NIST SP 800-163
Vetting the Security of Mobile Applications

Revision 1 Update

Michael Ogata

Applied Cyber Security Division

NIST

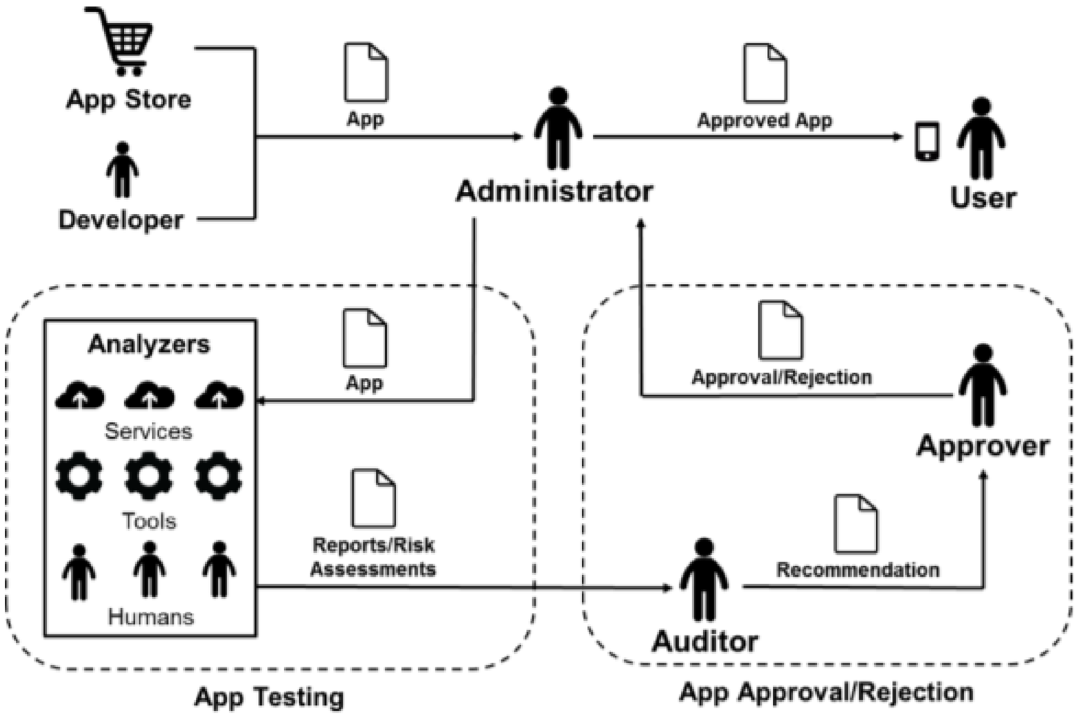
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

- Primary POC for Revision 1 of NIST SP 800-163
- 12 Years at NIST in ITL
- 5 years collaboration with Public Safety Communications Research (PSCR)
- Software and Systems Division Software Assurance Metrics and Tool Evaluation (SAMATE) Project

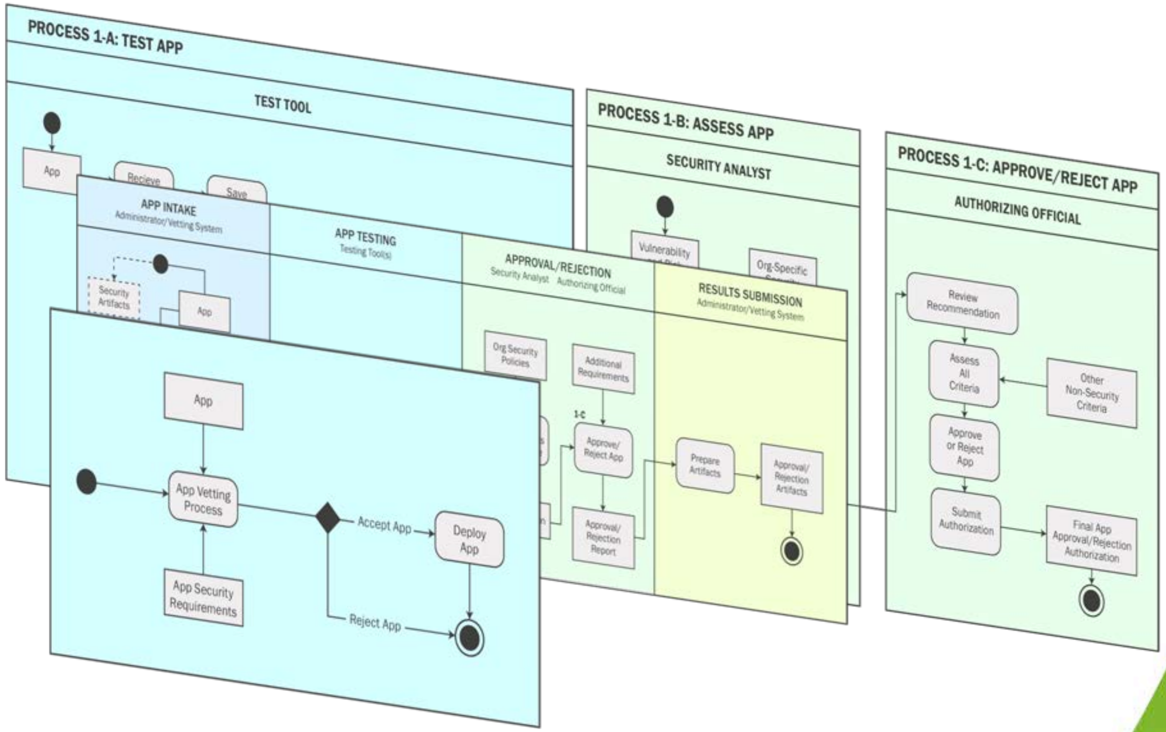
Original Document (2015)

- Defined app vetting process
- Defined an app's path through that process
- Explored threats in the mobile app landscape

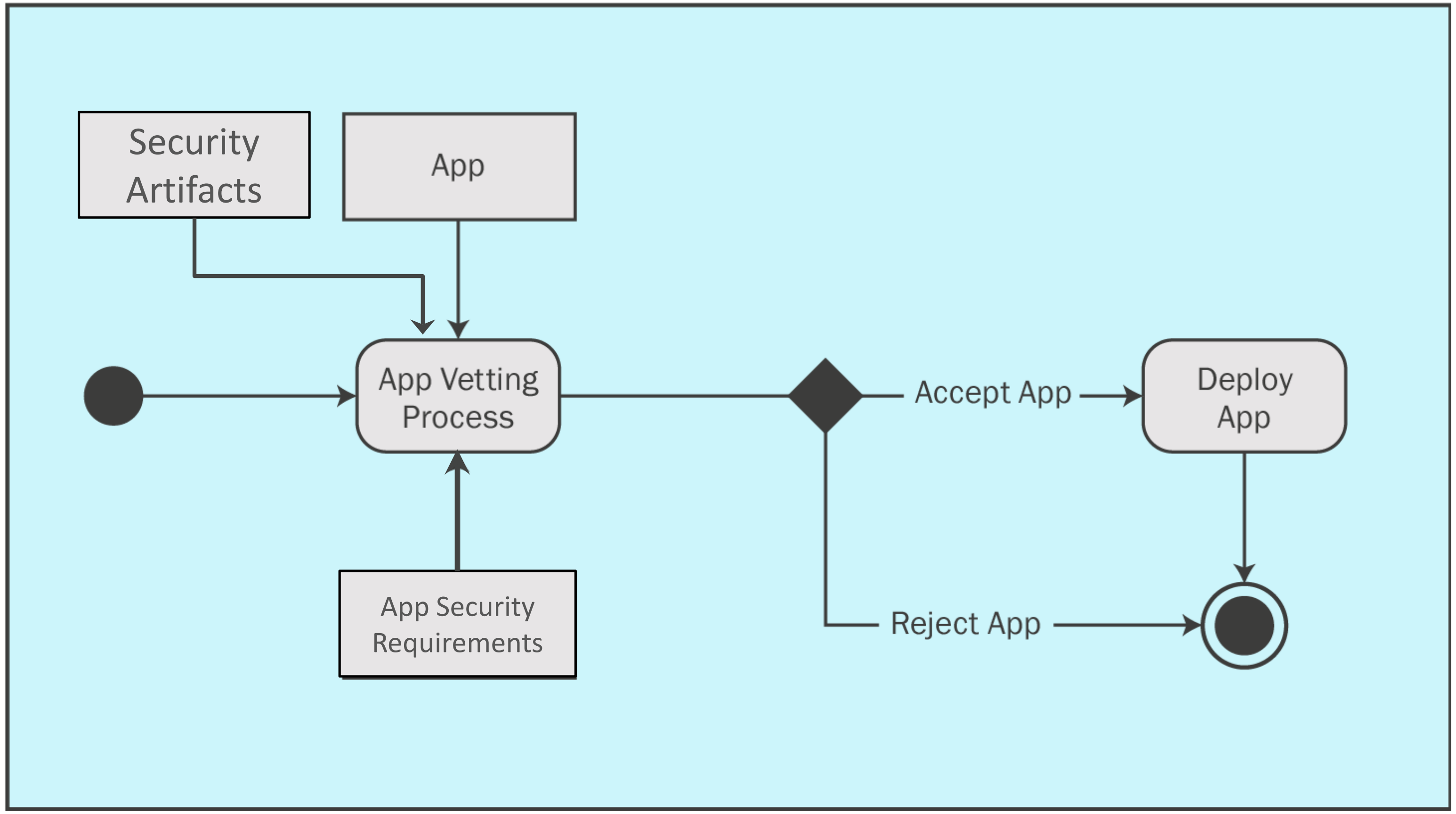


Revision 1 (2018)

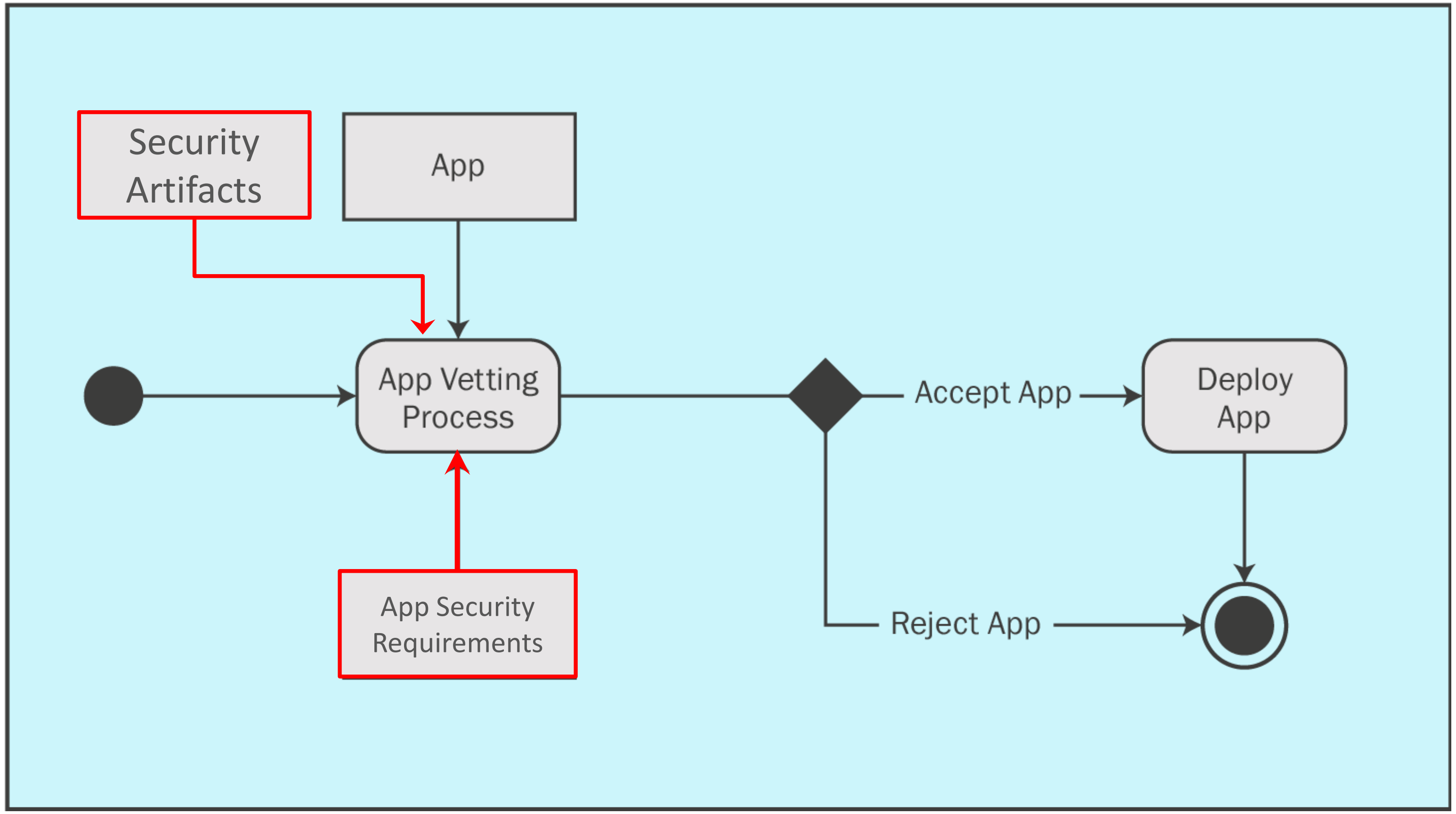
- *Expands* and *refines* vetting process
- Incorporates existing requirements and recommendations for app
  - Testing
  - Vulnerability assessment and description
- Explores threats in the mobile app landscape



Expanding Document Scope



Expanding Document Scope

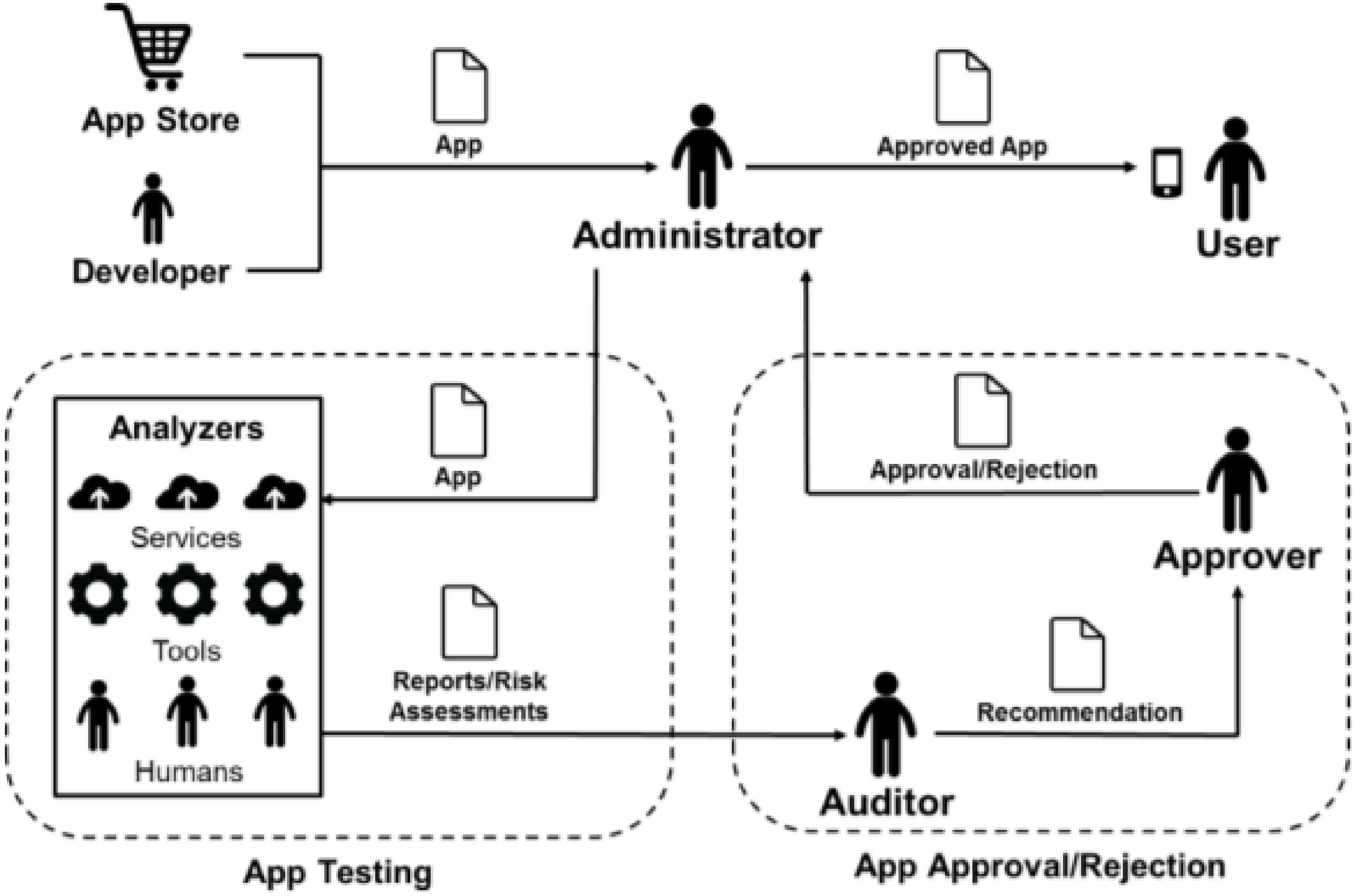


Application Security Requirements

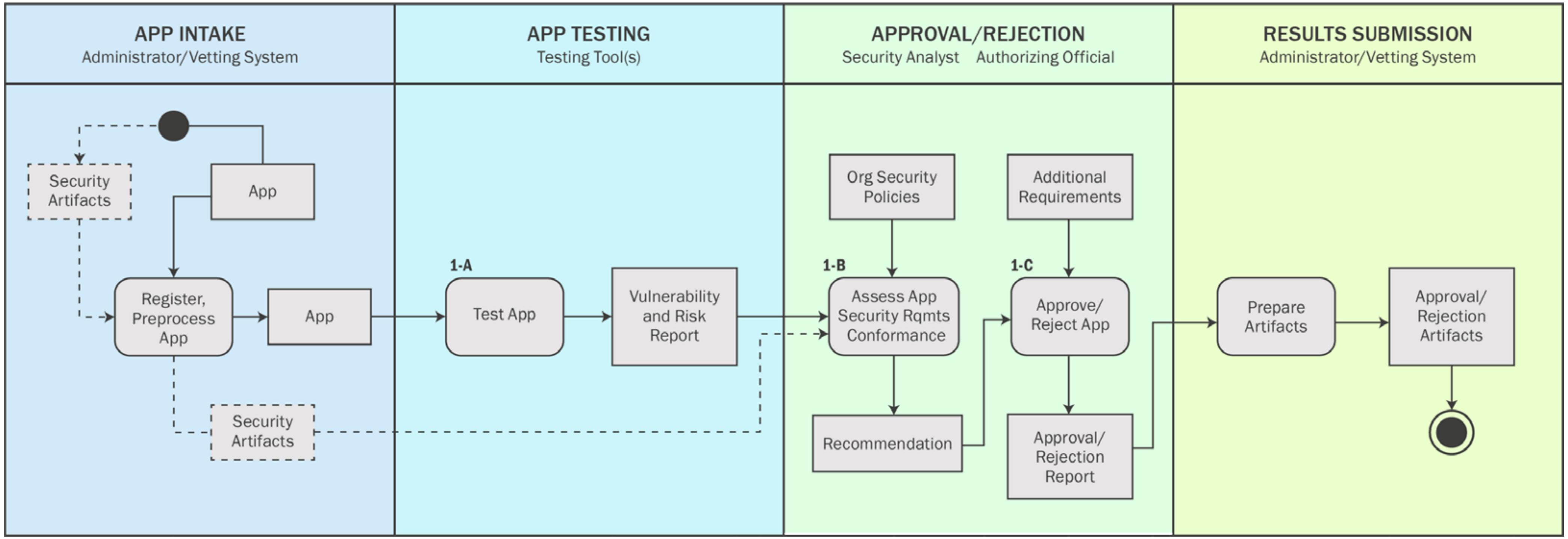
- Referencing existing requirements
  - NIAP
  - OWASP
  - MITRE
  - NIST SP 800-53

- Detailing organization-specific requirements
  - Policies
  - Provenance
  - Data Sensitivity
  - App Criticality
  - Target Users
  - Target Hardware
  - Target Environment

Refining the Process

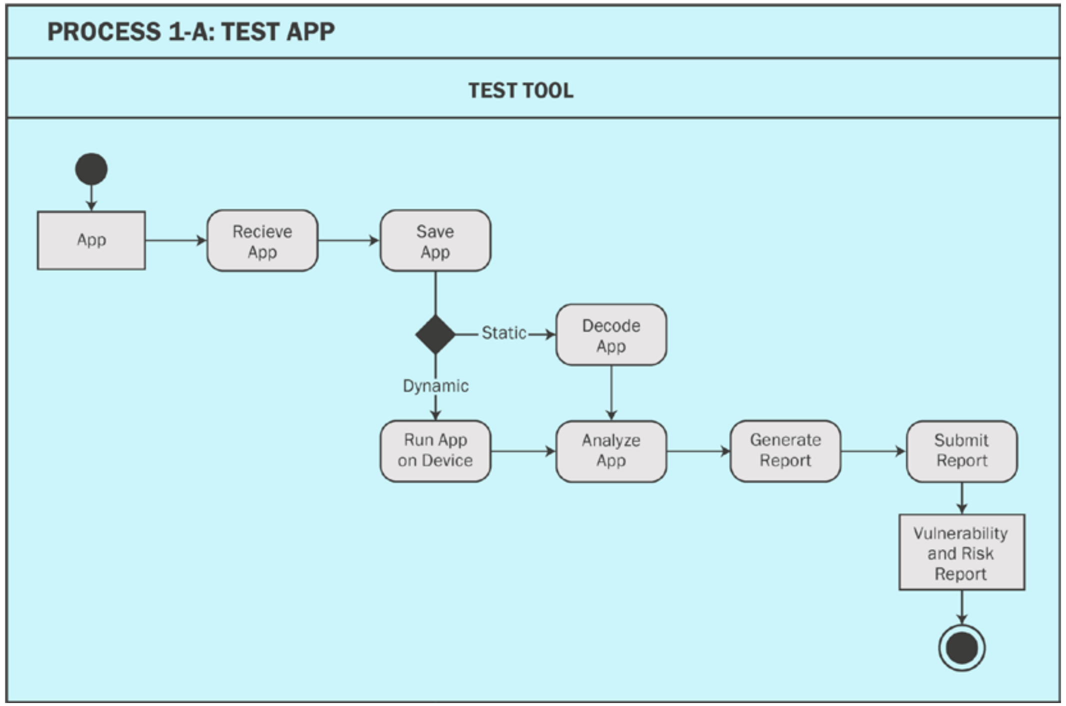


Refining the Process



App Testing and Vulnerability Classifiers

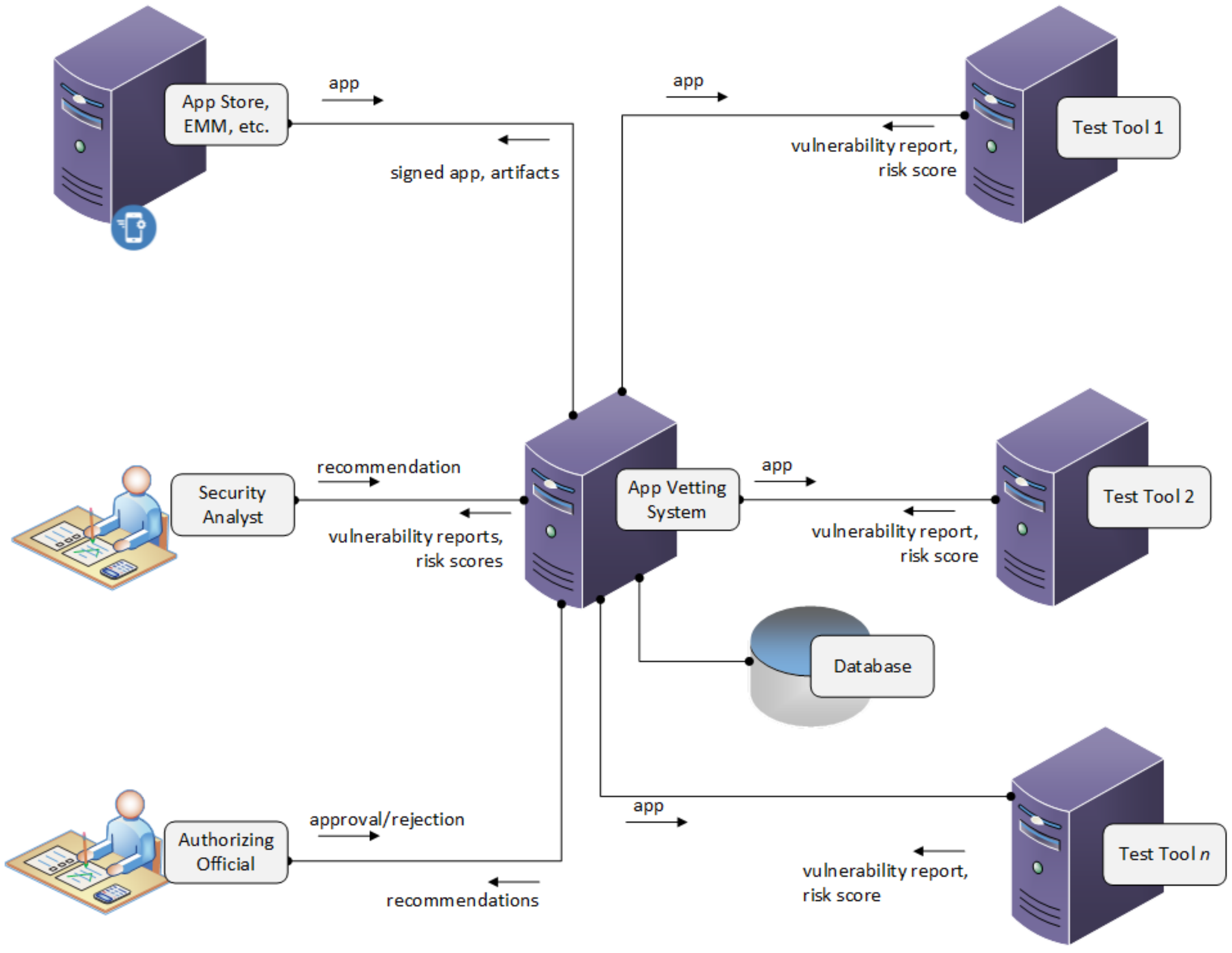
- Testing Approaches
  - Correctness Testing
  - Source and Binary Code Testing
  - Static and Dynamic Testing
- Vulnerability Classifiers and Quantifiers
  - Common Weakness Enumeration (CWE)
  - Common Vulnerability and Exposures (CVE)
  - Common Vulnerability Scoring System (CVSS)



App Vetting Considerations

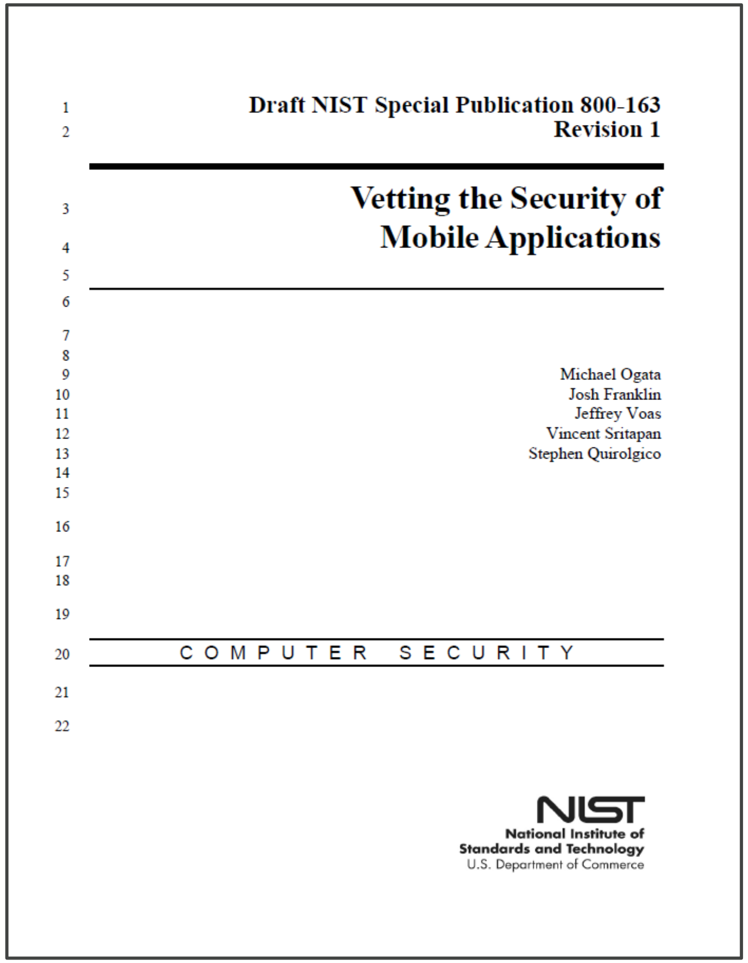
- Managed and Unmanaged Apps
- App Vetting Limitations
- Local and Remote Tools and Services
- Automated Approval/Rejection
- Reciprocity
- Budget and Staffing

Example App Vetting Architecture



Public Comment Period

- Ends September 6th
- Email comments to
  - nist800-163@nist.gov



Draft NIST Special Publication 800-163
Revision 1

Vetting the Security of Mobile Applications

Michael Ogata
Josh Franklin
Jeffrey Voas
Vincent Sritapan
Stephen Quirolgico

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce