions must be Balanced.

- Urgency and importance are driven by actual risk.
- Activities span all phases of software acquisition or development.
- Security considerations must support business priorities.

Visibility is the goal, not perfection.

- Vulnerabilities and flaws are expected.
- Awareness drives mitigation first, remediation second.
- Expectations must be expressed and codified.
- Security information will be fully disclosed

NuHarbor SECURITY

Recommendation

Statewide Application Security Center of Excellence (ASCOE)

Establishment of central, strategic, certifying authority for application security to create and demonstrate measurable improvement in application security and accountability.

Benefits

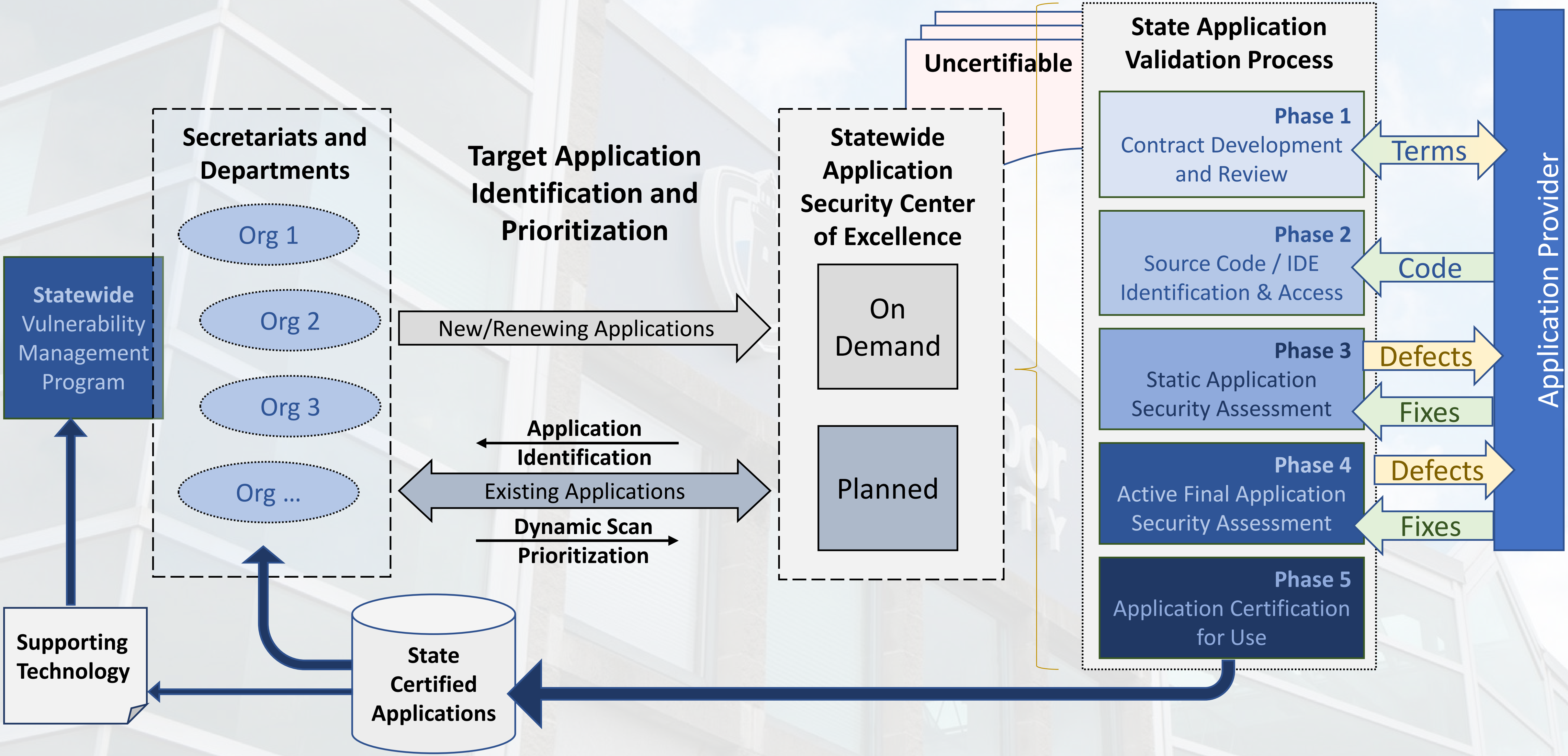
Control : Contracts for software and application acquisition written with application security conditions for acceptance of new, renewing, and priority applications, provides forward-looking improvement and security consistency.

Risk Reduction : Centralized oversight enables assessment of all applications during initial purchase or on renewal, as well as a process for regular reassessment and remediation.

Centralized Savings : Applications **certified** by the ASCOE do not require assessment on additional and future purchases, increasing shared use of applications while decreasing administrative and licensing costs.

NuHarbor
SECURITY

Application Security Center of Excellence



Statewide Vulnerability Management Program

Secretariats and Departments

Org 1

Org 2

Org 3

Org …

Target Application Identification and Prioritization

New/Renewing Applications

Application Identification

Existing Applications

Dynamic Scan Prioritization

Statewide Application Security Center of Excellence

On Demand

Planned

Uncertifiable

State Application Validation Process

Phase 1
Contract Development and Review

Phase 2
Source Code / IDE Identification & Access

Phase 3
Static Application Security Assessment

Phase 4
Active Final Application Security Assessment

Phase 5
Application Certification for Use

Terms

Code

Defects

Fixes

Defects

Fixes

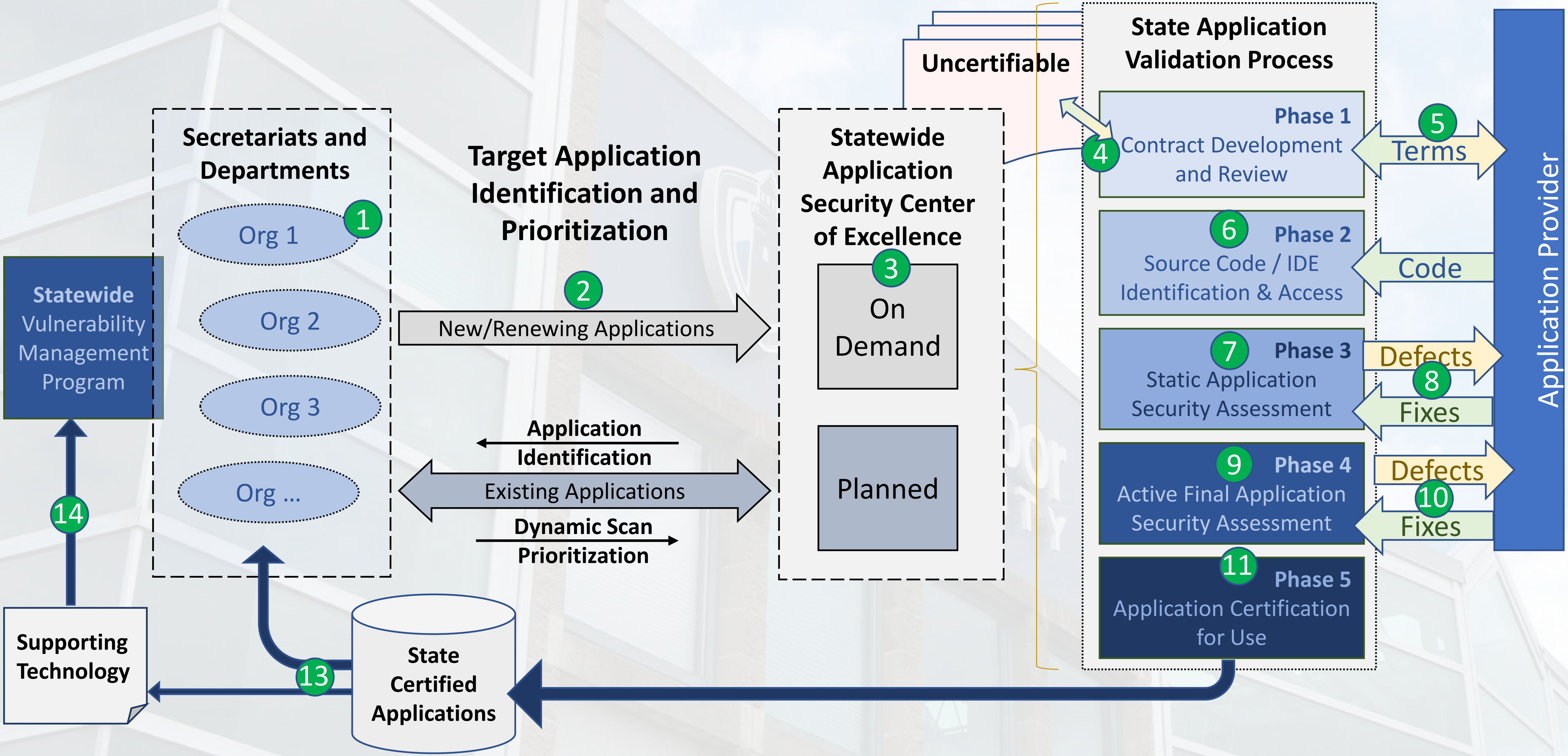
Application Provider

Supporting Technology

State Certified Applications

NuHarbor
SECURITY

New/Renewing Application Path



Secretariats and Departments

1 Org 1

Org 2

Org 3

Org ...

Target Application Identification and Prioritization

2 New/Renewing Applications

Application Identification

Existing Applications

Dynamic Scan Prioritization

Statewide Application Security Center of Excellence

3 On Demand

Planned

Uncertifiable

State Application Validation Process

4 Phase 1 Contract Development and Review

5 Terms

6 Phase 2 Source Code / IDE Identification & Access

Code

7 Phase 3 Static Application Security Assessment

Defects

8 Fixes

9 Phase 4 Active Final Application Security Assessment

Defects

10 Fixes

11 Phase 5 Application Certification for Use

Application Provider

State Certified Applications

13

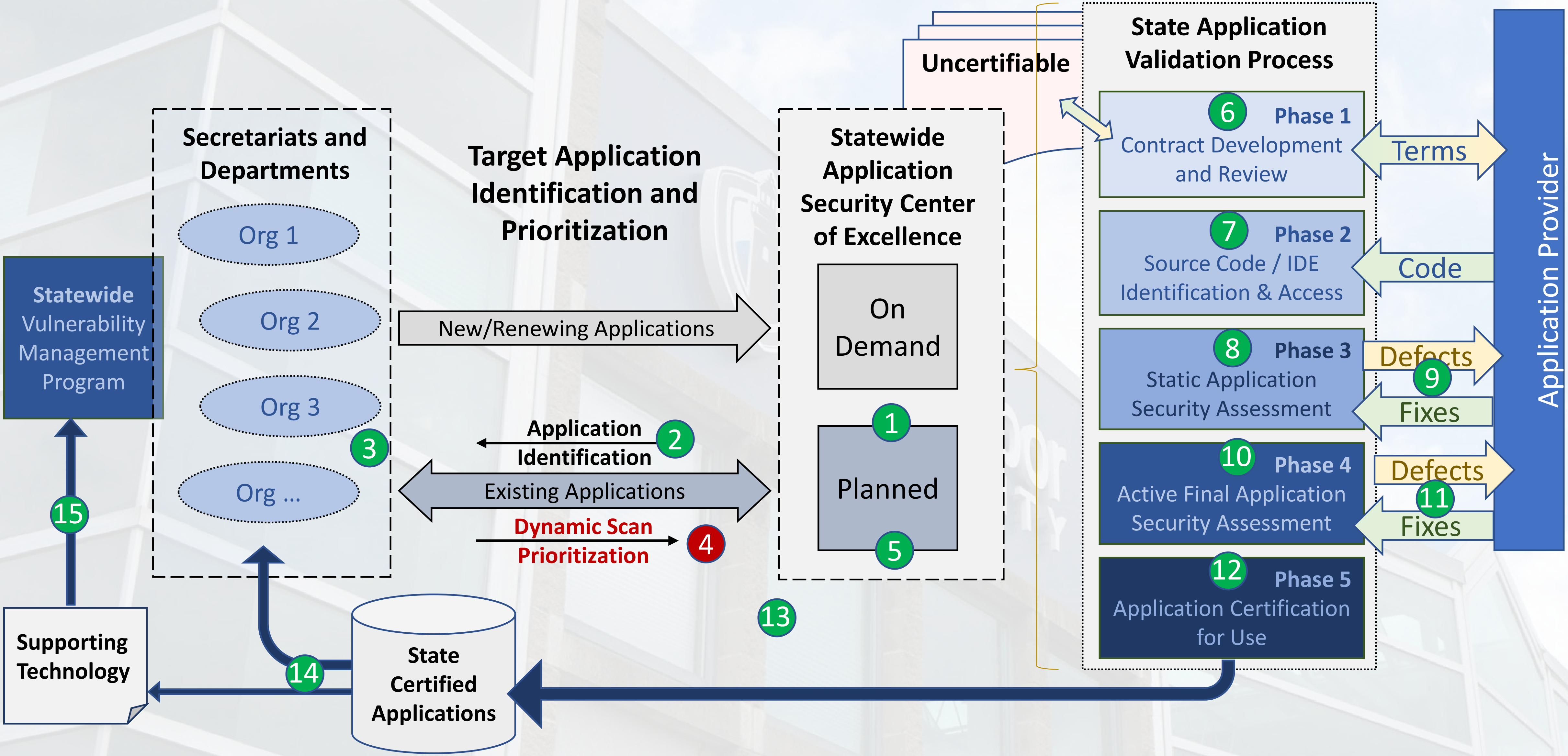
Supporting Technology

14

Statewide Vulnerability Management Program

NuHarbor SECURITY

Select Existing Application Path


Secretariats and Departments
Org 1
Org 2
Org 3
Org ...
3
Target Application Identification and Prioritization
New/Renewing Applications
Application Identification
2
Existing Applications
Dynamic Scan Prioritization
4
Statewide Application Security Center of Excellence
On Demand
1
Planned
5
Uncertifiable
State Application Validation Process
6
Phase 1
Contract Development and Review
7
Phase 2
Source Code / IDE Identification & Access
8
Phase 3
Static Application Security Assessment
10
Phase 4
Active Final Application Security Assessment
12
Phase 5
Application Certification for Use
Terms
Code
Defects
9
Fixes
Defects
11
Fixes
Application Provider
13
Statewide Vulnerability Management Program
15
Supporting Technology
14
State Certified Applications

In Conclusion

Collateral Benefits

Leadership : The ASCOE is a comprehensive strategic approach to application security.

Collaboration : Statistics, certifications, and lessons learned will benefit any similar state effort.

Communication : Internal and vendor-related assessment and trade-offs create transparency.

Vendor Rating : Application and vendor security performance are automatically gathered, rated, and reviewed to influence future contracts.

Publication : The ASCOE can publish the contract language, architecture, implementation, and results to assist other public sector organizations.

Promotion : The ASCOE has demonstrable progress during every time period without creating intractable challenges for partner organizations.

Questions?

jdanahy@nuharborsecurity.com