Federal Mobile Computing Summit: Mobile Application Vetting Criteria

February 18, 2015

CIO COUNCIL

Background

- **Federal CIO Council**
  - Innovate - Innovating for the American People
  - Deliver - Maximizing the Value of Federal IT
  - Protect - Advancing our Nation's Cybersecurity
  - *Leadership – OMB/FedCIO/DHS*
- **Information Security and Identity Management Committee (ISIMC)**
  - The committee will recommend standard organization structures for information security committees across the Federal Government; and ensure the tools, metrics, and measures will lead to defensive operational capabilities and protections of the Federal networks, systems, and applications.
  - *Leadership – DoJ/DoD/NARA*
- **Mobile Technology Tiger Team (MTTT)**
  - Build broad representative membership to discuss topics of critical importance to mobile implementations across the Federal landscape. Support progress and innovation through informing development of standards.
  - *Leadership – DoJ/GSA/DoD/DHS*

Initiative

- **New "mobile" business model centered around apps**
  - As of June 2014 (Statista), both Apple and Google report over 1.2 million apps available in their stores
- **Volume too large for any one organization**
  - Opportunity to leverage collective effort/progress

- **Vision:** Establish Federal criteria for mobile application vetting to achieve reciprocity across Federal departments and agencies
  - Create a collaborative community across Government to capture, share, and leverage knowledge based on Government and private sector sources
  - Develop a common set of criteria to structure app vetting findings as part of a process to share information and encourage reciprocity across agencies while reducing the time and resources required for determination

Desired Outcomes

- **Initial goal:**
  - Draft specifications and guidance on evaluation criteria, security controls, and best practices to assess and certify the security posture of mobile apps
- **Ultimate goal:**
  - In coordination with existing Federal standards bodies, establish Federal-wide guidance for agencies to use in defining and executing their mobile app vetting and approval efforts

- **Methodology used:**
  - Key players should be in agreement to build this collaborative community
  - The group defines a scope for this effort, to include the activities and products it will develop and maintain
  - Define key near-term activities and execution plan

Process

- **Established Group (MAVSWG):**
  - Reviewed NIST 800-53, DISA MAPP SRG, Common Weakness Enumeration, OWASP Top Ten, NSA Vulnerabilities A to C, NIAP Protection Profile and other sources to evaluate as potential sources of criteria
- **Analyzed, Deliberated and Gained consensus:**
  - Produced high-level criteria to which CWE, NIAP Protection Profile requirements, and agency-specific requirements can be mapped as necessary
  - Organized criteria into categories to simplify presentation and use
  - Explored opportunities to align with NIAP Protection Profile relative and NIST App Vetting effort
  - Positioned criteria to reflect risk to an organization
- **Determine path to widest adoption**
  - Need adoption and sustainability model

Recommendation to the Federal CIO Council

- **Federal Mobile Application Vetting Criteria Adoption and Sustainment**
  - Continued Alignment with NIST 800-163 and NIAP Protection Profile as core programs for guidance
  - Publish within Digital Government Strategy and Federal CIO Council constructs for reference
  - Take advantage of NIST and NIAP established structures and review cycles to keep criteria fresh and representative of current capabilities
  - Leverage broad representation available to these processes to maintain integrity of the criteria

- **Follow on activities**
  - Processes to support Federal reciprocity
  - Support to industry for adoption

Discussion