DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

OCT - 6 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Mobile Application Security Requirements

Mobile application usage has expanded dramatically within the Department of Defense (DoD). Mission critical and business applications previously tethered to desktops are increasingly mobile-enabled. Attachment 2 included with this memorandum outlines the scope, identifies security requirements, and assigns responsibilities for the evaluation and use of unclassified mobile applications in the DoD. Security evaluations of mobile applications will adopt the DoD Risk Management Framework (Reference (a)) "Assess Only" process and require the reuse of testing artifacts leading to the reciprocal acceptance of tested results. The DoD, in collaboration with the Federal Chief Information Officers Council's Mobile Technology Tiger Team, has chosen the evaluation requirements outlined in Attachment 2 as the standard for the DoD to maintain alignment with the Federal Government.

The point of contact for this matter is Ms. Patricia (Trish) Janssen, (571) 372-4221, Patricia.l.janssen.civ@mail.mil.

John A. Zangardi
Acting

Attachments:
1) List of References
2) Mobile Application Security Requirements

Attachment 1

REFERENCES

(a) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," May 24, 2016
(b) Committee on National Security Systems (CNSS) Instruction 4009 Glossary, "Committee on National Security Systems Glossary," April 6, 2015
(c) National Information Assurance Partnership, "Requirements for Vetting Mobile Applications from the Protection Profile for Application Software," April 22, 2016
(d) National Information Assurance Partnership, "Protection Profile for Mobile Device Fundamentals," June 10, 2016
(e) DoD CIO Memorandum, "Cybersecurity Reciprocity," October 24, 2016
(f) Committee on National Security Systems Policy #11, "Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT)," June 1, 2013
(g) National Information Assurance Partnership, "Protection Profile for Application Software," April 22, 2016
(h) DoD 5500.07-R, "The Joint Ethics Regulation (JER)," November 17, 2011

Attachment 2

Subject: Mobile Application Security Requirements

A. Purpose

The purpose of this attachment is to outline the scope, identify security requirements, and assign responsibilities for the evaluation and use of mobile applications in the DoD.

B. Scope

This attachment identifies the security requirements for applications on unclassified DoD mobile devices, herein after referred to as mobile devices. Mobile devices are defined in Reference (b). Mobile applications reside on or are installed on devices with mobile operating systems (e.g. Apple iOS, Android, BlackBerry). Mobile applications are grouped into two categories: Managed and Unmanaged Applications, as defined below:

- Managed Applications are defined as applications that are controlled and installed by an enterprise management system (e.g. Mobile Device Management, Enterprise Mobility Management, Mobile Application Management) and/or have access to Controlled Unclassified Information (CUI) or connect to systems that contain CUI. These applications are segregated from unmanaged applications and unmanaged data on the device. Examples of Managed Applications include productivity and mission related applications which may be available through commercial application stores (e.g. Apple App Store, Google Play Store) or government developed/sponsored.

    - Note: All applications that reside on the managed side of the device controlled by the enterprise management system could have access to CUI and therefore shall be evaluated against the managed application requirements.

- Unmanaged Applications are defined as applications, primarily for personal use, which do not reside on the managed side of the device. These applications are typically obtained from the device's native mobile application store. These applications do not have access to CUI or information systems which may contain CUI in which the mobile device may connect or communicate. These applications are segregated by the enterprise management system, which controls the devices' capabilities. Examples of these types of applications include weather, restaurant, and public news applications.

Mobile code (e.g., web applications), as defined in Reference (b), is outside the scope of this attachment. While desktop and mobile device operating systems are converging at a fast pace, the scope of this attachment does not include the evaluation of applications for use on traditional desktop operating systems (e.g., Windows 7, Windows 10, MacOS). Mobile applications which process classified information or reside on classified devices are outside the scope of this attachment. Additionally, DoD developed applications that do not process CUI and are intended for public distribution (e.g., recruiting applications) are outside the scope of this attachment unless deployed as a Managed Application.

C. Application Security and Evaluation Requirements

The requirements in this attachment are effective immediately. Applications approved for use prior to signature of this memorandum are still approved, but must be re-evaluated in accordance with the requirements of this attachment within one year of its signature.

1. Managed Applications

To foster Federal standardization, DoD Components will use the requirements established by the National Information Assurance Partnership (NIAP), "Requirements for Vetting Mobile Applications from the Protection Profile for Application Software" (Reference (c)) for the evaluation of Managed Applications. The NIAP developed the baseline set of security requirements for organizations engaged in locally evaluating mobile applications. These requirements are achievable, testable, and repeatable and provide a basis for technical evaluation and risk determination by Authorization Officials (AOs).

Prior to deploying managed applications on mobile devices, the following requirements shall be met:

a. Managed applications shall only be used on devices which have been validated as compliant with the Mobile Device Fundamentals Protection Profile (MDFPP) (Reference (d)).
b. Managed applications shall be evaluated in accordance with Reference (c) and any applicable DoD Annexes.
c. DoD Components shall conduct their own evaluations or partner with other DoD Components with established application evaluation capabilities and expertise.
d. DoD Components conducting evaluations shall document the results of the evaluations in accordance with the DoD Mobile Application Evaluation template (to be developed, as tasked in this attachment).
e. DoD Components shall upload completed evaluation results for applications to the DoD Mobile Application Portal once established by the Defense Information Systems Agency (DISA).
f. Completed evaluation results of mobile applications shall be referenced or incorporated into existing RMF artifacts and included as part of the mobile system's overall authorization documentation.
    1) RMF authorization documentation may point to external resources where records of approved applications will be located.
g. DoD Components must leverage existing evaluation results to the greatest extent possible, in accordance with Reference (a) and DoD CIO Memorandum "Cybersecurity Reciprocity" (Reference (e)).

In addition to the requirements above, Managed Security Applications (e.g., "Secure containers," virtual private network (VPN) clients, virtual clients) whose primary purpose is to provide security in addition to the native security capabilities offered by the device shall meet the following requirements:

a. Commercial-Off-The-Shelf (COTS) applications shall comply with CNSS Policy #11 (Reference (f)) and be validated against NIAP "Protection Profile for Application Software" (Reference (g)).
b. Managed Security Applications developed by the DoD or DoD sponsored contractors (i.e., Government-Off-The-Shelf (GOTS)) shall consult the NIAP to determine the necessary evaluation requirements.

2. Unmanaged Applications

The following security requirements shall be met for the use of unmanaged applications on mobile devices:

a. The installation and use of unmanaged applications on mobile devices shall be approved by the system's AO.
b. The mobile device shall be NIAP validated in accordance with Reference (d), which includes requirements for the segregation of managed and unmanaged applications and data.
c. Unmanaged applications shall only be permitted on mobile devices capable of segregating unmanaged and managed applications and data contained therein. Mobile devices that do not support this capability shall not allow the use of unmanaged applications.
d. Mobile devices shall be configured to prevent unmanaged applications from accessing or extracting CUI and from connecting to any systems which contain CUI.
e. Acquisition of unmanaged applications is the responsibility of the user and shall not obligate the federal government for unapproved or unallowed expenses, subscriptions, or dues unless authorized. Personal use of mobile applications shall comply with the DoD Directive 5500.07-R Joint Ethics Regulation (Reference (h)).
f. Users must sign a user agreement acknowledging they received training, which includes at a minimum, operational security concerns introduced by unmanaged applications including applications utilizing global positioning system (GPS) tracking and other non-cybersecurity and/or privacy related concerns.
g. When the requirements listed above (2. a-f) are met, unmanaged applications installed from and evaluated by the devices native application store (e.g. Apple App Store, Google Play Store) do not require further evaluation.

   Note: Applications that process or store CUI which are not considered managed/unmanaged applications based on the aforementioned definitions shall still be evaluated in accordance with the requirements of a managed application.

D. Application Updates

Mobile applications are frequently updated to enhance functionality, mitigate issues (i.e. bugs), and enhance security. DoD Components must establish procedures to ensure managed applications are regularly re-evaluated in accordance with the requirements of this attachment using the following guidelines:

1. Mobile devices must be configured to automatically install application updates, as appropriate.

2. DoD Component AOs have the latitude to determine their re-evaluation frequency in accordance with Reference (a). These procedures must include the requirements for re-evaluation at a minimum of once annually.

3. Mobile Applications updates occur frequently. If the DoD Mobile Application Portal does not contain artifacts (i.e., testing results) for the current version of an application (e.g., the artifacts listed are from an older version of the application), DoD Component AOs should consider the available (existing) results and make a risk determination based on the age of the evaluation results and changes to the application since the evaluation. Retesting of only critical areas is acceptable in this instance.

4. Managed applications that are no longer supported (by the developer), have been deemed end of life, or do not pass re-evaluation must be removed from the mobile device.

E. Responsibilities:

1. DoD CIO shall:

    a. Provide guidance and review DISA's DoD Mobile Application Portal;

    b. Participate in the Commercial Mobile Device Working Group: Mobile Application Focus Group;

    c. Provide guidance and direction in the development of the DoD Mobile Application Evaluation templates; and

    d. Recommend the Enterprise Cybersecurity Software Steering Group (ESSG) consider an enterprise purchase of an automated application security evaluation tool.

2. National Security Agency (NSA) shall:

    a. Continually evaluate the risk mobile applications may present to the DoD and update References (c), (d), and (g), as appropriate; and

b. Support and advise DISA in the development of a DoD Mobile Application Evaluation template.

3. DISA shall:

a. Participate in the Mobile Application Focus Group;

b. Within 90 days, with support from NSA, develop the DoD Mobile Application Evaluation template to capture the results of DoD Components' Application evaluation results based on the criteria of Reference (c);

c. Within 90 days, establish, host, and maintain a DoD Mobile Application Portal to support the submission, hosting, searching, reporting, and availability of completed DoD Mobile Application Evaluation templates;

d. Report progress to DoD CIO on the development of the DoD Mobile Application Evaluation template and DoD Mobile Application Portal; and

e. Review and update applicable Security Technical Implementation Guides to ensure alignment with this attachment.

4. Heads of DoD Components shall:

a. Ensure mobile applications are evaluated in accordance with this attachment;

b. Review the DoD Mobile Application Portal and commercial application stores prior to developing or procuring a mobile application (to reduce duplication of efforts);

c. Submit completed DoD Mobile Application Evaluation artifacts to the DoD Mobile Application Portal hosted by DISA;

d. Review the DoD Mobile Application Portal prior to initiating an Application Evaluation and reuse any applicable evaluation results (to reduce duplication of efforts);

e. Establish an application re-evaluation process for managed applications;

f. Provide security training to users on the potential threats and risks associated with using unmanaged applications which may contain capabilities such as location sharing, personal information sharing, or may have nefarious characteristics (e.g. marketing scams, human trafficking, etc.). Additionally, training must provide users' awareness of best practices when using managed applications; and

g. Ensure user agreements for mobile devices include guidance on acceptable personal use, including unmanaged applications, and an acknowledgement by the user that they have received appropriate training.